

DIN EN ISO 16484-5

ICS 35.240.99; 91.140.01

Einsprüche bis 2013-11-27
Vorgesehen als Ersatz für
DIN EN ISO 16484-5:2012-11**Entwurf****Systeme der Gebäudeautomation –
Teil 5: Datenkommunikationsprotokoll (ISO 16484-5:2012);
Englische Fassung prEN ISO 16484-5:2013, nur auf CD-ROM**

Building automation and control systems –
Part 5: Data communication protocol (ISO 16484-5:2012);
English version prEN ISO 16484-5:2013, only on CD-ROM

Systèmes d'automatisation et de gestion technique du bâtiment –
Partie 5: Protocole de communication de données (ISO 16484-5:2012);
Version anglaise prEN ISO 16484-5:2013, seulement en CD-ROM

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-09-27 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nhrs@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Heiz- und Raumluftechnik (NHRS) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 1073 Seiten

Normenausschuss Heiz- und Raumluftechnik (NHRS) im DIN
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Dieses Dokument (prEN ISO 16484-5:2013) wurde vom Technischen Komitee ISO/TC 205 „Building environment design“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 247 „Gebäudeautomation und Gebäudemanagement“ (Sekretariat: SNV, Schweiz) unter Beteiligung deutscher Experten erarbeitet.

Das zuständige deutsche Gremium ist der Arbeitsausschuss NA 041-03-68 AA „Gebäudeautomation und -kommunikation (SpA CEN/TC 247/WG 4)“ im Normenausschuss Heiz- und Raumlufttechnik (NHRS).

Dieses Dokument (prEN ISO 16484-5:2013) übernimmt den englischen Originaltext des ANSI/ASHRAE Standard 135 „BACnet — A Data Communication Protocol for Building Automation and Control Networks“, Ausgabe 2012. In derselben Weise sollen zwischenzeitlich veröffentlichte bzw. noch zu veröffentlichende Änderungen und Erweiterungen von ANSI/ASHRAE Standard 135 bei der Fortschreibung von EN ISO 16484-5 übernommen werden. Der Inhalt dieses Dokumentes befindet sich auf der beiliegenden CD-ROM.

Der NHRS war für das DIN Deutsches Institut für Normung e. V. an der Erstellung dieser Norm beteiligt. Da davon auszugehen ist, dass die Fachleute der Kommunikationstechnik sich bereits mit der englischen Fassung befasst haben, wurde von einer Übersetzung ins Deutsche abgesehen. Nach dem DIN-Präsidialbeschluss 13/1983 ist insbesondere auf dem Gebiet der Informatik die Veröffentlichung in Englisch zulässig, insbesondere wenn dadurch Fehler bei der Übertragung vermieden werden können.

Dieses Dokument (prEN ISO 16484-5:2013) stellt ein Kommunikationsverfahren zur Verfügung, mit dem Geräte der Gebäudeautomation untereinander Informationen austauschen können, unabhängig von der gebäudetechnischen Anlage, zu der sie gehören. Das in dieser Norm spezifizierte Protokoll kann universell für den Datenaustausch von Geräten und Systemen in der Gebäudeautomation sowohl zum allgemeinen Einsatz, als auch für anwenderspezifische Lösungen eingesetzt werden.

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 9545 siehe DIN ISO/IEC 9545

Änderungen

Gegenüber DIN EN ISO 16484-5:2012-11 wurden folgende Änderungen vorgenommen:

- a) Inhalt technisch überarbeitet.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 9545, *Informationstechnik — Kommunikation Offener Systeme — Struktur der Anwendungsschicht*

Nationaler Anhang NB (informativ)

Begriffe

Im Folgenden wird ISO 16484-5:2013, Abschnitt 3 ins Deutsche übersetzt. Die Benennung der folgenden Begriffe und Abkürzungen ist identisch mit der Benennung in der englischen Fassung.

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden aus Internationalen Normen übernommenen bzw. für die vorliegende Norm definierten Begriffe.

3.1 Aus Internationalen Normen übernommene Begriffe

Die folgenden in dieser Norm verwendeten Begriffe sind in Internationalen Normen bzw. Norm-Entwürfen zur Kommunikation offener Systeme (open system interconnection, OSI) definiert. Diese Definitionen sind an dieser Stelle unter Verweisung auf die entsprechende Norm erneut aufgeführt. Abschnitt 25 enthält die Titel aller im vorliegenden Abschnitt und an weiteren Stellen in dieser Norm genannten nationalen und Internationalen Normen. Kursiv dargestellte Wörter oder Wortgruppen beziehen sich auf Begriffe, die an anderer Stelle im vorliegenden Abschnitt definiert sind.

3.1.1

abstrakte Syntax

(en: abstract syntax)

Festlegung von Daten der Anwendungsschicht oder von *Anwendungsprotokoll-Steuerinformationen* durch Anwendung von Notationsregeln, die von der zu ihrer Darstellung verwendeten Kodierungstechnik unabhängig sind (ISO 8822)

3.1.2

Anwendung

(en: application)

Menge von Informationsverarbeitungsanforderungen eines *Benutzers* (ISO 8649)

3.1.3

Anwendungsentität

(en: application-entity)

die OSI betreffenden Aspekte eines *Anwendungsprozesses* (ISO 7498)

3.1.4

Anwendungsprozess

(en: application-process)

Element innerhalb eines *realen offenen Systems*, das die Informationsverarbeitung für eine bestimmte *Anwendung* durchführt (ISO 7498)

3.1.5

Anwendungsprotokoll-Steuerinformationen

(en: application-protocol-control-information)

Informationen, die mit Hilfe von Darstellungsdiensten zwischen *Anwendungsentitäten* ausgetauscht werden, um deren gemeinsame Operation zu koordinieren (ISO 9545)

3.1.6

Anwendungsprotokoll-Dateneinheit

(en: application-protocol-data-unit)

in einem Anwendungsprotokoll festgelegte Dateneinheit, die aus *Anwendungsprotokoll-Steuerinformationen* und eventuell Anwendungsbenutzerdaten besteht (ISO 9545)

3.1.7

Anwendungsdienstelement

(en: application-service-element)

Teil einer *Anwendungsentität*, der eine OSI-Umgebungsfähigkeit bereitstellt, gegebenenfalls unter Verwendung zugrunde liegender Dienste (ISO 7498)

3.1.8

konkrete Syntax

(en: concrete syntax)

diejenigen Aspekte der bei der formalen Festlegung von Daten angewendeten Regeln, die eine spezifische Darstellung dieser Daten verkörpern (ISO 7498)

3.1.09

Bestätigung (primitiv)

(en: confirm (primitive))

Darstellung einer Interaktion, bei der ein *Dienstanbieter* an einem bestimmten *Dienstzugangspunkt* anzeigt, dass er eine Prozedur abgeschlossen hat, die an diesem *Dienstzugangspunkt* zuvor durch eine durch ein *Anforderungsprimitiv* dargestellte Interaktion aufgerufen wurde (ISO/TR 8509)

3.1.10

Anzeige (primitiv)

(en: indication (primitive))

Darstellung einer Interaktion, bei der ein *Dienstanbieter* entweder

- a) anzeigt, dass er auf eigene Veranlassung hin eine Prozedur aufgerufen hat oder
- b) anzeigt, dass eine Prozedur vom *Dienstbenutzer* am gleichrangigen *Dienstzugangspunkt* aufgerufen wurde (ISO TR 8509)

3.1.11

Peer-Entitäten

(en: peer-entities)

Entitäten innerhalb derselben Schicht (ISO 7498)

3.1.12

reales offenes System

(en: real open system)

reales System, das bei seiner Kommunikation mit anderen *realen Systemen* die Anforderungen von OSI-Normen einhält (ISO 7498)

3.1.13

reales System

(en: real system)

Satz von einem oder mehreren Rechnern, der dazugehörigen Software, Peripheriegeräten, Endgeräten, menschlichen Bedienern, physikalischen Prozessen, Informationsübertragungsmitteln usw., der ein autonomes Ganzes bildet, das in der Lage ist, Informationsverarbeitung und/oder Informationstransfer durchzuführen (ISO 7498)

3.1.14

Anforderung(primitiv)

(en: request (primitive))

Darstellung einer Interaktion, bei der ein *Dienstbenutzer* eine Prozedur aufruft (ISO/TR 8509)

3.1.15

Antwort (primitiv)

(en: response (primitive))

Darstellung einer Interaktion, bei der ein *Dienstbenutzer* anzeigt, dass er eine Prozedur abgeschlossen hat, die zuvor durch eine durch ein *Anzeigeprimitiv* dargestellte Interaktion aufgerufen wurde (ISO/TR 8509)

3.1.16

(N)-Dienstzugangspunkt

(en: (N)-service-access-point)

Punkt, an dem (N)-Dienste von einer (N)-*Entität* für eine (N+1)-*Entität* bereitgestellt werden (ISO 7498)

3.1.17

(N)-Dienstdateneinheit

(en: (N)-service-data-unit)

Menge von (N)-Schnittstellendaten, deren Identität vom einen Ende einer (N)-Verbindung bis zum anderen gewahrt bleibt (ISO 7498)

3.1.18

Dienstbenutzer

(en: service-user)

Entität in einem einzelnen offenen System, die über *Dienstzugangspunkte* einen Dienst benutzt (ISO/TR 8509)

3.1.19

Dienstprimitiv; Primitiv

(en: service-primitive; primitive)

abstrakte, implementierungsunabhängige Darstellung einer Interaktion zwischen dem *Dienstbenutzer* und dem *Dienstanbieter* (ISO/TR 8509)

3.1.20

Dienstanbieter

(en: service-provider)

Abstraktum der Gesamtheit der Entitäten, die gleichrangigen *Dienstbenutzern* einen Dienst bereitstellen (ISO TR 8509)

3.1.21

Transfersyntax

(en: transfer syntax)

bei der Übertragung von Daten zwischen offenen Systemen verwendete *konkrete Syntax* (ISO 7498)

3.1.22

Benutzerelement

(en: user element)

Darstellung des Teils eines *Anwendungsprozesses*, der die zur Erreichung der Kommunikationsziele dieses *Anwendungsprozesses* notwendigen *Anwendungsdienstelemente* nutzt (ISO 7498)

3.2 Für die vorliegende Norm definierte Begriffe

3.2.1

Zugriffskontrolle

(en: access control)

Verfahren zur Regelung oder Einschränkung des Zugriffs auf *Netzwerkressourcen*

3.2.2

Zugriffsrechte (physische Zugangskontrolle)

(en: access rights (physical access control))

Zugriffsrechte, die auf Anmeldedaten gewährt werden

3.2.3

Zugreifender Benutzer (physische Zugangskontrolle)

(en: access user (physical access control))

Person oder Inhalt, welche/welcher ein oder mehrere Anmeldeinformationen hat

3.2.4

Alarm

(en: alarm)

1. hörbare und/oder sichtbare Meldung, die einen Bediener auf einen nicht normalen Zustand, der eine Korrekturmaßnahme erfordern kann, aufmerksam macht
2. von einem Gerät oder Controller erkannter nicht normaler Zustand, wobei das Gerät bzw. der Controller eine speziell für diesen Zustand ausgelegte Regel oder Logik implementiert

3.2.5

Algorithmic Change Reporting

(en: algorithmic change reporting)

Erkennen und Berichten eines Alarms oder Ereignisses auf der Grundlage eines in einem Event-Enrollment-Objekt festgelegten Algorithmus. Siehe auch *Intrinsic Reporting* unter 3.2.37

3.2.6

Authentifizierung

(en: authentication)

Vorgang zur Verifizierung der Identität

3.2.7

Authentifizierungs-Faktor

(en: authentication factor)

Datenelement der Anmeldeinformationen, das verwendet wird, um die Identität des Anmeldenden zu verifizieren

3.2.8

Autorisierung (Netzwerksicherheit)

(en: authorization (network security))

Kontrolle des Zugangs zu Netzwerkressourcen basierend auf Identitätsprüfung und Zugriffsregeln

3.2.9

Autorisierung (physische Zugangskontrolle)

(en: authorization (physical access control))

Prozess zur Bestimmung, ob es für den Anwender zulässig ist, einen geschützten Bereich über einen zugangskontrollierten Punkt zu betreten

3.2.10

BACnet-Gerät

(en: BACnet device)

jedes reale oder virtuelle Gerät, das eine digitale Kommunikation unter Anwendung des BACnet-Protokolls unterstützt

3.2.11

BACnet-Benutzer

(en: BACnet-user)

Teil eines *Anwendungsprozesses*, der durch das *BACnet-Benutzerelement* repräsentiert wird

3.2.12

Bridge

(en: bridge)

Einrichtung, die zwei oder mehr *Segmente* auf der physikalischen Schicht und der Daten Verbindungsschicht miteinander verbindet. Diese Einrichtung kann auf der Grundlage von MAC-Schicht-Adressen auch Nachrichten filtern

