International Standard

ISO 16484-5

Eighth edition
2026-08

Building automation and control systems (BACS) —

Part 5: Data communication protocol

Systèmes d'automatisation et de gestion technique du bâtiment (BACS) —

Partie 5: Protocole de communication de données

Reference number
ISO 16484-5:2026(en)

© ISO 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

CONTENTS

Foreword xi
FOREWORD xii
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 8
4 BACnet PROTOCOL ARCHITECTURE 12
4.1 The BACnet Collapsed Architecture 13
4.2 BACnet Network Topology 15
4.3 Security 16
5 THE APPLICATION LAYER 17
5.1 The Application Layer Model 17
5.2 Segmentation of BACnet Messages 23
5.3 Transmission of BACnet APDUs 24
5.4 Application Protocol State Machines 28
5.5 Application Protocol Time Sequence Diagrams 46
5.6 Application Layer Service Conventions 55
6 THE NETWORK LAYER 57
6.1 Network Layer Service Specification 57
6.2 Network Layer PDU Structure 59
6.3 Messages for Multiple Recipients 65
6.4 Network Layer Protocol Messages 65
6.5 Network Layer Procedures 69
6.6 BACnet Routers 71
6.7 Point-To-Point Half-Routers 76
7 DATA LINK/PHYSICAL LAYERS: Ethernet (ISO 8802-3) LAN 81
7.1 The Use of ISO 8802-2 Logical Link Control (LLC) 81
7.2 Parameters Required by the LLC Primitives 81
7.3 Parameters Required by the MAC Primitives 81
7.4 Physical Media 81
8 DATA LINK/PHYSICAL LAYERS: ARCNET (ATA 878.1) LAN 82
8.1 The Use of ISO 8802-2 Logical Link Control (LLC) 82
8.2 Parameters Required by the LLC Primitives 82
8.3 Mapping the LLC Services to the ARCNET MAC Layer 82
8.4 Parameters Required by the MAC Primitives 82
8.5 Physical Media 82
9 DATA LINK/PHYSICAL LAYERS: MULTIDROP SERIAL BUS/TOKEN PASSING (MS/TP) LAN 84
9.1 Service Specification 84
9.2 Physical Layer 86
9.3 MS/TP Frame Format 96
9.4 Overview of the MS/TP Network 98
9.5 MS/TP Medium Access Control 99
9.6 Cyclic Redundancy Check (CRC) 120
9.7 Interfacing MS/TP LANs with Other BACnet LANs 121
9.8 Responding BACnet User Processing of Messages from MS/TP 121
9.9 Repeaters 122
9.10 COBS (Consistent Overhead Byte Stuffing) Encoding 123
9.11 Documenting MS/TP Node Design Choices 127
10 DATA LINK/PHYSICAL LAYERS: POINT-TO-POINT (PTP) 128
10.1 Overview 128
10.2 Service Specification 128
10.3 Point-to-Point Frame Format 133

© ISO 2026 – All rights reserved

10.4 PTP Medium Access Control Protocol 135
11 DATA LINK/PHYSICAL LAYERS: LonTalk (ISO/IEC 14908.1) LAN 157
11.1 The Use of ISO 8802-2 Logical Link Control (LLC) 157
11.2 Parameters Required by the LLC Primitives 157
11.3 Mapping the LLC Services to the LonTalk Application Layer 157
11.4 Parameters Required by the Application Layer Primitives 157
11.5 Physical Media 158
12 MODELING CONTROL DEVICES AS A COLLECTION OF OBJECTS 160
12.1 Object Characteristics and Requirements 160
12.2 Analog Input Object Type 167
12.3 Analog Output Object Type 174
12.4 Analog Value Object Type 182
12.5 Averaging Object Type 190
12.6 Binary Input Object Type 194
12.7 Binary Output Object Type 201
12.8 Binary Value Object Type 210
12.9 Calendar Object Type 218
12.10 Command Object Type 221
12.11 Device Object Type 228
12.12 Event Enrollment Object Type 244
12.13 File Object Type 253
12.14 Group Object Type 257
12.15 Life Safety Point Object Type 260
12.16 Life Safety Zone Object Type 268
12.17 Loop Object Type 276
12.18 Multi-state Input Object Type 286
12.19 Multi-state Output Object Type 292
12.20 Multi-state Value Object Type 299
12.21 Notification Class Object Type 307
12.22 Program Object Type 313
12.23 Pulse Converter Object Type 320
12.24 Schedule Object Type 328
12.25 Trend Log Object Type 336
12.26 Access Door Object Type 347
12.27 Event Log Object Type 357
12.28 Load Control Object Type 365
12.29 Structured View Object Type 376
12.30 Trend Log Multiple Object Type 381
12.31 Access Point Object Type 391
12.32 Access Zone Object Type 409
12.33 Access User Object Type 418
12.34 Access Rights Object Type 422
12.35 Access Credential Object Type 429
12.36 Credential Data Input Object Type 439
12.37 CharacterString Value Object Type 446
12.38 DateTime Value Object Type 453
12.39 Large Analog Value Object Type 459
12.40 BitString Value Object Type 467
12.41 OctetString Value Object Type 474
12.42 Time Value Object Type 479
12.43 Integer Value Object Type 485
12.44 Positive Integer Value Object Type 493
12.45 Date Value Object Type 501
12.46 DateTime Pattern Value Object Type 507
12.47 Time Pattern Value Object Type 513
12.48 Date Pattern Value Object Type 519
12.49 Deleted Clause 525

