Discovering and fingerprinting BACnet devices - Help Net Security

By Help Net Security

Published: 2019-07-10 · Archived: 2026-04-05 19:34:56 UTC

BACnet is a communication protocol deployed for building automation and control networks. The most widely accepted networks include Internet Protocol (BACnet/IP) and the Master-Slave Token-Passing network (BACnet MS/TP). Generally, routers are required to interconnect BACnet networks while gateways are preferred for connecting non-compliant devices to a primary BACnet network.

It is anticipated that 64% of the building automation industry uses BACnet for effective operations. From a security perspective, it is essential to fingerprint IoT devices that use BACnet for communication.

BACnet/IP device object

As per the standard, there should be one BACNet device object associated with the BACnet device. The BACnet object constitutes a number of properties related to the device itself in which certain properties are optional.

From a fingerprinting perspective, a BACnet/IP device runs a service on UDP ports 47808 and 47809. A well-crafted UDP request sent to the associated service running on the stated UDP port result in information about the BACnet device. A number of examples of different properties of a BACnet device object is shown below:

Description property: This property basically contains the information about the device and is optional in nature. Listing 1 shows the description property highlighting the presence of BACnet.

```
 Instance ID: 1
Object Name: Telus_Commercial_1
Location: unknown
Vendor Name: Tridium
Application Software: Tridium 3.8.111
Firmware: 3.8.111
Model Name: NiagaraAX Station
Description: Local BACnet Device object
```

```
 Instance ID: 77000
Object Name: pCOWeb77000
Location: Unknown
Vendor Name: Carel S.p.A.
Application Software: 2.15.2C
Firmware: A1.5.4 - B1.2.4
Model Name: PCO1000WB0
Description: Carel BACnet Gateway
```

Application software property: This property is required by the BACnet device object so that the client knows which software version is installed on the device. Listing 2 highlights the application software property revealing the presence of software running on the targeted BACnet device.

```
 Instance ID: 424242
Object Name: Compass_424242
Location: unknown
Vendor Name: Alerton
Application Software: 1.5.20170510.1 - BACnet: Tridium 3.8.41.32
Firmware: 3.8.208
Model Name: Compass
Description: Compass NBT - Internal BACnet device
```

```
 Instance ID: 250001
Object Name: device250001
Location: Device Location
Vendor Name: Automated Logic Corporation
Application Software: PRG:vrec_novel_ice_bacnet
Firmware: BOOT(id=0,ver=0.01:001,crc=0x0000) MAIN(id=3,ver=6.00a:054,crc=0xB079)
Model Name: LGR25
Description: Device Description
```

Model and firmware properties: The firmware and model name properties are required and could reveal the presence of a BACnet device. Listing 3 shows that associated properties contain the information about the presence of BACnet device.

```
 Instance ID: 7020
Object Name: PXCC20
Location: RTU-20
Vendor Name: Siemens Industry Inc., Bldg Tech
Application Software: BXE1230
Firmware: EPXC V3.2.3 BACnet 4.3g
Model Name: Siemens BACnet Field Panel
Description: RTU-20
```

Object name property: This property reflects the name of the object itself. In certain scenarios, the value of this property could reveal the presence of a BACnet device as shown in Listing 4.

```
 Instance ID: 1
Object Name: Bacnet
Vendor Name: American Auto-Matrix
Application Software: R_02_06_01
Firmware: 1.2
```

```
Model Name: AAM-Router
Description: Router
```

BBMD device property: BACnet/IP Broadcast Management Device (BBMD) is deployed to broadcast and distribute messages throughout the BACnet/IP network, which constitutes a number of interconnected TCP/IP sub networks. Once the BACnet/IP messages are sent by the devices in the subnet, the associated BBMD forwards the same messages to other peer BBMDs. Once the destination BBMD receives the message, it is then re-broadcasted to the same subnet. Listing 5 shows the response obtained from the UDP querying which highlight the presence of BDMD device.

```
 Instance ID: 2210125
Object Name: AS_2210125
Vendor Name: Schneider Electric
Application Software: N/A
Firmware: Server 1.5.0.2307
Model Name: Building Operation Automation Server

 BACnet Broadcast Management Device (BBMD):
50.127.108.206:47808
```