3.2.13

Broadcast

(en: broadcast)

als einzelne Einheit gesendete Nachricht, die sich an mehr als ein Gerät richten kann

3.2.14

Zustandsänderung

(en: change of state)

Ereignis, das dann auftritt, wenn sich ein gemessener oder berechneter Boolescher Wert oder ein diskreter numerischer bzw. Zählwert ändert

3.2.15

Wertänderung

(en: change of value)

Ereignis, das dann auftritt, wenn sich ein Messwert oder ein berechneter Analogwert um einen definierten Wert ändert

3.2.16

Client

(en: client)

System oder Einrichtung, das/die eine andere Einrichtung für einen bestimmten Zweck über eine *Dienstanforderungsinstanz* einsetzt. Ein Client fordert einen Dienst bei einem *Server* an

3.2.17

konfigurierbar

(en: configurable)

Eigenschaft, Einstellung oder Wert in einem Gerät ist konfigurierbar, wenn er/sie über BACnet-Dienste oder ein anderes Verfahren geändert werden kann. Eine Eigenschaft, Einstellung, oder ein Wert, die/der nur einmal beschreibbar oder in situ nicht veränderbar ist, wird nicht als konfigurierbar betrachtet

3.2.18

Kontext

(en: context)

Satz von Daten oder Informationen, der eine bestimmte Kommunikationsumgebung zu einem bestimmten Zeitpunkt vollständig beschreibt

3.2.19

Controller

(en: controller)

Einrichtung zur Regelung bzw. zum Management eines Systems oder einer Komponente

3.2.20

Anmeldeinformationen (physische Zugangskontrolle)

(en: credentials (physical access control))

Kombination aus Authentifizierungs-Faktoren und Zugangsrechten

3.2.21

Vertraulichkeit von Daten

(en: data confidentiality)

Eigenschaft, dass Informationen unbefugten Personen, Entitäten oder Prozessen nicht zur Verfügung gestellt oder offengelegt werden

3.2.22

Datenintegrität

(en: data integrity)

Eigenschaft, dass Daten nicht auf nicht autorisierte Weise verändert oder zerstört wurden

3.2.23

Authentifizierung der Datenherkunft

(en: data origin authentication)

Bestätigung, dass die Quelle der empfangenen Daten tatsächlich den Angaben entspricht

3.2.24

Datumsmuster

(en: date pattern)

Datum, das eine oder mehrere nicht spezifische Oktette oder spezielle Datumswerte enthalten kann

3.2.25

direkt verbundenes Netzwerk

(en: directly connected network)

Netzwerk, das von einem Router aus zugänglich ist, ohne dass Nachrichten über einen Zwischenrouter weitergeleitet werden müssen. Zu einem direkt verbundenen Netzwerk besteht eine PTP-Verbindung, wenn die PTP-Verbindung gerade aktiv ist und kein Zwischenrouter verwendet wird

3.2.26

Download

Herunterladen

(en: download)

bestimmte Art der Dateiübertragung, die sich auf die Übertragung eines ausführbaren Programms oder einer Datenbank auf ein abgesetztes Gerät bezieht, auf dem die Datei ausgeführt werden kann

3.2.27

verschlüsselte Nachricht

(en: encrypted message)

Nachricht, die in einen Security Header eingehüllt, signiert, und verschlüsselt ist

3.2.28

Entität

Gebilde

(en: entity)

eigenständiger, sich unterscheidender Gegenstand der Betrachtung. Ein identifizierbares Element, das mittels einer Sammlung oder eines Satzes von Eigenschaften beschrieben wird

3.2.29

Fehlererkennung

(en: error detection)

Prozedur, die dazu verwendet wird, das Vorhandensein von Fehlern in einer Kommunikation zu identifizieren

3.2.30

Fehlerbehebung

(en: error recovery)

Prozedur, die als Reaktion auf einen erkannten Fehler aufgerufen wird und ein Fortsetzen des Informationsaustausches erlaubt

3.2.31

Ereignis-Algorithmus

(en: event algorithm)

Regeln, die bestimmen, wann ein ereignis-initiierendes Objekt zwischen normalen und offnormal Status wechselt. Der Ereignis-Algorithmus hat keine Auswirkungen auf den Übergang eines ereignis-initiierenden Objektes zu oder von einem Fehler.

3.2.32

ereignis-initiierendes Objekt

(en: event-initiating object)

Objekt, das so konfiguriert ist, seinen Ereignis-Zustand zu überwachen und Änderungen seines Ereignis-Zustandes zu melden

3.2.33

Ereignis-Benachrichtigungs-Verteilung

(en: event-notification-distribution)

Prozess, den ein Benachrichtigung-Server bei der Bestimmung der Notification-Clients und der Zusendung von Benachrichtigungen an Notification-Clients durchführt, wenn ein ereignis-initiiierendes Objekt das Ereignis oder den Anerkennungs-Zustand (en: acknowledgment state) wechselt

3.2.34

Ereignisbenachrichtigung

(en: event notification message)

ConfirmedEventNotification oder UnconfirmedEventNotification Dienstanforderung, die dazu verwendet wird, um eine Veränderung des Ereignisses oder des Anerkennungs-Zustandes eines ereignis-initiiierenden Objektes anzuzeigen

3.2.35

Ereignisstatus-Feststellung

(en: event-state-detection)

Prozess der Ausführung des Ereignis-Algorithmus eines ereignis-initiiierenden Objektes und die Überwachung der Zuverlässigkeitseigenschaft des Objektes um Veränderungen des Ereignis-Zustands des Objektes zu erfassen

3.2.36

Ereigniszusammenfassung

(en: event-summarization)

Abfrage von ereignis-initiiierenden Objekten in einem Gerät durch einen der Ereigniszusammenfassungs-Dienste um diejenigen zu bestimmen, die bestimmte Ereignis-Zustand- oder Berichterstattungs-Bedingungen erfüllen

3.2.37

Fading

(en: fading)

allmähliche Erhöhung oder Verringerung der tatsächlichen Ausgabe von einer Einstellung in eine andere über einen bestimmten Zeitraum

3.2.38

Gateway

Netzübertragungseinheit

(en: gateway)

Einrichtung zur Verbindung zweier oder mehrerer nicht gleicher *Netzwerke*, um den Informationsaustausch zwischen diesen Netzwerken zu ermöglichen

3.2.39

global

(en: global)

alle Geräte oder Knoten auf einem *Inter-Netzwerk* betreffend

3.2.40

globales Broadcast

en: global broadcast

an alle Geräte oder *Knoten* auf allen Netzwerken in einem BACnet-*Internet* adressierte Nachricht

3.2.41

Halbrouter

(en: half router)

Gerät oder *Knoten*, der als ein Partner an einer PTP-Verbindung teilnehmen kann. Die beiden Halbrouter-Partner, die zusammen eine aktive PTP-Verbindung bilden, ergeben einen einzelnen *Router*

3.2.42

unfähiges Gerät

(en: incapable device)

Gerät, das von Natur aus unfähig ist oder konfiguriert wurde, unfähig zu erscheinen, sichere BACnet Nachrichten zu produzieren oder zu verarbeiten

3.2.43

Initialisierung

(en: initialization)

Vorgang des Herbeiführens eines bekannten Zustands, üblicherweise nach einer Stromanschaltung. Die Initialisierung kann eine Wiedereingabe der logischen oder physikalischen Adresse eines Knotens erfordern

3.2.44

Inter-Netzwerk

Verbindungsnetzwerk

(en: internetwork)

Verbindung von zwei oder mehreren *Netzwerken* über *Router*. In einem BACnet-*Inter-Netzwerk* gibt es zwischen zwei beliebigen Knoten genau einen Nachrichtenweg

3.2.45

Intrinsic Reporting

(en: intrinsic reporting)

Erkennen und Berichten eines Alarms oder Ereignisses auf der Grundlage eines als Teil der *Objekttyp*-Spezifikation definierten Algorithmus. Dabei findet keine externe Verweisung auf ein „Event Enrollment“ statt. Siehe auch *Algorithmic Change Reporting* unter 3.2.5

3.2.46

invertiertes Netzwerk

(en: inverted network)

BACnet Inter-Netzwerk, bei dem zwei oder mehr Netzwerke durch ein Netzwerk verbunden sind, dessen NPDU kleiner als die des beitretenden Netzwerkes ist

3.2.47

Schlüssel

(en: key)

Symbolsequenz zur Regelung der Chiffrierung und Dechiffrierung

3.2.48

lokal

(en: local)

Geräte auf demselben *Netzwerk* wie das betrachtete Gerät betreffend

3.2.49

lokales Broadcast

(en: local broadcast)

Nachricht, die an alle Geräte oder *Knoten* adressiert ist, die sich auf demselben *Netzwerk* wie die Nachrichtenquelle befinden

3.2.50

Medium

(en: medium)

physikalische Übertragungsentität. Typische Medien sind verdrehte Doppelader-Leitungen, Faseroptik-Kabel und Koaxialkabel

3.2.51

Medienzugriffskontrolle

(en: medium access control)

Vorgang zur Wahrung der Ordnung und zur Gewährung des Zugriffs auf das Kommunikationsmedium

3.2.52

Netzwerk

(en: network)

Satz von einem oder mehreren durch *Bridges* verbundenen *Segmenten* mit derselben Netzwerkadresse

3.2.53

Netzwerkressource

(en: network resource)

jede physikalische oder logische *Entität*, auf die über ein Kommunikationsmedium zugegriffen werden kann

3.2.54

Knoten

(en: node)

mit dem Kommunikationsmedium verbundene adressierbare Einrichtung

3.2.55

Notification-Client

(en: notification-client)

BACnet-Gerät, das Ereignisbenachrichtigungen empfängt und verarbeitet

3.2.56

Benachrichtigungsserver

(en: notification-server)

BACnet-Gerät, das ereignis-initiierende Objekte enthält und die Verteilung von Ereignisbenachrichtigungen durchführt

3.2.57

Objekt

(en: object)

spezifische Instanz eines *Objektyps*. Während ein Objekttyp durch eine eindeutige *Object_Type*-Eigenschaft bezeichnet ist, ist ein Objekt durch seine *Object_Identifier*-Eigenschaft bezeichnet

3.2.58

Objektprofil

(en: object profile)

Mittel zum Definieren von Objekten über die in Abschnitt 12 definierten Objekte hinaus. Ein Profil definiert den Satz von Eigenschaften, Verhalten und/oder Anforderungen, der für ein proprietäres Objekt oder proprietäre Erweiterungen eines Normobjekts gilt

3.2.59

Objekttyp

Objektart

(en: object type)

generische Datenklassifizierung, definiert durch einen Satz *Eigenschaften*

3.2.60

Bediener-Authentifizierung

(en: operator authentication)

Bestätigung der Identität des sich an einer Einrichtung anmeldenden Bedieners

3.2.61

Authentifizierung der Peer-Entität

(en: peer entity authentication)

die Bestätigung der Identität einer assoziierten Peer-Entität

3.2.62

physische Zugangskontrolle (PACS)

(en: physical access control (PACS))

elektronisches System, das durch Authentifizierung und Autorisierung an Zugangskontrollpunkten die Fähigkeit von Personen und Fahrzeugen, einen geschützten Bereich zu betreten, kontrolliert

3.2.63

physikalisches Segment

(en: physical segment)

einzelnes zusammenhängendes *Medium*, an das BACnet-Knoten angebunden sind

3.2.64

physisch unsicher

(en: physically insecure)

nicht physisch sicher

3.2.65

physisch sicher

(en: physically secure)

Gerät oder Netzwerk, das vor physischem Zugang nicht autorisierter Individuen geschützt ist

3.2.66

einfaches Gerät

(en: plain device)

Gerät, das normalerweise keine sicheren BACnet-Nachrichten erzeugt oder verarbeitet. Alle unfähigen Geräte sind einfache Geräte. Ein einfaches Gerät, das kein unfähiges Gerät ist, ist fähig, sichere BACnet-Nachrichten zu erzeugen und zu verarbeiten, wenn die Kommunikation mit einem anderen Gerät dies erfordert

3.2.67

einfaches Netzwerk

(en: plain network)

Netzwerk, das keinen signierten oder verschlüsselten Datenverkehr benötigt

3.2.68

einfache Nachricht

(en: plain message)

Nachricht, die nicht durch einen BACnet Security Wrapper geschützt ist

3.2.69

druckbares Zeichen

(en: printable character)

Zeichen, das im Gegensatz zu einem Gerätesteuersymbol ein druckbares Symbol darstellt. Dazu gehören unter anderem Groß- und Kleinbuchstaben, Satzzeichen und mathematische Symbole. Der genaue Satz hängt von dem verwendeten Zeichensatz ab