© ISO 2026 – All rights reserved

12.50 Global Group Object Type ... 526
12.51 Notification Forwarder Object Type ... 534
12.52 Alert Enrollment Object Type ... 542
12.53 Channel Object Type ... 546
12.54 Lighting Output Object Type ... 557
12.55 Binary Lighting Output Object Type ... 575
12.56 Network Port Object Type ... 587
12.57 Timer Object Type ... 629
12.58 Elevator Group Object Type ... 642
12.59 Lift Object Type ... 646
12.60 Escalator Object Type ... 659
12.61 Accumulator Object Type ... 667
12.62 Staging Object Type ... 677
12.63 Audit Reporter Object Type ... 688
12.64 Audit Log Object Type ... 694
12.65 Color Object Type ... 701
12.66 Color Temperature Object Type ... 707
13 ALARM AND EVENT SERVICES ... 714
13.1 Change of Value Reporting ... 714
13.2 Event Reporting ... 719
13.3 Event Algorithms ... 732
13.4 Fault Algorithms ... 764
13.5 AcknowledgeAlarm Service ... 772
13.6 ConfirmedCOVNotification Service ... 774
13.7 UnconfirmedCOVNotification Service ... 776
13.8 ConfirmedEventNotification Service ... 777
13.9 UnconfirmedEventNotification Service ... 780
13.10 GetAlarmSummary Service ... 783
13.11 GetEnrollmentSummary Service ... 785
13.12 GetEventInformation Service ... 788
13.13 LifeSafetyOperation Service ... 791
13.14 SubscribeCOV Service ... 793
13.15 SubscribeCOVProperty Service ... 796
13.16 SubscribeCOVPropertyMultiple Service ... 799
13.17 ConfirmedCOVNotificationMultiple Service ... 805
13.18 UnconfirmedCOVNotificationMultiple Service ... 808
13.19 AuditLogQuery ... 810
13.20 ConfirmedAuditNotification ... 814
13.21 UnconfirmedAuditNotification ... 815
14 FILE ACCESS SERVICES ... 816
14.1 AtomicReadFile Service ... 816
14.2 AtomicWriteFile Service ... 819
15 OBJECT ACCESS SERVICES ... 822
15.1 AddListElement Service ... 822
15.2 RemoveListElement Service ... 825
15.3 CreateObject Service ... 827
15.4 DeleteObject Service ... 830
15.5 ReadProperty Service ... 831
15.6 Deleted Clause ... 833
15.7 ReadPropertyMultiple Service ... 834
15.8 ReadRange Service ... 837
15.9 WriteProperty Service ... 845
15.10 WritePropertyMultiple Service ... 848
15.11 WriteGroup Service ... 851
16 REMOTE DEVICE MANAGEMENT SERVICES ... 853
16.1 DeviceCommunicationControl Service ... 853
16.2 ConfirmedPrivateTransfer Service ... 855