BACnet APDU errors: The Application Protocol Data Units (APDU) constitutes application layer specific parameters. Generally, protocol data units transfer the information in the form of units among peers in the associated network for sharing and processing of information. APDU errors can also be used to validate and verify the presence of BACnet devices in the network. Example: the device responds back to the client with notification error messages as “BACnet ADPU Type: Error (5)”. As a result, a BACnet device can be detected accordingly.

Additionally, a number of BACnet device have built-in embedded HTTP web servers that can also be used to discover the devices. A number of scenarios are discussed below:

HTTP response header – WWW-Authenticate Realm: The WWW-Authenticate HTTP response header defines the web authentication method supported by the resource on the remote location. This header is primarily used as a response received from the web server or application over HTTP/HTTPS. The header has type and realm parameters. The type defines the authentication scheme, whereas realm defines the description of the protected resource. Listing 6 highlights a BACnet/IP resource (or device) running over HTTP and protected with BASIC authentication and realm as “UC32.net BACnet(2)”.

```
 HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="UC32.net BACnet(2)"
Content-Type: text/html
Transfer-Encoding: chunked
Server: Allegro-Software-RomPager/4.01
Connection: close

 HTTP/1.1 401 Authorization Required
WWW-Authenticate: Basic realm="EasyBAC BACnet Device WebSetup"
```

```
Server: Cimetrics Eplus Web Server v.1.2
Connection: Close
```

HTTP response header-server: The embedded web server present in BACnet devices can also be queried via HTTP to detect the presence of a BACnet device. Listing shows that HTTP response header “Server” discloses the presence of a BACnet device. Additionally, certain embedded web servers also reveal information about “BACnet Network” via HTTP/1.0 request acceptance as shown in Listing 7.

```
 HTTP/1.0 200 OK
Connection: keep-alive
Server: SB-BACnet
Content-Length: 2960
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=iso-8859-

 HTTP/1.0 200 BACnet Network
Server: BACnet4Linux
Content-Type: text/html
Content-Length: 599
Connection: close
```

Web HTML elements: A number of HTML web elements can also disclose the presence of a BACnet device. When a client sends a HTTP GET/POST request to an embedded web server, the web page contents are returned in addition to the HTTP response header. The elements present in the web page can reveal the information about the BACnet. Listing 8 shows that “title” element in the web page disclosing the same.

```
 HTTP/1.1 200 OK
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
Content-Length: 145
Last-Modified: Mon, 27 May 2019 02:06:13 GMT
Content-Type: text/html

 <html><head><title>ACP BACnet</title></head>
```

Apart from the UDP querying and HTTP traffic analysis, NetBIOS can also be used to detect the presence of BACnet devices. A similar scenario is discussed below.

NetBIOS traffic: NetBIOS over TCP/IP is used for obtaining information about nameservice listening on the remote target. Generally, the query is sent to UDP port 137, the server responds with the details of all the services as part of a NetBIOS response. There is a name code (number) associated with the response as shown in Listing 9 below. The numeric code “0x1e” shows the usage of browser service elections on the domain BACnet. This information highlights the presence of BACnet devices on the network.

```
NetBIOS Response
Servername: LAZNAS
Names:
LAZNAS <0x0>
LAZNAS <0x3>
LAZNAS <0x20>
BACNET <0x0>
BACNET <0x1e>
```