3.2.70

Eigenschaft

(en: property)

spezielles Charakteristikum eines *Objektyps*

3.2.71

proprietär

herstellerspezifisch

(en: proprietary)

im BACnet-Kontext jede Erweiterung oder Ergänzung der in dieser Norm festgelegten *Objektypen*, *Eigenschaften*, PrivateTransfer-Diensten oder Aufzählungen

3.2.72

Ramping

(en: ramping)

allmähliche Zunahme oder Abnahme des tatsächlichen Ausgangs von einer Einstellung zur anderen mit einer festen Veränderungsrate

3.2.73

empfangender BACnet-Benutzer

(en: receiving BACnet-user)

der *BACnet-Benutzer*, der ein *Anzeige-* oder *Bestätigungs-*Dienstprimitiv empfängt

3.2.74

abgesetzt

Fern-

(en: remote)

Geräte oder *Knoten* betreffend, die sich auf einem anderen Netzwerk als das referenzierte Gerät befinden

3.2.75

Fern-Broadcast

(en: remote broadcast)

Nachricht, die an alle Geräte oder *Knoten* adressiert ist, die sich auf einem anderen *Netzwerk* als die Nachrichtenquelle befinden

3.2.76

Repeater

Verstärker

(en: repeater)

Einrichtung, die zwei oder mehr *physikalische Segmente* auf der physikalischen Schicht verbindet

3.2.77

anfordernder BACnet-Benutzer

(en: requesting BACnet-user)

BACnet-Benutzer, der in einem bestätigten Dienst die Rolle eines *Clients* übernimmt

3.2.78

antwortender BACnet-Benutzer

(en: responding BACnet-user)

BACnet-Benutzer, der in einem bestätigten Dienst die Rolle eines *Servers* übernimmt

3.2.79

Funktionsgruppenbasierte Zugangskontrolle (RBAC)

(en: role-based access control)

Zugangsrechte, die spezifischen Funktionsgruppen zugewiesen sind. Der Nutzer erhält die Zugangsrechte über die ihm zugewiesene Funktionsgruppe

3.2.80

Router

Wegwahleinheit

(en: router)

Gerät zur Verbindung eines oder mehrerer *Netzwerke* auf der Vermittlungsschicht

3.2.81

sicheres Netzwerk

(en: secure network)

Netzwerk, in dem sämtlicher Datenverkehr signiert oder verschlüsselt sein muss

3.2.82

Sicherheit

Schutz

(en: security)

eine von einer Vielzahl von Vorgehensweisen zur Sicherstellung der Überwachung des Informationsaustausches, um einer Offenlegung gegenüber unbefugten Personen vorzubeugen. Sicherheitsmaßnahmen sollen die Offenlegung sensibler Informationen auch gegenüber jenen verhindern, die einen gültigen Zugriff auf das Kommunikationsnetzwerk haben. Sicherheit unterscheidet sich von Zugriffskontrolle, wenngleich auch durch die Einschränkung des physischen Zugriffs auf das Kommunikationsmedium selbst ein gewisses Maß an Sicherheit erreicht werden kann

3.2.83

Segment

(en: segment)

Segment besteht aus einem oder mehreren miteinander über Repeater verbundenen *physikalischen Segment(en)*

3.2.84

sendender BACnet-Benutzer

(en: sending BACnet-user)

BACnet-Benutzer, der ein *Anforderungs-* oder *Antwort-Dienst* primitiv ausgibt

3.2.85

Server

(en: server)

System oder Einrichtung bzw. Gerät, das (die) für einen bestimmten Zweck auf eine Dienstanforderungsinstanz antwortet. Der Server stellt einen Dienst für einen *Client* bereit

3.2.86

signierte Nachricht

(en: signed message)

Nachricht, die in einen Security Header eingehüllt, signiert, und nicht verschlüsselt ist

3.2.87

spezieller Datumswert

(en: special date value)

Datumswert, der einem speziellen Wert wie z. B. „gerade Monate“, „letzter Tag des Monats“ usw. entspricht. Diese speziellen Datumswerte werden in Unterkomponenten (Oktetten) eines Datumswertes verwendet

3.2.88

spezifisches Datum

(en: specific date)

vollständig spezifiziertes Datum, das keine nicht spezifischen Oktette oder spezielle Datumswerte enthalten darf

BEISPIEL Januar 24, 1991, Wochentag = Donnerstag.

3.2.89

spezifische Datumszeit

(en: specific datetime)

BACnetDateTime-Konstrukt zusammengesetzt aus einem spezifischen Datum und einer spezifischen Zeit

3.2.90

spezifische Zeit

(en: specific time)

vollständig spezifizierte Zeit, die keine nicht spezifischen Oktette enthalten darf

BEISPIEL 17:35:45,17 (= 5:35:45,17 P. M.).

3.2.91

Standard-Objektyp

(en: standard object type)

durch diese Norm definierter Objektyp, bei dem der numerische Wert im für ASHRAE reservierten Bereich liegt

3.2.92

Standard-Eigenschaft

(en: standard property)

erforderliche oder optionale Eigenschaft eines Standard-Objektyps, bei der der numerische Wert der Eigenschaftskennung im für ASHRAE reservierten Bereich liegt und die Eigenschaft in der Objektyp-Eigenschafts Tabelle in Abschnitt 12 aufgeführt ist

3.2.93

Staffelung

(en: stepping)

Zunahme oder Abnahme eines Ausgangswertes in diskreten Schritten

3.2.94

Synchronisierung

(en: synchronization)

Möglichkeit für Prozesse, bestimmte Stellen in einer Übertragung oder einem Austausch zu definieren und zu identifizieren, die genutzt werden können, um eine Kommunikationssitzung in einen vordefinierten Zustand zurückzusetzen

3.2.95

Zeitmuster

(en: time pattern)

Zeit, die ein oder mehrere nicht spezifizierte Oktette enthalten kann

3.2.96

Zeitstempel

(en: timestamp)

einem Ereignis oder einer Handlung zugeordneter Eintrag über Datum und Uhrzeit

3.2.97

vertrauenswürdig

(en: trusted)

Begriff, der für Geräte oder Netzwerke angewendet wird, deren Nachrichten für authentisch gehalten werden, entweder durch die Verwendung von sicheren Nachrichten oder basierend auf der physischen Sicherheit des Gerätes oder Netzwerkes

3.2.98

Zeiteinheit

(en: unit_time)

Länge der Zeit, die erforderlich ist, um ein Oktett mit einem Startbit und einem einzigen Stoppbit zu senden. Zehn Bitintervalle

3.2.99

nicht spezifiziertes Datum

(en: unspecified date)

Datum, das ausschließlich aus nicht spezifizierten Oktetten besteht (Wert von X'FF' = D'255')

3.2.100

nicht spezifizierte Datumszeit

(en: unspecified datetime)

BACnetDateTime Konstrukt zusammengesetzt aus einem nicht spezifizierten Datum und einer nicht spezifizierten Zeit

3.2.101

nicht spezifiziertes Oktett

(en: unspecified octet)

Oktett, das im Zusammenhang mit Datum, Zeit oder BACnetWeekNDay Werten verwendet wird und den Wert X'FF' = D'255' beinhaltet

3.2.102

nicht spezifizierte Zeit

(en: unspecified time)

Zeit, die ausschließlich aus nicht spezifizierten Oktetten besteht (Wert von X'FF' = D'255')

3.2.103

Upload

Hochladen

(en: upload)

Prozess, ein Abbild eines ausführbaren Programms oder eine Datenbank von einer abgesetzten Einrichtung so zu übertragen, dass ein anschließender Download erfolgen kann

3.3 Abkürzungen in der vorliegenden Norm

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
A	application layer	Anwendungsschicht (Präfix)
ABA	American Bankers Association	American Bankers Association
AE	application entity	Anwendungsentität
ANSI	American National Standards Institute	American National Standards Institute
APCI	application protocol control information	Anwendungsprotokoll-Steuerinformationen
APDU	application layer protocol data unit	Protokolldateneinheit der Anwendungsschicht
API	application program interface	Anwendungsprogramm-Schnittstelle
ARCNET	attached resource computer network	Attached Resource Computer Network
ASE	application service element	Anwendungsdienstelement
ASN.1	Abstract Syntax Notation One	Notation Eins für Abstrakte Syntax (ISO 8824)
B' '	denotes that binary notation is used between the single quotes	gibt an, dass zwischen den Anführungszeichen eine Binärschreibweise verwendet wird
BAC	building automation and control	Gebäudeautomation (GA)
BBMD	BACnet/IP broadcast management device	Einrichtung für das BACnet/IP-Broadcast-Management
BDT	broadcast distribution table	Broadcast-Verteilungstabelle
B/IP	BACnet/IP	BACnet/IP
B/IP-M	BACnet/IP multicast	BACnet/IP-Multicast
BVLC	BACnet virtual link control	virtuelle Verbindungsteuerung von BACnet
BVLCI	BACnet virtual link control information	Steuerinformationen der virtuellen Verbindung von BACnet
BVLL	BACnet virtual link layer	virtuelle Verbindungsschicht von BACnet
C	conditional	bedingt

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
C(=)	conditional (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	bedingt (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
CNF	confirm primitive	Bestätigungsprimitiv
COV	change of value	Wertänderung
CRC	cyclic redundancy check	zyklische Redundanzprüfung
D' '	denotes that decimal notation is used between the single quotes	gibt an, dass zwischen den Anführungszeichen eine Dezimalschreibweise verwendet wird
DA	local destination MAC layer address	MAC-Schicht-Adresse des lokalen Ziels
DADR	ultimate destination MAC layer address	MAC-Schicht-Adresse des endgültigen Ziels
DER	data expecting reply	Daten erwarten Antwort
DES	Data Encryption Standard (FIPS 46-1)	Datenverschlüsselungsstandard (FIPS 46-1)
DESFire	Data Encryption Standard Fast, Innovative, Reliable and Secure	Datenverschlüsselungsstandard Schnell, Innovativ, Zuverlässig und Sicher
DID	ARCNET destination MAC address	MAC-Adresse des ARCNET-Ziels
DLEN	1-octet length of ultimate destination MAC layer address	1-Oktett-Länge der MAC-Schicht-Adresse des endgültigen Ziels
DNET	2-octet length of ultimate destination MAC layer address	2-Oktett-Länge der MAC-Schicht-Adresse des endgültigen Ziels
DSAP	LLC destination service access point (X'82' for BACnet)	Dienstzugangspunkt des LLC-Ziels (X'82' für BACnet)
EIB	European Installation Bus	Europäischer Installationsbus
EIBA	European Installation Bus Association	European Installation Bus Association
EXEC	capable of executing a service request	fähig, eine Dienstanforderung auszuführen (execute)
FDT	foreign device table	Fremdgerätetabelle
ICI	interface control information	Schnittstellensteuerinformation
IL	ARCNET information length field	ARCNET-Feld Informationslänge
IND	indication primitive	Anzeigeprimitiv
INF	„Infinity“, a unique binary pattern representing positive infinity (see ANSI/IEEE 754-1985)	„Unendlich“, ein eindeutiges Binärmuster, das positiv unendlich darstellt (siehe ANSI/IEEE 754-1985)
-INF	„Negative infinity“, a unique binary pattern representing negative infinity (see ANSI/IEEE 754-1985)	„Negativ unendlich“, ein eindeutiges Binärmuster, das negativ unendlich darstellt (siehe ANSI/IEEE 754-1985)
IEEE	Institute of Electrical and Electronics Engineers	Institute of Electrical and Electronics Engineers
INIT	capable of initiating a service request	fähig, eine Dienstanforderung einzuleiten (initiate)

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
IP	Internet Protocol – RFC 791	Internet-Protokoll – RFC 791
ISO	International Organization for Standardization	Internationale Organisation für Normung
KNX	Konnex System Specification: EIB is the core protocol of the Konnex standard. The Konnex System Specification reflects the current status for EIB.	Konnex-System-Spezifikation: EIB ist das Kernprotokoll des Konnex-Standards. Die Konnex-System-Spezifikation spiegelt den derzeitigen Stand für EIB wider.
L	data link (prefix)	Datenverbindung (Präfix)
LAN	local area network	Local Area Network
LLC	logical link control (ISO 8802-2)	logische Verbindungssteuerung
LPCI	link protocol control information	Verbindungsprotokoll-Steuerinformation
LPDU	link protocol data unit	Verbindungsprotokoll-Dateneinheit
LRC	Longitudinal Redundancy Check	Longitudinale Redundanzprüfung
LSAP	link service access point (X'82' for BACnet)	Verbindungsdienstzugriffspunkt (X'82' für BACnet)
LSDU	link service data unit	Verbindungsdienstdateneinheit
M	mandatory	verpflichtend
M(=)	mandatory (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	verpflichtend (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
MA	medium access (prefix)	Medienzugriff (Präfix)
MAC	medium access control	Medienzugriffskontrolle
MPCI	MAC protocol control information	MAC-Protokollsteuerinformation
MPDU	MAC layer protocol data unit	MAC-Schicht-Protokolldateneinheit
MSDU	MAC service data unit	MAC-Dienstdateneinheit
MS/TP	master-slave/token-passing	Master-Slave/Token-Passing
N	network layer (prefix)	Vermittlungsschicht (Präfix)
NaN	„Not a Number“, a unique binary pattern representing an invalid number (see ANSI/IEEE 754-1985)	„Keine Zahl“, ein eindeutiges Binärmuster, das eine ungültige Zahl darstellt (siehe ANSI/IEEE 754-1985)
NAT	Network Address Translation – RFC 2663	Network Address Translation – RFC 2663
NP	network priority	Netzwerkpriorität
NPCI	network protocol control information	Netzwerkprotokoll-Steuerinformationen
NPDU	network layer protocol data unit	Vermittlungsschicht-Protokolldateneinheit
NRZ	non-return to zero	Non-Return-To-Zero
NSAP	network service access point	Netzwerkdienstzugriffspunkt
NSDU	network service data unit	Netzwerkdienstdateneinheit