© ISO 2026 – All rights reserved

16.3 UnconfirmedPrivateTransfer Service ... 857
16.4 ReinitializeDevice Service ... 858
16.5 ConfirmedTextMessage Service ... 860
16.6 UnconfirmedTextMessage Service ... 862
16.7 TimeSynchronization Service ... 863
16.8 UTCTimeSynchronization Service ... 864
16.9 Who-Has and I-Have Services ... 865
16.10 Who-Is and I-Am Services ... 867
16.11 Who-Am-I and You-Are Services ... 869
17 AUTHENTICATION AND AUTHORIZATION SERVICES ... 872
17.1 Overview ... 872
17.2 Trust of Intermediaries ... 873
17.3 Authentication ... 874
17.4 Authorization ... 876
17.5 Conformance Requirements ... 882
17.6 AuthRequest Service ... 883
18 ERROR, REJECT, and ABORT CODES ... 887
18.1 Error Class - DEVICE ... 887
18.2 Error Class - OBJECT ... 887
18.3 Error Class - PROPERTY ... 888
18.4 Error Class - RESOURCES ... 890
18.5 Error Class - SECURITY ... 890
18.6 Error Class - SERVICES ... 892
18.7 Error Class - COMMUNICATION ... 893
18.8 Error Class - VT ... 898
18.9 Reject Reason ... 898
18.10 Abort Reason ... 899
18.11 Confirmed Service Common Errors ... 900
19 BACnet PROCEDURES ... 901
19.1 Backup and Restore ... 901
19.2 Command Prioritization ... 906
19.3 Device Restart Procedure ... 911
19.4 Determining Maximum Conveyable APDU ... 912
19.5 Value Source Mechanism ... 914
19.6 Audit Logging ... 916
19.7 Unconfigured Device Discovery and Address Assignment ... 927
19.8 Replacing Certificates in a BACnet/SC Network ... 928
19.9 Device Address Proxying ... 930
20 ENCODING BACnet PROTOCOL DATA UNITS ... 934
20.1 Encoding the Fixed Part of BACnet APDUs ... 935
20.2 Encoding the Variable Part of BACnet APDUs ... 947
21 FORMAL DESCRIPTION OF APPLICATION PROTOCOL DATA UNITS ... 963
21.1 APDU Definitions ... 963
21.2 Confirmed Service Productions ... 965
21.3 Unconfirmed Service Productions ... 976
21.4 Error Productions ... 980
21.5 Application Types ... 992
21.6 Base Types ... 994
22 CONFORMANCE AND INTEROPERABILITY ... 1082
22.1 Conformance to BACnet ... 1082
22.2 BACnet Interoperability ... 1083
23 EXTENDING BACnet TO ACCOMMODATE VENDOR PROPRIETARY INFORMATION ... 1085
23.1 Extending Enumeration Values ... 1085
23.2 Using the PrivateTransfer Services to Invoke Non-Standardized Services ... 1086
23.3 Adding Proprietary Properties to a Standardized Object ... 1086
23.4 Adding Proprietary Object Types to BACnet ... 1087
23.5 Restrictions on Extending BACnet ... 1087