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
O	indicates that support of a property is optional	gibt an, dass die Unterstützung einer Eigenschaft optional ist
OSI	open systems interconnection	Kommunikation offener Systeme
P	physical layer (prefix)	physikalische Schicht (Präfix)
PAC	ARCNET data packet header octet	Oktett des ARCNET-Datenpaket-Headers
PCI	protocol control information	Protokollsteuerinformation
PDU	protocol data unit	Protokolldateneinheit
PICS	protocol implementation conformance statement	Konformitätserklärung zur Protokollimplementierung
PK	Private Key	privater Schlüssel
PPCI	physical layer protocol control information	Protokollsteuerinformationen der physikalischen Schicht
PPDU	physical protocol data unit	physikalische Protokolldateneinheit
PPP	Point-To-Point protocol – RFC 1661	Punkt-zu-Punkt-Protokoll – RFC 1661
PSDU	physical service data unit	physikalische Dienstdateneinheit
PTP	point-to-point	Punkt-zu-Punkt
R	indicates that a property shall be supported and readable using BACnet services	gibt an, dass eine Eigenschaft unterstützt werden und lesbar (readable) sein muss
REQ	request primitive	Anforderungsprimitiv
RFC	request for comment	Request for Comment
RSP	response primitive	Antwortprimitiv
S	selection	Auswahl
S(=)	selection (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	Auswahl (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
SA	local network source MAC layer address	MAC-Schicht-Adresse der lokalen Netzwerkquelle
SAP	service access point	Dienstzugangspunkt
SC	ARCNET system code (X'CD' for BACnet)	ARCNET-Systemcode (X'CD' für BACnet)
SDU	service data unit	Dienstdateneinheit
SIA	Security Industry Association	Security Industry Association
SID	ARCNET source MAC address	MAC-Adresse der ARCNET-Quelle
SK	Session Key	Sitzungsschlüssel
SLEN	1-octet length of original source MAC layer address	1-Oktett-Länge der MAC-Schicht-Adresse der ursprünglichen Quelle
SLIP	Serial Line Internet Protocol	Serial Line Internet Protocol (RFC 1055)

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
SNET	2-octet original source network number	2-Oktett-Netzwerknummer der ursprünglichen Quelle
SPC	standard project committee	ASHRAE-Ausschuss für Normungsvorhaben
SSAP	LLC source service access point (X'82' for BACnet)	LLC-Quellen-Dienstzugangspunkt (X'82' für BACnet)
TSM	transaction state machine	Transaktionszustandsmaschine
U	user option	Benutzeroption
U(=)	user option (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	Benutzeroption (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
UART	universal asynchronous receiver/transmitter	Universeller Asynchron-Empfänger/-Sender
UDP	User Datagram Protocol – RFC 768	User Datagram Protocol – RFC 768
UTC	Universal Time Coordinated	Koordinierte Weltzeit
VT	virtual terminal	virtuelles Terminal
W	indicates that a property shall be supported, readable, and writable using BACnet services	gibt an, dass eine Eigenschaft unterstützt werden und lesbar und schreibbar (writable) sein muss
X'	denotes that hexadecimal notation is used between the single quotes	gibt an, dass zwischen den Anführungszeichen eine Hexadezimalschreibweise verwendet wird
XID	eXchange IDentification (ISO 8802-2)	Exchange Identification (ISO 8802-2)

Blank page

CONTENTS

FOREWORD	vii
1 PURPOSE	1
2 SCOPE	1
3 DEFINITIONS	1
3.1 Terms Adopted from International Standards	1
3.2 Terms Defined for this Standard	2
3.3 Abbreviations and Acronyms Used in this Standard	7
4 BACnet PROTOCOL ARCHITECTURE	10
4.1 The BACnet Collapsed Architecture	11
4.2 BACnet Network Topology	13
4.3 Security	15
5 THE APPLICATION LAYER	16
5.1 The Application Layer Model	16
5.2 Segmentation of BACnet Messages	20
5.3 Transmission of BACnet APDUs	21
5.4 Application Protocol State Machines	25
5.5 Application Protocol Time Sequence Diagrams	42
5.6 Application Layer Service Conventions	51
6 THE NETWORK LAYER	53
6.1 Network Layer Service Specification	53
6.2 Network Layer PDU Structure	55
6.3 Messages for Multiple Recipients	60
6.4 Network Layer Protocol Messages	61
6.5 Network Layer Procedures	64
6.6 BACnet Routers	66
6.7 Point-To-Point Half-Routers	71
7 DATA LINK/PHYSICAL LAYERS: ISO 8802-3 ("Ethernet") LAN	76
7.1 The Use of ISO 8802-2 Logical Link Control (LLC)	76
7.2 Parameters Required by the LLC Primitives	76
7.3 Parameters Required by the MAC Primitives	76
7.4 Physical Media	76
8 DATA LINK/PHYSICAL LAYERS: ARCNET LAN	77
8.1 The Use of ISO 8802-2 Logical Link Control (LLC)	77
8.2 Parameters Required by the LLC Primitives	77
8.3 Mapping the LLC Services to the ARCNET MAC Layer	77
8.4 Parameters Required by the MAC Primitives	77
8.5 Physical Media	77
9 DATA LINK/PHYSICAL LAYERS: MASTER-SLAVE/TOKEN PASSING (MS/TP) LAN	79
9.1 Service Specification	79
9.2 Physical Layer	81
9.3 MS/TP Frame Format	92
9.4 Overview of the MS/TP Network	93
9.5 MS/TP Medium Access Control	94
9.6 Cyclic Redundancy Check (CRC)	111
9.7 Interfacing MS/TP LANs with Other BACnet LANs	112
9.8 Responding BACnet User Processing of Messages from MS/TP	112
9.9 Repeaters	112
10 DATA LINK/PHYSICAL LAYERS: POINT-TO-POINT (PTP)	114
10.1 Overview	114
10.2 Service Specification	114
10.3 Point-to-Point Frame Format	119
10.4 PTP Medium Access Control Protocol	121
11 DATA LINK/PHYSICAL LAYERS: EIA/CEA-709.1 ("LonTalk") LAN	142
11.1 The Use of ISO 8802-2 Logical Link Control (LLC)	142
11.2 Parameters Required by the LLC Primitives	142

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

Contents

11.3	Mapping the LLC Services to the LonTalk Application Layer	142
11.4	Parameters Required by the Application Layer Primitives	142
11.5	Physical Media	143
12	MODELING CONTROL DEVICES AS A COLLECTION OF OBJECTS	144
12.1	Accumulator Object Type	148
12.2	Analog Input Object Type	157
12.3	Analog Output Object Type	162
12.4	Analog Value Object Type	167
12.5	Averaging Object Type	172
12.6	Binary Input Object Type	175
12.7	Binary Output Object Type	181
12.8	Binary Value Object Type	187
12.9	Calendar Object Type	193
12.10	Command Object Type	195
12.11	Device Object Type	199
12.12	Event Enrollment Object Type	208
12.13	File Object Type	215
12.14	Group Object Type	218
12.15	Life Safety Point Object Type	220
12.16	Life Safety Zone Object Type	227
12.17	Loop Object Type	234
12.18	Multi-state Input Object Type	242
12.19	Multi-state Output Object Type	247
12.20	Multi-state Value Object Type	252
12.21	Notification Class Object Type	257
12.22	Program Object Type	260
12.23	Pulse Converter Object Type	266
12.24	Schedule Object Type	274
12.25	Trend Log Object Type	280
12.26	Access Door Object Type	289
12.27	Event Log Object Type	297
12.28	Load Control Object Type	304
12.29	Structured View Object Type	314
12.30	Trend Log Multiple Object Type	317
12.31	Access Point Object Type	326
12.32	Access Zone Object Type	342
12.33	Access User Object Type	350
12.34	Access Rights Object Type	353
12.35	Access Credential Object Type	359
12.36	Credential Data Input Object Type	368
12.37	CharacterString Value Object Type	373
12.38	DateTime Value Object Type	378
12.39	Large Analog Value Object Type	381
12.40	BitString Value Object Type	386
12.41	OctetString Value Object Type	391
12.42	Time Value Object Type	394
12.43	Integer Value Object Type	397
12.44	Positive Integer Value Object Type	402
12.45	Date Value Object Type	407
12.46	DateTime Pattern Value Object Type	410
12.47	Time Pattern Value Object Type	413
12.48	Date Pattern Value Object Type	416
12.49	Network Security Object Type	419
12.50	Global Group Object Type	422
12.51	Notification Forwarder Object Type	429
12.52	Alert Enrollment Object Type	435
12.53	Channel Object Type	438

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

Contents

12.54	Lighting Output Object Type	447
13	ALARM AND EVENT SERVICES.....	460
13.1	Change of Value Reporting	461
13.2	Event Reporting	464
13.3	Event Algorithms	475
13.4	Fault Algorithms	504
13.5	AcknowledgeAlarm Service.....	509
13.6	ConfirmedCOVNotification Service	511
13.7	UnconfirmedCOVNotification Service	512
13.8	ConfirmedEventNotification Service	514
13.9	UnconfirmedEventNotification Service	517
13.10	GetAlarmSummary Service	519
13.11	GetEnrollmentSummary Service.....	521
13.12	GetEventInformation Service.....	524
13.13	LifeSafetyOperation Service	526
13.14	SubscribeCOV Service.....	528
13.15	SubscribeCOVProperty Service	531
14	FILE ACCESS SERVICES	534
14.1	AtomicReadFile Service	535
14.2	AtomicWriteFile Service.....	538
15	OBJECT ACCESS SERVICES.....	541
15.1	AddListElement Service	541
15.2	RemoveListElement Service	543
15.3	CreateObject Service.....	545
15.4	DeleteObject Service.....	547
15.5	ReadProperty Service.....	548
15.6	Deleted Clause	550
15.7	ReadPropertyMultiple Service	551
15.8	ReadRange Service	554
15.9	WriteProperty Service	559
15.10	WritePropertyMultiple Service	561
15.11	WriteGroup Service.....	564
16	REMOTE DEVICE MANAGEMENT SERVICES	566
16.1	DeviceCommunicationControl Service.....	566
16.2	ConfirmedPrivateTransfer Service.....	568
16.3	UnconfirmedPrivateTransfer Service	570
16.4	ReinitializeDevice Service	571
16.5	ConfirmedTextMessage Service	573
16.6	UnconfirmedTextMessage Service	575
16.7	TimeSynchronization Service	576
16.8	UTCTimeSynchronization Service	577
16.9	Who-Has and I-Have Services	578
16.10	Who-Is and I-Am Services	580
17	VIRTUAL TERMINAL SERVICES.....	582
17.1	Virtual Terminal Model	582
17.2	VT-Open Service.....	586
17.3	VT-Close Service	588
17.4	VT-Data Service.....	589
17.5	Default-terminal Characteristics.....	591
18	ERROR, REJECT, and ABORT CODES.....	595
18.1	Error Class - DEVICE	595
18.2	Error Class - OBJECT	595
18.3	Error Class - PROPERTY	596
18.4	Error Class - RESOURCES	597
18.5	Error Class - SECURITY	597
18.6	Error Class - SERVICES.....	599
18.7	Error Class - COMMUNICATION.....	600

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

Contents

18.8	Error Class - VT	602
18.9	Reject Reason.....	603
18.10	Abort Reason.....	603
18.11	Confirmed Service Common Errors.....	604
19	BACnet PROCEDURES	605
19.1	Backup and Restore.....	605
19.2	Command Prioritization	609
19.3	Device Restart Procedure	613
20	ENCODING BACnet PROTOCOL DATA UNITS	614
20.1	Encoding the Fixed Part of BACnet APDUs.....	614
20.2	Encoding the Variable Part of BACnet APDUs	625
21	FORMAL DESCRIPTION OF APPLICATION PROTOCOL DATA UNITS	639
22	CONFORMANCE AND INTEROPERABILITY	714
22.1	Conformance to BACnet	714
22.2	BACnet Interoperability	715
23	EXTENDING BACnet TO ACCOMMODATE VENDOR PROPRIETARY INFORMATION	717
23.1	Extending Enumeration Values.....	717
23.2	Using the PrivateTransfer Services to Invoke Non-Standardized Services.....	718
23.3	Adding Proprietary Properties to a Standardized Object.....	718
23.4	Adding Proprietary Object Types to BACnet.....	719
23.5	Restrictions on Extending BACnet	719
24	NETWORK SECURITY	720
24.1	Overview	720
24.2	Security Wrapper.....	724
24.3	Security Messages	728
24.4	Securing an APDU	744
24.5	Securing an NPDU	745
24.6	Securing a BVLL	745
24.7	Securing Messages	747
24.8	Network Security Network Trust Levels.....	749
24.9	Network Security Policies	750
24.10	Network Security.....	751
24.11	End-to-End Security.....	752
24.12	Wrapping and Unwrapping Secure Messages	752
24.13	Authenticating Messages.....	754
24.14	User Authentication.....	757
24.15	Time Synchronization Requirements	758
24.16	Integrating the Security Layer into the BACnet Stack	759
24.17	BACnet Security In A NAT Environment	766
24.18	BACnet Security Proxy.....	766
24.19	Deploying Secure Device on Non-Security Aware Networks.....	766
24.20	Deploying Secure Single Network Installations	766
24.21	Security Keys	767
24.22	Key Server.....	768
25	REFERENCES	772
	ANNEX A - PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (NORMATIVE)	775
	ANNEX B - GUIDE TO SPECIFYING BACnet DEVICES (INFORMATIVE)	778
	ANNEX C - Removed	779
	ANNEX D - Removed.....	780
	ANNEX E - EXAMPLES OF BACnet APPLICATION SERVICES (INFORMATIVE).....	781
	E.1 Alarm and Event Services	781
	E.2 File Access Services.....	785
	E.3 Object Access Services.....	787
	E.4 Remote Device Management Services	793
	E.5 Virtual Terminal Services.....	796
	ANNEX F - EXAMPLES OF APDU ENCODING (INFORMATIVE)	798
	F.1 Example Encodings for Alarm and Event Services	798

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

Contents

F.2 Example Encodings for File Access Services	807
F.3 Example Encodings for Object Access Services	809
F.4 Example Encodings for Remote Device Management Services	819
F.5 Example Encodings for Virtual Terminal Services	824
ANNEX G - CALCULATION OF CRC (INFORMATIVE)	827
G.1 Calculation of the Header CRC	827
G.2 Calculation of the Data CRC	833
ANNEX H - COMBINING BACnet NETWORKS WITH NON-BACnet NETWORKS (NORMATIVE)	838
H.1 Mapping Non-BACnet Networks onto BACnet Routers	838
H.2 Multiple "Virtual" BACnet Devices in a Single Physical Device	838
H.3 Using BACnet with the DARPA Internet Protocols	838
H.4 Using BACnet with the IPX Protocol	839
H.5 Using BACnet with EIB/KNX	841
H.6 Using BACnet with the BACnet/WS Web Services Interface (Annex N)	854
H.7 Virtual MAC Addressing	856
ANNEX I - COMMANDABLE PROPERTIES WITH MINIMUM ON AND OFF TIMES (INFORMATIVE)	857
ANNEX J - BACnet/IP (NORMATIVE)	859
J.1 General	859
J.2 BACnet Virtual Link Layer	859
J.3 BACnet/IP Directed Messages	863
J.4 BACnet/IP Broadcast Messages	863
J.5 Addition of Foreign B/IP Devices to an Existing B/IP Network	865
J.6 Routing Between B/IP and non-B/IP BACnet Networks	867
J.7 Routing Between Two B/IP BACnet Networks	868
J.8 Use of IP Multicast within BACnet/IP	873
J.9 Sources for Internet Information	874
ANNEX K - BACnet INTEROPERABILITY BUILDING BLOCKS (BIBBs) (NORMATIVE)	875
K.1 Data Sharing BIBBs	875
K.2 Alarm and Event Management BIBBs	882
K.3 Scheduling BIBBs	890
K.4 Trending BIBBs	893
K.5 Device and Network Management BIBBs	897
ANNEX L - DESCRIPTIONS AND PROFILES OF STANDARDIZED BACnet DEVICES (NORMATIVE)	905
L.1 Operator Interfaces	905
L.2 BACnet Building Controller (B-BC)	907
L.3 BACnet Advanced Application Controller (B-AAC)	907
L.4 BACnet Application Specific Controller (B-ASC)	908
L.5 BACnet Smart Actuator (B-SA)	908
L.6 BACnet Smart Sensor (B-SS)	909
L.7 Profiles of the Standard BACnet Devices	910
ANNEX M - GUIDE TO EVENT NOTIFICATION PRIORITY ASSIGNMENTS (INFORMATIVE)	911
ANNEX N - BACnet/WS WEB SERVICES INTERFACE (NORMATIVE)	915
N.1 Data Model	915
N.2 Paths	916
N.3 Normalized Points	916
N.4 Reference Nodes	917
N.5 Localization	917
N.6 Security	917
N.7 Sessions	918
N.8 Attributes	918
N.9 Standard Nodes	924
N.10 Encodings	925
N.11 Service Options	926
N.12 Services	929
N.13 Errors	947
N.14 Extending BACnet/WS	948
ANNEX O - BACnet OVER ZigBee AS A DATA LINK LAYER (NORMATIVE)	949

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

Contents

O.1 General.....	949
O.2 ZigBee Overview	949
O.3 Definitions	950
O.4 Unicast Addressing	950
O.5 Broadcast Addressing	950
O.6 BACnet/ZigBee Data Link Layer (BZLL).....	951
O.7 Maximum Payload Size	954
O.8 Vendor Specific Commands	954
ANNEX P - BACnet ENCODING OF STANDARD AUTHENTICATION FACTOR FORMATS (NORMATIVE)	955
ANNEX Q - XML DATA FORMATS (NORMATIVE).....	962
Q.1 Introduction.....	962
Q.2 Document Structure	965
Q.3 Expressing BACnet Datatypes in XML	966
Q.4 Expressing BACnet Objects and Properties in XML	1000
Q.5 Definitions, Types, Instances, and Inheritance	1000
Q.7 Extensibility	1007
ANNEX R - MAPPING NETWORK LAYER ERRORS (NORMATIVE)	1010
ANNEX S - EXAMPLES OF SECURE BACnet MESSAGES (INFORMATIVE).....	1012
HISTORY OF REVISIONS	1027

NOTE

Approved addenda, errata, or interpretations for this standard can be downloaded free of charge from the ASHRAE Web site at www.ashrae.org/technology.

© 2012 ASHRAE

1791 Tullie Circle NE · Atlanta, GA 30329 · www.ashrae.org · All rights reserved.

ASHRAE is a registered trademark of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

ANSI is a registered trademark of the American National Standards Institute.

BACnet is a registered trademark in the U.S. Patent & Trademark Office, owned by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers, Inc.

FOREWORD

BACnet, the ASHRAE building automation and control networking protocol, has been designed specifically to meet the communication needs of building automation and control systems for applications such as heating, ventilating, and air-conditioning control, lighting control, access control, and fire detection systems. The BACnet protocol provides mechanisms by which computerized equipment of arbitrary function may exchange information, regardless of the particular building service it performs. As a result, the BACnet protocol may be used by head-end computers, general-purpose direct digital controllers, and application specific or unitary controllers with equal effect.

The motivation for this Standard was the widespread desire of building owners and operators for "interoperability," the ability to integrate equipment from different vendors into a coherent automation and control system - and to do so competitively. To accomplish this, the Standard Project Committee (SPC) solicited and received input from dozens of interested firms and individuals; reviewed all relevant national and international data communications standards, whether de facto or the result of committee activity; and spent countless hours in debate and discussion of the pros and cons of each element of the protocol.

What has emerged from the committee deliberations is a network protocol model with these principal characteristics:

(a) All network devices (except MS/TP slaves) are peers, but certain peers may have greater privileges and responsibilities than others.

(b) Each network device is modeled as a collection of network-accessible, named entities called "objects." Each object is characterized by a set of attributes or "properties." While this Standard prescribes the most widely applicable object types and their properties, implementors are free to create additional object types if desired. Because the object model can be easily extended, it provides a way for BACnet to evolve in a backward compatible manner as the technology and building needs change.

(c) Communication is accomplished by reading and writing the properties of particular objects and by the mutually acceptable execution of other protocol "services." While this Standard prescribes a comprehensive set of services, mechanisms are also provided for implementors to create additional services if desired.

(d) Because of this Standard's adherence to the ISO concept of a "layered" communication architecture, the same messages may be exchanged using various network access methods and physical media. This means that BACnet networks may be configured to meet a range of speed and throughput requirements with commensurately varying cost. Multiple BACnet networks can be interconnected within the same system forming an internetwork of arbitrarily large size. This flexibility also provides a way for BACnet to embrace new networking technologies as they are developed.

BACnet was designed to gracefully improve and evolve as both computer technology and demands of building automation systems change. Upon its original publication in 1995, a Standing Standards Project Committee was formed to deliberate enhancements to the protocol under ASHRAE rules for "continuous maintenance." Much has happened since the BACnet standard was first promulgated. BACnet has been translated into Chinese, Japanese, and Korean, and embraced across the globe. BACnet devices have been designed, built and deployed on all seven continents. Suggestions for enhancements and improvements have been continually received, deliberated, and, ultimately, subjected to the same consensus process that produced the original standard. This publication is the result of those deliberations and brings together all of the corrections, refinements, and improvements that have been adopted.

Among the features that have been added to BACnet are: increased capabilities to interconnect systems across wide area networks using Internet Protocols, new objects and services to support fire detection and other life safety applications, capabilities to backup and restore devices, standard ways to collect trend data, new tools to make specifying BACnet systems easier, a mechanism for making interoperable extensions to the standard visible, and many others. The successful addition of these features demonstrates that the concept of a protocol deliberately crafted to permit extension of its capabilities over time as technology and needs change is viable and sound.

All communication protocols are, in the end, a collection of arbitrary solutions to the problems of information exchange and all are subject to change as time and technology advance. BACnet is no exception. Still, it is the hope of those who have contributed their time, energies, and talents to this work that BACnet will help to fulfill, in the area of building automation and control, the promise of the information age for the public good!

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

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).

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

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.

alarm-acknowledgment: the process of indicating that a human operator has seen and responded to an event notification.

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*.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

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*.

blink-warn: in lighting control, typically a method of notifying room occupants of an impending automated command to turn off the lights whereby the lights may be blinked, once or multiple times, or an audible signal is generated. After the warning occurs, the room lights are held on for a grace period to allow occupants to either safely leave the room or to initiate a request to keep the room lights on. Also known as "flick warn" or "flash warn."

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*.

configurable: a property, setting, or value in a device is configurable if it can be changed via BACnet services or some other method. A property, setting, or value that is one-time writable or not changeable in situ is not considered to be configurable.

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.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

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.

event algorithm: the rules that determine when an event-initiating object changes between normal and offnormal states. The event algorithm has no impact on an event-initiating object's transition to or from fault.

event-initiating object: an object that is configured to monitor its event state and can report changes in its event state.

event-notification-distribution: the process that a notification-server performs in the determination of notification-clients and in the sending of notifications to notification-clients when an event-initiating object changes the event or acknowledgment state.

event notification message: a ConfirmedEventNotification or UnconfirmedEventNotification service request used to indicate a change in the event or acknowledgment state of an event-initiating object.

event-state-detection: the process of executing an event-initiating object's event algorithm and monitoring the object's Reliability property to detect changes in the object's event state.

event-summarization: the querying of event-initiating objects in a device through one of the event summarization services to determine those that meet specific event state or reporting conditions.

fading: the gradual increase or decrease of the actual output from one setting to another over a fixed period of time.

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.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

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*.

notification-client: a BACnet device that receives and processes event notification messages.

notification-server: a BACnet device that contains event-initiating objects and performs event notification distribution.

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.

ramping: the gradual increase or decrease of the actual output from one setting to another at a fixed rate of change.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

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

reliability-evaluation: the process by which an object determines its reliability and thus the value to set into its Reliability property.

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.

stepping: the increase or decrease of an output value in discrete steps.