© ISO 2026 – All rights reserved

24 DELETED CLAUSE 1088
25 REFERENCES 1089
ANNEX A - PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (NORMATIVE) 1094
ANNEX B - GUIDE TO SPECIFYING BACnet DEVICES (INFORMATIVE) 1098
ANNEX C - Removed 1099
ANNEX D - Removed 1100
ANNEX E - EXAMPLES OF BACnet APPLICATION SERVICES (INFORMATIVE) 1101
E.1 Alarm and Event Services 1101
E.2 File Access Services 1106
E.3 Object Access Services 1107
E.4 Remote Device Management Services 1114
E.5 Virtual Terminal Services 1117
ANNEX F - EXAMPLES OF APDU ENCODING (INFORMATIVE) 1120
F.1 Example Encodings for Alarm and Event Services 1120
F.2 Example Encodings for File Access Services 1131
F.3 Example Encodings for Object Access Services 1134
F.4 Example Encodings for Remote Device Management Services 1144
F.5 Example Encodings for Virtual Terminal Services 1150
ANNEX G - CALCULATION OF CRC (INFORMATIVE) 1153
G.1 Calculation of the Header CRC 1153
G.2 Calculation of the Data CRC 1159
G.3 Calculation of the Encoded CRC-32K 1163
ANNEX H - COMBINING BACnet NETWORKS WITH NON-BACnet NETWORKS (NORMATIVE) 1167
H.1 BACnet Gateways 1167
H.2 Requirements and Best Practices for BACnet Gateway Implementations 1167
H.3 Using BACnet with the DARPA Internet Protocols 1169
H.4 Using BACnet with the IPX Protocol 1171
H.5 Using BACnet with EIB/KNX 1172
H.6 Using BACnet with the Former BACnet/WS Web Services Interface Defined by Annex N 1182
H.7 Virtual MAC Addressing 1183
ANNEX I - COMMANDABLE PROPERTIES WITH MINIMUM ON AND OFF TIMES (INFORMATIVE) 1185
ANNEX J - BACnet/IP (NORMATIVE) 1187
J.1 General 1187
J.2 BACnet Virtual Link Layer 1188
J.3 BACnet/IP Directed Messages 1191
J.4 BACnet/IP Broadcast Messages 1191
J.5 Addition of Foreign B/IP Devices to an Existing B/IP Network 1194
J.6 Routing Between B/IP and non-B/IP BACnet Networks 1195
J.7 Routing Between Two B/IP BACnet Networks 1196
J.8 Use of IP Multicast within BACnet/IP 1202
ANNEX K - BACnet INTEROPERABILITY BUILDING BLOCKS (BIBBs) (NORMATIVE) 1203
K.1 Data Sharing BIBBs 1203
K.2 Alarm and Event Management BIBBs 1224
K.3 Scheduling BIBBs 1237
K.4 Trending BIBBs 1242
K.5 Device Management BIBBs 1245
K.6 Network Management BIBBs 1253
K.7 Gateway BIBBs 1257
K.8 Audit Reporting BIBBs 1258
K.9 Authentication and Authorization BIBBs 1259
ANNEX L - DESCRIPTIONS AND PROFILES OF STANDARDIZED BACnet DEVICES (NORMATIVE) 1261
L.1 Operator Interface Profiles 1261
L.2 Life Safety Operator Interface Profiles 1264
L.3 Access Control Operator Interface Profiles 1267
L.4 Controller Profiles 1270
L.5 Life Safety Controller Profiles 1272

© ISO 2026 – All rights reserved

L.6 Access Control Controller Profiles ... 1274
L.7 Miscellaneous Profiles ... 1276
L.8 BACnet General (B-GENERAL) Profile ... 1279
L.9 Lighting Operator Interface Profiles ... 1280
L.10 Lighting Control Station Profiles ... 1282
L.11 Lighting Controller Profiles ... 1283
L.12 Elevator Operator Interface Profiles ... 1285
L.13 Elevator Controller Profiles ... 1287
L.14 Authentication and Authorization Profiles ... 1289
ANNEX M - GUIDE TO EVENT NOTIFICATION PRIORITY ASSIGNMENTS (INFORMATIVE) ... 1290
M.1 Life Safety Message Group (0 - 31) ... 1290
M.2 Property Safety Message Group (32 - 63) ... 1291
M.3 Supervisory Message Group (64 - 95) ... 1292
M.4 Trouble Message Group (96 - 127) ... 1292
M.5 Miscellaneous Higher Priority Message Group (128 - 191) ... 1293
M.6 Miscellaneous Lower Priority Message Group (192 - 255) ... 1293
ANNEX N - FORMER BACnet/WS WEB SERVICES INTERFACE (INFORMATIVE) ... 1294
N.1 Data Model ... 1294
N.2 Paths ... 1295
N.3 Normalized Points ... 1296
N.4 Reference Nodes ... 1296
N.5 Localization ... 1297
N.6 Security ... 1297
N.7 Sessions ... 1297
N.8 Attributes ... 1297
N.9 Standard Nodes ... 1303
N.10 Encodings ... 1304
N.11 Service Options ... 1305
N.12 Services ... 1307
N.13 Errors ... 1325
N.14 Extending BACnet/WS ... 1326
ANNEX O - BACnet OVER ZigBee AS A DATA LINK LAYER (NORMATIVE) ... 1327
O.1 General ... 1327
O.2 ZigBee Overview ... 1327
O.3 Definitions ... 1328
O.4 Unicast Addressing ... 1328
O.5 Broadcast Addressing ... 1328
O.6 BACnet/ZigBee Data Link Layer (BZLL) ... 1329
O.7 Maximum Payload Size ... 1332
O.8 Vendor Specific Commands ... 1332
ANNEX P - BACnet ENCODING OF STANDARD AUTHENTICATION FACTOR FORMATS (NORMATIVE) ... 1333
ANNEX Q - XML DATA FORMATS (NORMATIVE) ... 1339
Q.1 Introduction ... 1339
Q.2 XML Document Structure ... 1343
Q.3 Expressing Data ... 1346
Q.5 Expressing Values ... 1348
Q.6 Binary Encoding and Access Rules ... 1350
Q.7 Extensibility ... 1350
Q.8 BACnet URI Scheme ... 1351
ANNEX R - MAPPING NETWORK LAYER ERRORS (NORMATIVE) ... 1352
ANNEX S - Removed ... 1353
ANNEX T - COBS (CONSISTENT OVERHEAD BYTE STUFFING) FUNCTIONS (INFORMATIVE) ... 1354
T.1 Preparing a COBS-Encoded MS/TP Frame for Transmission ... 1354
T.2 Decoding an Extended MS/TP Frame upon Reception ... 1357
T.3 Example COBS-Encoded Frame - Who-Has Service ... 1359
ANNEX U - BACnet/IPv6 (NORMATIVE) ... 1361