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.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.
3. DEFINITIONS

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
BVLCI	BACnet virtual link control information
BVLL	BACnet virtual link layer
C	conditional
C(=)	conditional (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)
CNF	confirm primitive
COV	change of value
CRC	cyclic redundancy check
D' '	denotes that decimal notation is used between the single quotes
DA	local destination MAC layer address
DADR	ultimate destination MAC layer address
DER	data expecting reply
DES	Data Encryption Standard (FIPS 46-1)
DESFire	Data Encryption Standard Fast, Innovative, Reliable and Secure
DID	ARCNET destination MAC address
DLEN	1-octet length of ultimate destination MAC layer address
DNEN	2-octet ultimate destination network number

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

DSAP	LLC destination service access point (X'82' for BACnet)
EIB	European Installation Bus
EIBA	European Installation Bus Association
EXEC	capable of executing a service request
FDT	foreign device table
ICI	interface control information
IL	ARCNET information length field
IND	indication primitive
INF	"Infinity", a unique binary pattern representing positive infinity (see ANSI/IEEE 754-1985)
-INF	"Negative infinity", a unique binary pattern representing negative infinity (see ANSI/IEEE 754-1985)
IEEE	Institute of Electrical and Electronics Engineers
INIT	capable of initiating a service request
IP	Internet Protocol - RFC 791
ISO	International Organization for Standardization
KNX	The Konnex System Specification: EIB is the core protocol of the Konnex standard. The Konnex System Specification reflects the current status for EIB.
L	data link (prefix)
LAN	local area network
LLC	logical link control (ISO 8802-2)
LPCI	link protocol control information
LPDU	link protocol data unit
LRC	Longitudinal Redundancy Check
LSAP	link service access point (X'82' for BACnet)
LSDU	link service data unit
M	mandatory
M(=)	mandatory (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)
MA	medium access (prefix)
MAC	medium access control
MPCI	MAC protocol control information
MPDU	MAC layer protocol data unit
MSDU	MAC service data unit
MS/TP	master-slave/token-passing
N	network layer (prefix)
NaN	"Not a Number", a unique binary pattern representing an invalid number (see ANSI/IEEE 754-1985)
NAT	Network Address Translation - RFC 2663
NP	network priority
NPCI	network protocol control information
NPDU	network layer protocol data unit
NRZ	non-return to zero
NSAP	network service access point
NSDU	network service data unit
O	indicates that support of a property is optional
OSI	open systems interconnection
P	physical layer (prefix)
PAC	ARCNET data packet header octet
PCI	protocol control information
PDU	protocol data unit
PICS	protocol implementation conformance statement
PK	Private Key
PPCI	physical layer protocol control information
PPDU	physical protocol data unit
PPP	Point-To-Point protocol - RFC 1661
PSDU	physical service data unit
PTP	point-to-point
R	indicates that a property shall be supported and readable using BACnet services

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

3. DEFINITIONS

REQ	request primitive
RFC	request for comment
RSP	response primitive
S	selection
S(=)	selection (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)
SA	local network source MAC layer address
SAP	service access point
SC	ARCNET system code (X'CD' for BACnet)
SDU	service data unit
SIA	Security Industry Association
SID	ARCNET source MAC address
SK	Session Key
SLEN	1-octet length of original source MAC layer address
SLIP	Serial Line Internet Protocol -RFC 1055
SNET	2-octet original source network number
SPC	standard project committee
SSAP	LLC source service access point (X'82' for BACnet)
TSM	transaction state machine
U	user option
U(=)	user option (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)
UART	universal asynchronous receiver/transmitter
UDP	User Datagram Protocol - RFC 768
UTC	Universal Time Coordinated
VT	virtual terminal
W	indicates that a property shall be supported, readable, and writable using BACnet services
X'	denotes that hexadecimal notation is used between the single quotes
XID	eXchange IDentification (ISO 8802-2)

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

4. BACnet PROTOCOL ARCHITECTURE

4 BACnet PROTOCOL ARCHITECTURE

The Open System Interconnection (OSI) - Basic Reference Model (ISO 7498) is an international standard that defines a model for developing multi-vendor computer communication protocol standards. The OSI model addresses the general problem of computer-to-computer communication and breaks this very complex problem into seven smaller, more manageable sub-problems, each of which concerns itself with a specific communication function. Each of these sub-problems forms a "layer" in the protocol architecture.

The seven layers are arranged in a hierarchical fashion as shown in Figure 4-1. A given layer provides services to the layers above and relies on services provided to it by the layers below. Each layer can be thought of as a black box with carefully defined interfaces on the top and bottom. An application process connects to the OSI application layer and communicates with a second, remote application process. This communication appears to take place between the two processes as if they were connected directly through their application layer interfaces. Minimal knowledge or understanding of the other layers is required. In a similar manner, each layer of the protocol relies on lower layers to provide communication services and establishes a virtual peer-to-peer communication with its companion layer on the other system. The only real connection takes place at the physical layer.

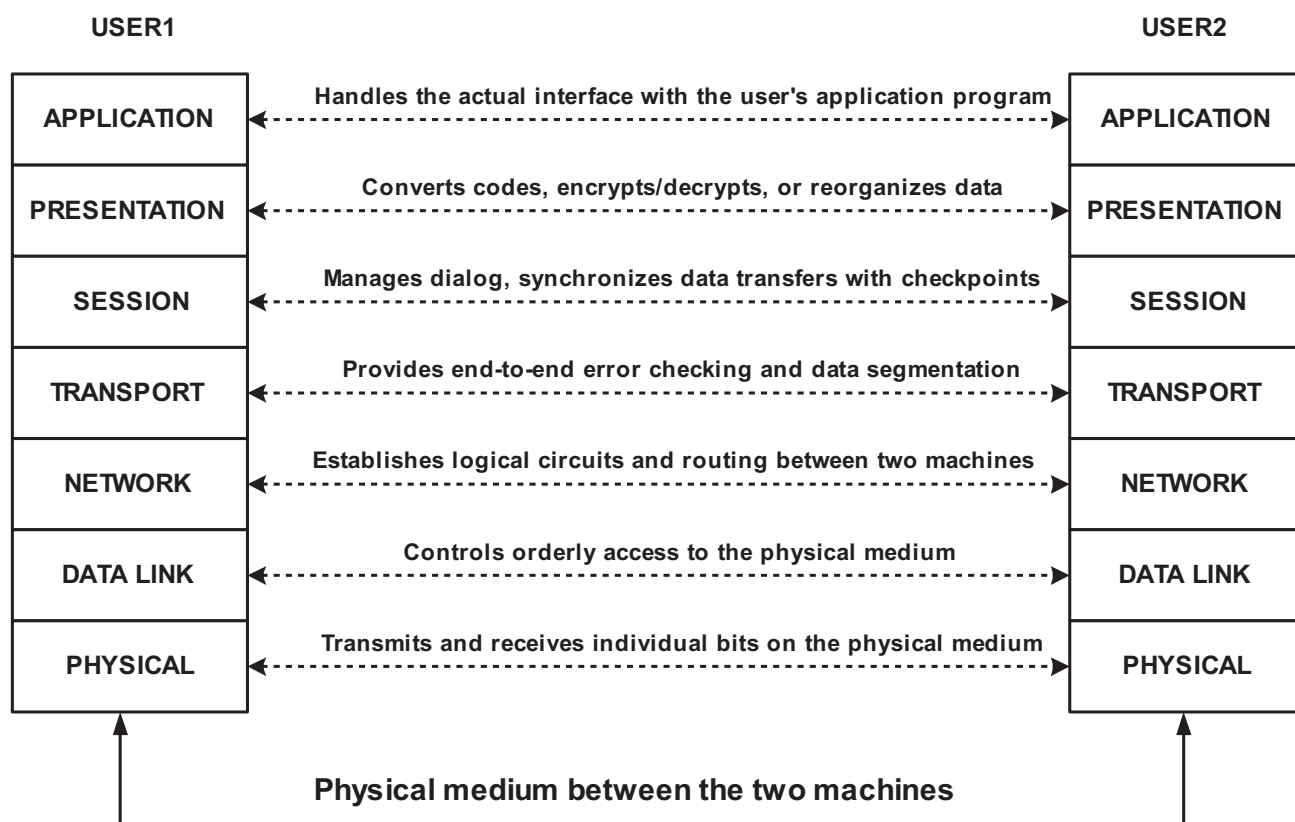


Figure 4-1. The ISO Open Systems Interconnection Basic Reference Model.

The OSI model addresses computer-to-computer communication from a very general perspective. It was designed to deal with the problems associated with computers in large, complex networks communicating with other computers in networks anywhere in the world. In this environment, computers can be separated by long distances and the messages might pass through several intermediate points, each of which may have to make routing decisions or perform some type of translation. Complex synchronization and error recovery schemes may also be needed.

The cost of implementing such a protocol today is prohibitively high for most building automation applications and is not generally required. Nevertheless, the OSI model is a good one to use for a building automation protocol if consideration is given to including only the OSI functionality that is actually needed, thereby collapsing the seven-layer architecture. In a

collapsed architecture, only selected layers of the OSI model are included. The other layers are effectively null, thus reducing message length and communication processing overhead. Such a collapsed architecture permits the building automation industry to take advantage of lower cost, mass-produced processor and local area network technologies such as have been developed for the process control and office automation industries. The use of readily available, widespread technologies, such as Ethernet,¹ ARCNET,² and LonTalk,³ will lower the cost, increase performance, and open new doors to system integration.

4.1 The BACnet Collapsed Architecture

BACnet is based on a four-layer collapsed architecture that corresponds to the physical, data link, network, and application layers of the OSI model as shown in Figure 4-2. The application layer and a simple network layer are defined in the BACnet standard. BACnet provides seven options that correspond to the OSI data link and physical layers. Option 1 is the logical link control (LLC) protocol defined by ISO 8802-2 Type 1, combined with the ISO 8802-3 medium access control (MAC) and physical layer protocol. ISO 8802-2 Type 1 provides unacknowledged connectionless service only. ISO 8802-3 is the international standard version of the well-known "Ethernet" protocol. Option 2 is the ISO 8802-2 Type 1 protocol combined with ARCNET (ATA 878.1). Option 3 is a Master-Slave/Token-Passing (MS/TP) protocol designed specifically for building automation and control devices as part of the BACnet standard. The MS/TP protocol provides an interface to the network layer that looks like the ISO 8802-2 Type 1 protocol and controls access to an EIA-485 physical layer. Option 4, the Point-To-Point protocol, provides mechanisms for hardwired or dial-up serial, asynchronous communication. Option 5 is the LonTalk protocol. Option 6, BACnet/IP, permits BACnet devices to use standard Internet Protocols (UDP and IP) as a virtual data link layer. Option 7, ZigBee, provides a wireless datalink. Collectively these options provide a master/slave MAC, deterministic token-passing MAC, high-speed contention MAC, dial-up access, star and bus topologies, and a choice of twisted-pair, coax, or fiber optic media, in addition to wireless connectivity. The details of these options are described in Clauses 7 through 11 Annex J, and Annex O.

A four-layer collapsed architecture was chosen after careful consideration of the particular features and requirements of BAC networks, including a constraint that protocol overhead needed to be as small as possible. The reasoning behind the selection of the physical, data link, network, and application layers for inclusion in the BACnet architecture is outlined in this subclause.

What layers are required for the proper operation of a BAC network? BAC networks function as local area networks, either physically, as with MS/TP, or logically, as with BACnet/IP. This is true even though in some applications it is necessary to exchange information with devices in a building that is very far away. This long-distance communication is done through the telephone networks or across the Internet. The routing, relaying, and guaranteed delivery issues are handled by the telephone and Internet systems and can be considered external to the BAC network. BAC devices are static. They don't move from place to place and the functions that they are asked to perform do not change in the sense that a manufacturing device may make one kind of part today and some very different part tomorrow. These are among the features of BAC networks that can be used to evaluate the appropriateness of the layers in the OSI model.

BACnet Layers						Equivalent OSI Layers
BACnet Application Layer						Application
BACnet Network Layer						Network
ISO 8802-2 (IEEE 802.2) Type 1	MS/TP	PTP	LonTalk	BVLL	BZLL	Data Link
ISO 8802-3 (IEEE 802.3)	ARCNET	EIA-485		UDP/IP	ZigBee	Physical

Figure 4-2. BACnet collapsed architecture.

¹ Ethernet is a registered trademark of Digital Equipment Corporation, Intel, and Xerox and is the basis for international standard ISO 8802-3.

² ARCNET is a registered trademark of Datapoint Corporation.

³ LonTalk is a registered trademark of Echelon Corporation.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

4. BACnet PROTOCOL ARCHITECTURE

The physical layer provides a means of connecting the devices and transmitting the electronic signals that convey the data. Clearly the physical layer is needed in a BAC protocol.

The data link layer organizes the data into frames or packets, regulates access to the medium, provides addressing, and handles some error recovery and flow control. These are all functions that are required in a BAC protocol. The conclusion is that the data link layer is needed.

Functions provided by the network layer include translation of global addresses to local addresses, routing messages through one or more networks, accommodating differences in network types and in the maximum message size permitted by those networks, sequencing, flow control, error control, and multiplexing. BACnet is designed so that there is only one logical path between devices, thus eliminating the need for optimal path routing algorithms. A network is made up of one or more physical segments connected by repeaters or bridges but with a single local address space. In the case of a single network, most network layer functions are either unnecessary or duplicate data link layer functions. For some BACnet systems, however, the network layer is a necessity. This is the case when two or more networks in a BACnet internet use different MAC layer options. When this occurs, there is a need to recognize the difference between local and global addresses and to route messages to the appropriate networks. BACnet provides this limited network layer capability by defining a network layer header that contains the necessary addressing and control information.