© ISO 2026 – All rights reserved

U.1 General 1361
U.2 BACnet/IPv6 BACnet Virtual Link Layer 1362
U.3 BACnet/IPv6 Directed Messages 1366
U.4 BACnet/IPv6 Broadcast Messages 1366
U.5 BACnet /IPv6 VMAC Table Management 1371
ANNEX V - MIGRATION FROM SOAP SERVICES (INFORMATIVE) 1373
V.1 Services 1373
V.2 Service Options 1375
ANNEX W - BACnet/WS RESTful WEB SERVICES INTERFACE (NORMATIVE) 1377
W.1 Data Model 1377
W.2 Paths 1377
W.3 Security 1378
W.4 Sessions 1388
W.5 Standard Data Items 1388
W.6 Metadata 1393
W.7 Functions 1393
W.8 Query Parameters 1395
W.9 Representation of Data 1397
W.10 Representation of Metadata 1397
W.11 Representation of Logs 1398
W.12 Filtering Items 1403
W.13 Limiting Number of Items 1405
W.14 Selecting Children 1405
W.15 Controlling Content of Data Representations 1405
W.16 Specifying Ranges 1409
W.17 Localized Values 1411
W.18 Accessing Individual Tags and Bits 1412
W.19 Semantics 1412
W.20 Links and Relationships 1412
W.21 Foreign XML and Other Media Types 1412
W.22 Logical Modeling 1413
W.23 Mapped Modeling 1414
W.24 Commandability 1414
W.25 Writability and Visibility 1414
W.26 Working with Optional Data 1416
W.27 Working with Optional Metadata 1416
W.28 Creating Data 1417
W.29 Setting Data 1418
W.30 Deleting Data 1420
W.31 Parentally Inherited Values 1420
W.32 Concurrency Control 1420
W.33 Server Support for Data Definitions 1421
W.34 Server Support for Metadata 1421
W.35 Client Implementation Guidelines 1422
W.36 Subscriptions 1423
W.37 Reading Multiple Resources 1424
W.38 Writing Multiple Resources 1426
W.39 Mapping of BACnet Systems 1426
W.40 Errors 1430
W.41 Examples 1432
ANNEX X - EXTENDED DISCOVERY OF DEVICES, PROFILES, AND VIEWS (NORMATIVE) 1460
X.1 Profiles 1460
X.2 xdd Files 1461
X.3 Example of Definition of Objects, Properties, and Datatypes. 1462
X.4 Views 1463
X.5 PICS Declarations 1469