The transport layer is responsible for guaranteeing end-to-end delivery of messages, segmentation, sequence control, flow control, and error recovery. Most of the functions of the transport layer are similar to functions in the data link layer, though different in scope. The scope of transport layer services is end-to-end whereas the scope of data link services is point-to-point across a single network. Since BACnet supports configurations with multiple networks, the protocol must provide the end-to-end services of the transport layer. Guaranteed end-to-end delivery and error recovery are provided in the BACnet application layer via message retry and timeout capabilities. Message segmentation and end-to-end flow control is required for buffer and processor resource management. This is because potentially large amounts of information may be returned for even simple BACnet requests. These functions are provided in the BACnet application layer. Last, sequence control is required in order to properly reassemble segmented messages. This is provided in the BACnet application layer within the segmentation procedure. Since BACnet is based on a connectionless communication model, the scope of the required services is limited enough to justify implementing these at a higher layer, thus saving the communication overhead of a separate transport layer.

The session layer is used to establish and manage long dialogues between communicating partners. Session layer functions include establishing synchronization checkpoints and resetting to previous checkpoints in the event of error conditions to avoid restarting an exchange from the beginning. Most communications in a BAC network are very brief. For example, reading or writing one or a few values, notifying a device about an alarm or event, or changing a setpoint. Occasionally longer exchanges take place, such as uploading or downloading a device. The few times when the services of this layer would be helpful do not justify the additional overhead that would be imposed on the vast majority of transactions, which are very brief and do not need them.

The presentation layer provides a way for communicating partners to negotiate the transfer syntax that will be used to conduct the communication. This transfer syntax is a translation from the abstract user view of data at the application layer to sequences of octets treated as data at the lower layers. If only one transfer syntax is permitted, then the presentation layer function reduces to an encoding scheme for representing the application data. BACnet defines such a fixed encoding scheme and includes it in the application layer, making an explicit presentation layer unnecessary.

The application layer of the protocol provides the communication services required by the applications to perform their functions, in this case monitoring and control of HVAC&R and other building systems. Clearly an application layer is needed in the protocol.

In summary:

- (a) The resource and overhead costs for implementing a full OSI seven-layer architecture make it impractical for current building automation devices.
- (b) Following the OSI model offers advantages in terms of adopting existing computer networking technology. This can result in cost savings and make integration with other computer network systems easier.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

4. BACnet PROTOCOL ARCHITECTURE

- (c) The expectations and environment of building automation systems permit simplification of the OSI model by eliminating the functionality of some of the layers.
- (d) A collapsed architecture made up of the physical, data link, network, and application layers is the optimum solution for today's building automation systems.

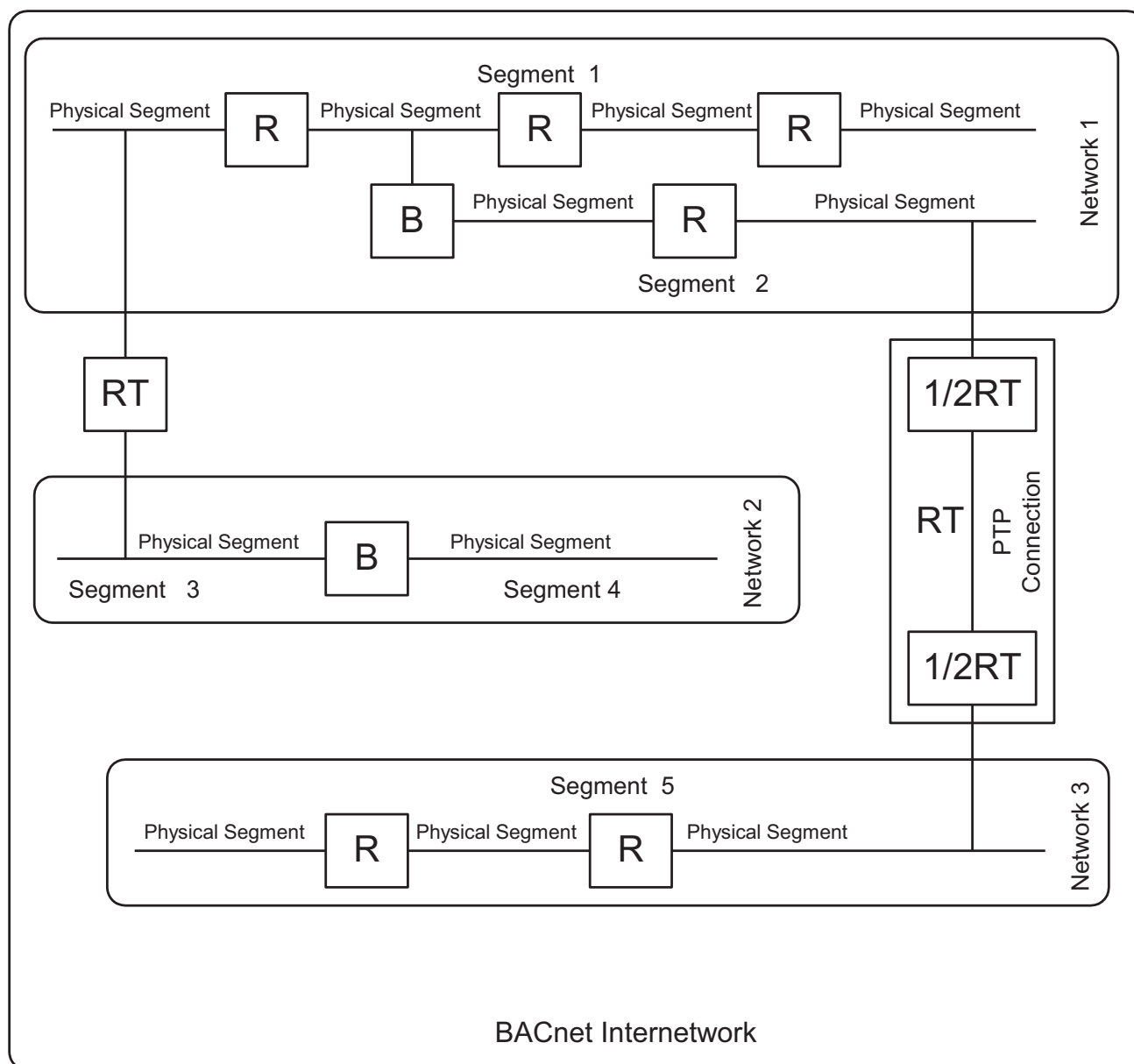
4.2 BACnet Network Topology

In the interest of application flexibility, BACnet does not prescribe a rigid network topology. Rather, BACnet devices are physically connected to one of five types of local area networks (LANs) or via dedicated or dial-up serial, asynchronous lines. These networks may then be further interconnected by BACnet routers as described in Clause 6.

In terms of LAN topology, each BACnet device is attached to an electrical medium or *physical segment*. A BACnet *segment* consists of one or more physical segments connected at the physical layer by *repeaters*. A BACnet *network* consists of one or more segments interconnected by *bridges*, devices that connect the segments at the physical and data link layers and may perform message filtering based upon MAC addresses; a network forms a single MAC address domain. Multiple networks, possibly employing different LAN technologies, may be interconnected by BACnet *routers* to form a BACnet *internetwork*. In a BACnet internetwork, there exists exactly one message path between any two nodes. These concepts are shown graphically in Figure 4-3.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

4. BACnet PROTOCOL ARCHITECTURE



B = Bridge
 R = Repeater
 RT = Router
 1/2RT = Half Router

Figure 4-3. A BACnet internetwork illustrating the concepts of Physical Segments, Repeaters, Segments, Bridges, Networks, Half Routers, and Routers.

4.3 Security

The principal security threats to BACnet systems are people who, intentionally or by accident, modify a device's configuration or control parameters. Problems due to an errant computer are outside the realm of security considerations. One important place for security measures is the operator-machine interface. Since the operator-machine interface is not part of the communication protocol, vendors are free to include password protection, audit trails, or other controls to this interface as needed. In addition, write access to any properties that are not explicitly required to be "writable" by this standard may be restricted to modifications made only in virtual terminal mode or be prohibited entirely. This permits vendors to protect key properties with a security mechanism that is as sophisticated as they consider appropriate. BACnet also defines services that can be used to provide peer entity, data origin, and operator authentication. See Clause 24.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

5. THE APPLICATION LAYER

5 THE APPLICATION LAYER

5.1 The Application Layer Model

This clause presents a model of the BACnet application layer. The purpose of the model is to describe and illustrate the interaction between the application layer and application programs, the relationship between the application layer and lower layers in the protocol stack, and the peer-to-peer interactions with a remote application layer. This model is not an implementation specification.

An Application Process is that functionality within a system that performs the information processing required for a particular application. All parts of the Application Process outside the Application Layer, (i.e., those that do not concern the communication function) are outside the scope of BACnet. The part of the Application Process that is within the Application Layer is called the Application Entity. In other words, an Application Entity is that part of the Application Process related to the BACnet communication function. An application program interacts with the Application Entity through the Application Program Interface (API). This interface is not defined in BACnet, but it would probably be a function, procedure, or subroutine call in an actual implementation. These concepts are illustrated in Figure 5-1. The shaded region indicates the portion of the Application Process that is within the BACnet Application Layer.

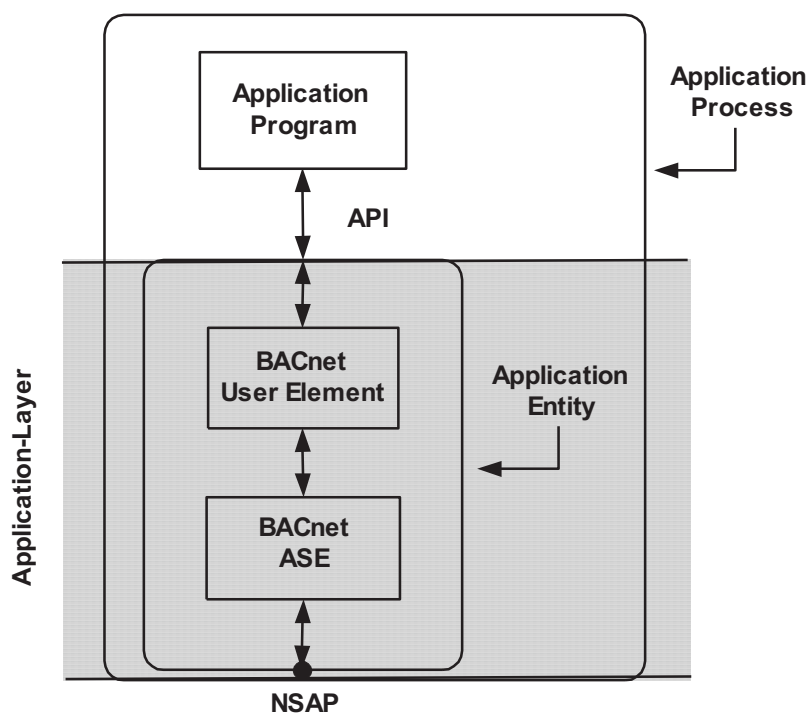


Figure 5-1. Model of a BACnet Application Process.

The Application Entity is itself made up of two parts: the BACnet User Element and the BACnet Application Service Element (ASE). The BACnet ASE represents the set of functions or application services specified in Clauses 13 through 17 and Clause 24. The BACnet User Element carries out several functions in addition to supporting the local API. It represents the implementation of the "service procedure" portion of each application service. It is responsible for maintaining information about the context of a transaction, including generating invoke IDs and remembering which invoke ID goes with which application service request (response) to (from) which device. It is also responsible for maintaining the time-out counters that are required for the retrying of a transmission. The BACnet User Element also presides over the mapping of a device's activities into BACnet objects.

Information exchanged between two peer application processes is represented in BACnet as an exchange of abstract service primitives, following the ISO conventions contained in the OSI technical report on service conventions, ISO TR 8509. These primitives are used to convey service-specific parameters that are defined in Clauses 13 through 17 and Clause 24. Four

service primitives are defined: request, indication, response, and confirm. The information contained in the primitives is conveyed using a variety of protocol data units (PDUs) defined in this standard. In order to make clear which BACnet PDU is being used, the notation will be as follows:

CONF_SERV.request	CONF_SERV.indication	CONF_SERV.response	CONF_SERV.confirm
UNCONF_SERV.request	UNCONF_SERV.indication		
SEGMENT_ACK.request	SEGMENT_ACK.indication		
REJECT.request	REJECT.indication		
ABORT.request	ABORT.indication		
	SEC_ERR.indication		

The designation CONF_SERV indicates that BACnet confirmed service PDUs are being used. Similarly, the designations UNCONF_SERV, SEGMENT_ACK, ERROR, REJECT, and ABORT indicate that unconfirmed service PDUs, segment acknowledge PDUs, error PDUs, reject PDUs, and abort PDUs, respectively, are being used. The designation SEC_ERR indicates that an error occurred in the BACnet security layer and is being indicated up to the BACnet application program. The format of a SEC_ERR.indication is a local matter.

An application program that needs to communicate with a remote application process accesses the local BACnet User Element through the API. Some of the API parameters, such as the identity (address) of the device to which the service request is to be sent and protocol control information, is passed directly down to the network or data link layers. The remainder of the parameters make up an application service primitive that is passed from the BACnet User Element to the BACnet ASE. Conceptually, the application service primitive results in the generation of an APDU that becomes the data portion of a network service primitive, which is passed to the network layer through the Network Service Access Point (NSAP). Similarly this request passes down through the lower layers of the protocol stack in the local device. This process is illustrated in Figure 5-2. The message is then transmitted to the remote device, where it is passed up through the protocol stack in the remote device, eventually appearing as an indication primitive passed from the remote BACnet ASE to the remote BACnet User Element. The response from the remote device, if any, returns to the initiator of the service in a similar fashion (see Clause 5.5).

In addition to the service primitives and the service specific parameters, the application entity exchanges interface control information (ICI) parameters with the application program via the API. The content of the ICI is dependent upon the service primitive type. The ICI parameters received by the application entity provide the information that is passed on to the lower layers (as ICI across layer interfaces) to help them construct their PDUs. The ICI parameters that are provided by the application entity to the application programs contain information recovered by the lower layers from their respective PDUs.

The following ICI parameters are exchanged with the various service primitives across an API:

'destination_address' (DA): the address of the device(s) intended to receive the service primitive. Its format (device name, network address, etc.) is a local matter. This address may also be a multicast, local broadcast or global broadcast type.

'source_address' (SA): the address of the device from which the service primitive was received. Its format (device name, network address, etc.) is a local matter.

'network_priority' (NP): a four-level network priority parameter described in 6.2.2.

'data_expecting_reply' (DER): a Boolean parameter that indicates whether (TRUE) or not (FALSE) a reply service primitive is expected for the service being issued.

'security_parameters' (SEC): The optional security parameters for the request to send, or from the received request. It indicates the level of security (Key Id, Plain/Signed/Encrypted, User Authentication data, End-To-End, etc.) and its format is a local matter.

BACnet Protocol Stack and Data Flow

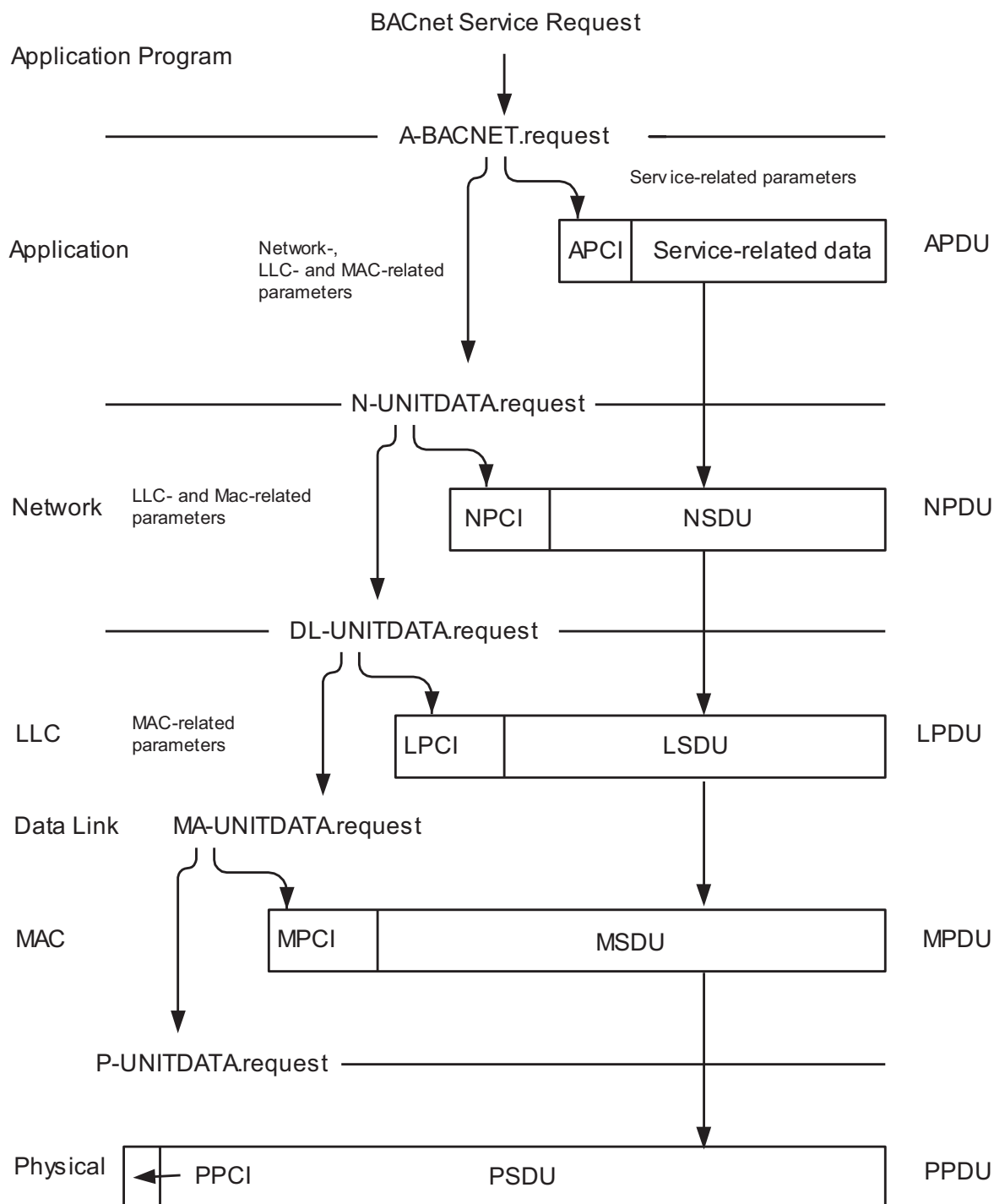


Figure 5-2. BACnet protocol stack and data flow.

Table 5-1 describes the applicability of the ICI parameters to the service primitives.

Table 5-1. Applicability of ICI Parameters for Abstract Service Primitives

Service Primitive	DA	SA	NP	DER	SEC
CONF_SERV.request	Yes	No	Yes	Yes	Yes
CONF_SERV.indication	Yes	Yes	Yes	Yes	Yes
CONF_SERV.response	Yes	No	Yes	Yes	Yes
CONF_SERV.confirm	Yes	Yes	Yes	No	Yes
UNCONF_SERV.request	Yes	No	Yes	No	Yes
UNCONF_SERV.indication	Yes	Yes	Yes	No	Yes
REJECT.request	Yes	No	Yes	No	Yes
REJECT.indication	Yes	Yes	Yes	No	Yes
SEGMENT_ACK.request	Yes	No	Yes	No	Yes
SEGMENT_ACK.indication	Yes	Yes	Yes	No	Yes
ABORT.request	Yes	No	Yes	No	Yes
ABORT.indication	Yes	Yes	Yes	No	Yes
SEC_ERR.indication	Yes	Yes	No	No	Yes

A "BACnetDevice" is any device, real or virtual, that supports digital communication using the BACnet protocol. Each BACnet Device contains exactly one Device object, as defined in 12.11. A BACnet Device is uniquely located by an NSAP, which consists of a network number and a MAC address.

In most cases, a physical device will implement a single BACnet Device. It is possible, however, that a single physical device may implement a number of "virtual" BACnet Devices. This is described in Annex H.

5.1.1 Confirmed Application Services

BACnet defines confirmed application services based on a client and server communication model. A client requests service from a server via a particular service request instance. The server provides service to a client and responds to the request. This relationship is illustrated in Figure 5-3. The BACnet-user that assumes the role of a client is called the "requesting BACnet-user" and the BACnet-user that assumes the role of the server is called the "responding BACnet-user."

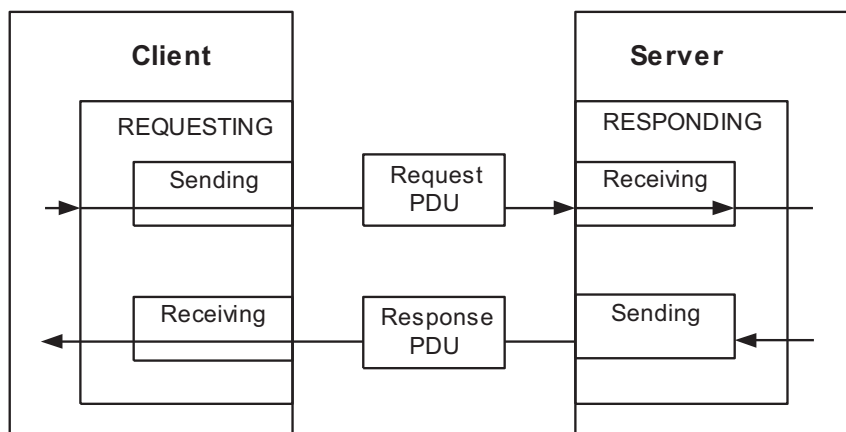


Figure 5-3. Relationship of a client and server.

Courtesy copy ONLY for staff/committees responsible for this document. © ASHRAE (www.ashrae.org). Per international copyright law, additional reproduction, distribution, or transmission in either print or digital form is not permitted without ASHRAE's prior written permission.

5. THE APPLICATION LAYER

A requesting BACnet-user issues a CONF_SERV.request primitive, which causes a request PDU to be sent. When a response PDU arrives, the requesting BACnet-user receives a CONF_SERV.confirm primitive. When a request PDU arrives, the responding BACnet-user receives a CONF_SERV.indication primitive. The responding BACnet-user issues a CONF_SERV.response primitive, which causes a response PDU to be sent. Thus, the requesting BACnet-user and the responding BACnet-user play a role in both sending and receiving PDUs. The term "sending BACnet-user" applies to a BACnet user that initiates the sending of a PDU. The term "receiving BACnet-user" applies to a BACnet-user that receives an indication that a PDU has arrived.

5.1.2 Unconfirmed Application Services

The client and server model, and the terms "requesting BACnet-user" and "responding BACnet-user," do not apply to unconfirmed services. The terms "sending BACnet-user" and "receiving BACnet-user" do apply, however, and they are used to define the service procedure for unconfirmed services.

In some cases, errors will be encountered when sending unconfirmed requests. While the standard does not provide a mechanism for reporting such errors to the application program, it is acceptable for an implementation to provide such a mechanism, if desired.

5.2 Segmentation of BACnet Messages

To provide for messages that are longer than the maximum length supported by a communications network, or by the sending or receiving device, BACnet provides a method to perform application layer segmentation. In BACnet, only Confirmed-Request and ComplexACK messages may be segmented. Segmentation is an optional feature of BACnet.

5.2.1 Message Segmentation Rules

This subclause prescribes rules for dividing a message into segments.

5.2.1.1 Rules for Segmenting APDU Data Streams

Each BACnet message is encoded into a sequence of tags and values according to the relevant ASN.1 definitions in Clause 21 and the encoding rules of Clause 20. The following rules apply to segmenting this data stream:

- (a) If possible, an entire message shall be sent in a single APDU.
- (b) If an entire message cannot be sent in a single APDU, the message shall be segmented into the minimum number of APDUs possible.
- (c) Messages shall be segmented only at octet boundaries.

5.2.1.2 Maximum APDU Length

The maximum length of a BACnet APDU shall be the smallest of

- (a) the maximum APDU size transmittable by a device, which may be restricted by local buffer limitations and is a local matter;
- (b) the maximum APDU size conveyable by the internetwork to the remote device, which is constrained by the maximum NPDU length permitted by the data links used by the local, remote, and any intervening networks, as specified in Clause 6;
- (c) the maximum APDU size accepted by the remote peer device, which must be at least 50 octets.

If the sending device is the requesting BACnet-user, i.e., the APDU to be sent is a BACnet-Confirmed-Request-PDU or a BACnet-Unconfirmed-Request-PDU, then the maximum APDU size accepted by the remote peer is specified by the Max_APDU_Length_Accepted property of the remote peer's Device object. The value of this property may be read using the read property services described in Clause 15 or the value may be obtained from the 'Max APDU Length Accepted' parameter of an I-Am service request received from the remote device. The remote peer may be solicited to transmit an I-Am service request by sending it a Who-Is service request, as described in 16.9