© ISO 2026 – All rights reserved

ANNEX Y - ABSTRACT DATA MODEL (NORMATIVE) 1470
Y.1 Model Components 1470
Y.2 Trees 1472
Y.3 Base Types 1474
Y.4 Common Metadata 1475
Y.5 Named Values 1489
Y.6 Named Bits 1492
Y.7 Primitive Values 1493
Y.8 Range Restrictions 1495
Y.9 Engineering Units 1497
Y.10 Length Restrictions 1497
Y.11 Collections 1499
Y.12 Primitive Data 1500
Y.13 Constructed Data 1504
Y.14 Data of Undefined Type 1508
Y.15 Logical Modeling 1508
Y.16 Links 1508
Y.17 Change Indications 1510
Y.18 Definitions, Types, Instances, and Inheritance 1510
Y.19 Data Revisions 1517
Y.20 BACnet-Specific Base Types 1519
Y.21 BACnet-Specific Metadata 1520
ANNEX Z - JSON DATA FORMATS (NORMATIVE) 1522
Z.1 Introduction 1522
Z.2 JSON Document Structure 1526
Z.3 Expressing Data 1528
Z.4 Expressing Metadata 1530
Z.5 Expressing Values 1531
Z.6 Extensibility 1533
ANNEX AA –FILE FORMATS 1535
AA.1 Time Series Data Exchange File Format (NORMATIVE) 1535
AA.2 Certificate Authority Requirements Interchange File Format (NORMATIVE) 1537
ANNEX AB – BACnet Secure Connect (NORMATIVE) 1540
AB.1 BACnet Secure Connect Data link 1540
AB.2 BACnet/SC Virtual Link Layer Messages 1546
AB.3 BACnet/SC Node Operation 1559
AB.4 Node Switch and Direct Connections 1562
AB.5 Hub Function and Hub Connector 1564
AB.6 BACnet/SC Connections 1567
AB.7 Application of WebSockets in BACnet/SC 1572
ANNEX AC - EXAMPLES OF AUTHENTICATION AND AUTHORIZATION (INFORMATIVE) 1578
AC.1 Authentication Examples 1578
AC.2 Authorization Examples 1580
ANNEX AD - BACNET ENERGY SERVICES INTERFACE (NORMATIVE) 1584
AD.1 Introduction to BACnet ESI 1584
AD.2 BACnet ESI Data Classes 1585
AD.3 Data Access 1586
AD.4 Data Definitions 1587
AD.5 Examples 1589
HISTORY OF REVISIONS 1590

© ISO 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 205, *Building environment design*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 247, *Building Automation, Controls and Building Management*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement) and with the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE).

This eighth edition cancels and replaces the seventh edition (ISO 16484-5:2022), which has been technically revised.

The main changes are as follows:

— see the detailed list of changes on pages 1506 to 1527.

A list of all parts in the ISO 16484 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2026 – All rights reserved

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 subordinates) 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, other life safety applications, lighting, physical access control, and elevator monitoring, 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.

The latest update to this standard includes many new capabilities and several clarifications. These new capabilities include a BACnet/SC Certificate Authority Requirements Interchange File Format, support for BACnet/SC configuration including certificate management, Device Proxying, Authentication and Authorization, new Color Object concepts and modernization of language used for defining to MS/TP.

© ISO 2026 – All rights reserved

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, th^e promise of the information age for the public good!

© ISO 2026 – All rights reserved

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).

© ISO 2026 – All rights reserved

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).

persistent: when used to describe property values, the property value is stored in non-volatile storage so as to survive device resets and power failures.

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.

© ISO 2026 – All rights reserved

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.

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 address: address format used by the BACnet network layer, as defined in Clause 6, consisting of a network number and a MAC address.

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

BACnet network: a network of BACnet devices that share the MAC or VMAC address space under a particular BACnet network number.

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.

clamped: the act of limiting a value based on another parameter to a restricted range.

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.

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

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.

© ISO 2026 – All rights reserved

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

correlated color temperature (CCT): a concept that is defined in **ANSI_ANSLG C78.377-2015** to specify the color temperature along a white light curve through the CIE chromaticity space.

credential (physical access control): the combination of authentication factors and access rights.
current command priority: In priority arrays, the array index of the entry in the priority array from which the Present_Value's value has been taken.

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

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

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

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

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

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

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 generates event notifications.

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 luminance from one setting to another over a fixed period of time, or the change of color or color temperature from one color to another over a fixed period of time, or a change of both luminance level and color.

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.

© ISO 2026 – All rights reserved

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 BACnet router.

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.

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

internetwork: a set of two or more networks interconnected by BACnet routers. In a BACnet internetwork interconnected by BACnet routers, 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.

invalid character: Character-level encoding within a BACnet character string that is not defined by the governing body of the character encoding, or that breaks the rules of the governing body, or is not allowed by the rules of BACnet such as a null character when printable characters are required.

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

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

link: a communication facility or medium over which nodes can communicate at the IP link layer.

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

local broadcast: a message addressed to all devices or nodes on the same BACnet 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.

multicast domain: A group of B/IPv6 nodes that can communicate with each other using a particular IPv6 multicast address and UDP port combination.

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.

numeric quantity: a value that is the magnitude of a quantity. A representation of a specific amount such as temperature, volume or counts.

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.

© ISO 2026 – All rights reserved

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

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.

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 BACnet 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: access privileges that are assigned to specific roles. Access users acquire privileges through their assigned role.

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

secure device: a device that is connected to a secure network.

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.

© ISO 2026 – All rights reserved

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.

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.

time distributor: a server device distributes time via the time synchronization services.

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.

universal floor number: the number of a floor, beginning with 1 for the absolute lowest floor of the building and incrementing by one for each subsequent floor up.

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.

© ISO 2026 – All rights reserved

virtual BACnet device: a BACnet device that is modeled in software, usually in a gateway, and does not exist as a physical BACnet device.

virtual BACnet network: a BACnet network of virtual BACnet devices, usually modeled by a gateway where no physical BACnet network exists.

xyColor: the numeric representation of a color in terms of its (x,y) coordinates in the CIE chromaticity diagram, independent of its luminance.

3.3 Abbreviations and Acronyms Used in this Standard

A application layer (prefix)
ABA American Bankers Association
ACL Access Control List
AE application entity
AHU air handling unit
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
BAS building automation system
BBMD BACnet/IP broadcast management device
BDT broadcast distribution table
B/IP BACnet/IP
B/IP-M BACnet/IP multicast
B/IPv6 BACnet/IPv6
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.)
CA certificate authoritiy
CNF confirm primitive
COV change of value
CRC cyclic redundancy check
CSML control system modeling language
CSR certificate signing request, as defined by RFC 2986
CSV comma-separated values, as defined by RFC 4180
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 (parameter in primitives and messages)
DER distinguished encoding rules (see ISO/IEC 8825-1)
DESFire Data Encryption Standard Fast, Innovative, Reliable and Secure
DHCP Dynamic Host Configuration Protocol
DID ARCNET destination MAC address
DLEN 1-octet length of ultimate destination MAC layer address
DNET 2-octet ultimate destination network number

© ISO 2026 – All rights reserved

DNS	Domain Name Service
DR	demand response
DSAP	LLC destination service access point (X'82' for BACnet)
EIB	European Installation Bus
EIBA	European Installation Bus Association
ESI	energy service interface
ESI-EM	ESI energy manager
ESP	energy service provider
EUI	Extended Unique Identifier (see IEEE 802)
EXEC	capable of executing a service request
FDT	foreign device table
HTTP	hypertext transfer protocol - RFC 2616
IANA	The Internet Assigned Numbers Authority
ICI	interface control information
IEEE	Institute of Electrical and Electronics Engineers
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)
INIT	capable of initiating a service request
IP	Internet Protocol - RFC 791
IPv4	Internet Protocol version 4 - RFC 791
IPv6	Internet Protocol version 6 - RFC 2460
IRI	internationalized resource identifier - RFC 3987
ISO	International Organization for Standardization
JSON	JavaScript object notation - RFC 4627, 7159
JWT	JSON web token - RFC 7519
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
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	multidrop serial bus/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 or Port 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

© ISO 2026 – All rights reserved

O	indicates that support of a property is optional
OEO	occupant evacuation operation
OSI	open systems interconnection
P	physical layer (prefix)
PAC	ARCNET data packet header octet
PACS	physical access control system
PCI	protocol control information
PDU	protocol data unit
PICS	protocol implementation conformance statement
PKI	public key infrastructure
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
RBAC	role-based access control
REQ	request primitive
REST	representational state transfer
RFC	request for comment
RSA	Rivest-Shamir-Adleman cryptosystem
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
SLAAC	IPv6 Stateless Auto Address Configuration - RFC 4862
SLEN	1-octet length of original source MAC layer address
SLIP	Serial Line Internet Protocol - RFC 1055
SNET	2-octet original source network number
SOAP	simple object access protocol
SPC	standard project committee
SSAP	LLC source service access point (X'82' for BACnet)
TLS	transport layer security - RFC 2246
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
URI	uniform resource identifier - RFC 3986
URL	uniform resource locator - RFC 1738
UTC	Universal Time Coordinated
UUID	universally unique identifier - RFC 4122
VAV	variable air volume
VEN	virtual end node
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VT	virtual terminal
VTN	virtual top node

© ISO 2026 – All rights reserved

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)
XML extensible markup language

© ISO 2026 – All rights reserved