Experiment

Using the indicators discussed above, we conducted a small analytical experiment to obtain the model numbers and type of devices supporting the BACnet protocol for communication. We designed our own custom script to trigger fast scanning. However, Nmap provides an associated script to perform the same activity. Figure 1 and Figure 2 show samples of the BACnet devices collected from the output retrieved from the conducted experiment.

```
Model Name  VLX-Platinu Model Name  Wiser for K Model Name  eBMGR-TCH-M
Model Name  VWGBACnet   Model Name  XLWeb2      Model Name  eBMGR-TCH-M
Model Name  Vacon 100   Model Name  XT-LB       Model Name  enteliWEB
Model Name  Veris E8951 Model Name  XT-RB       Model Name  foxcore
Model Name  Version 9   Model Name  YK-MAP1810- Model Name  homeLYnk
Model Name  View Master Model Name  YZP487 F101 Model Name  i-Vu CCN Ro
Model Name  WC-BACems   Model Name  Zensys_Mast Model Name  i-Vu Link
Model Name  WC-RB10+    Model Name  b3804       Model Name  iSMA-B-MIX1
Model Name  WC-RB11+    Model Name  bCX1-CR     Model Name  iTM
Model Name  WC-RB12+    Model Name  bCX1-R      Model Name  iTM BACnet
Model Name  WC-RP12     Model Name  bacds       Model Name  iVu Open In
Model Name  WC15        Model Name  cVu-ccn2    Model Name  iVu Open Li
Model Name  WC16        Model Name  eBCON       Model Name  iVu Open Ro
Model Name  WC17        Model Name  eBCON-MB    Model Name  iVu-Exp
Model Name  WC18        Model Name  eBMGR       Model Name  iVu-ccn2
Model Name  WC19        Model Name  eBMGR-MOD1  Model Name  ivuccnroute
Model Name  WC20        Model Name  eBMGR-MOD12 Model Name  ivulink_lon
Model Name  WIN900      Model Name  eBMGR-MOD14 Model Name  ivulink_mod
Model Name  WebAccess B Model Name  eBMGR-MOD2  Model Name  novaPro Ope
Model Name  WebPRTL     Model Name  eBMGR-MOD4  Model Name  pCOBCM@
Model Name  Wi-MGR/FDS- Model Name  eBMGR-MOD5  Model Name  pCOWeb@
Model Name  WiNG-MGR    Model Name  eBMGR-TCH   Model Name  spaceLYnk
```

Figure 1: Model names of devices supporting the BACnet protocol

Model Name		Model Name	C283T-3	Model Name	DSM_RTR-MOD
Model Name	AHU	Model Name	CIPC	Model Name	DSM_RTR-MOD
Model Name	189697	Model Name	CO-E283W-3	Model Name	DXR2.E09-1
Model Name	2.36",2019-	Model Name	COSMOS OPEN	Model Name	DXR2.E12P-1
Model Name	40CD30H3ABB	Model Name	CP3	Model Name	Desigo CC
Model Name	40MM62MA0AI	Model Name	CP3N	Model Name	E-DDC3.3 S
Model Name	40MM62MA0AI	Model Name	CV17	Model Name	E-DDC4.0
Model Name	750-830	Model Name	CV19	Model Name	E-DDC5.0
Model Name	750-831	Model Name	CV20	Model Name	E-LINK-ttek
Model Name	88.200.97.2	Model Name	CatNet CH-1	Model Name	E151DW-3
Model Name	88.200.97.2	Model Name	Climatix DH	Model Name	E283W-3
Model Name	A7810-0	Model Name	Climatix PO	Model Name	E34E Series
Model Name	A8810-0	Model Name	Compass	Model Name	EC1 HotelLi
Model Name	A8812-0	Model Name	Concierge C	Model Name	ECOM V4
Model Name	A8812-1	Model Name	ControlMaes	Model Name	ECY-303 Rev
Model Name	A8812-3G	Model Name	CopperCube	Model Name	ECY-PTU107
Model Name	A8812-GSM	Model Name	Cylon BACne	Model Name	ECY-PTU207
Model Name	AAC-PI	Model Name	D-BACS BACn	Model Name	ECY-PTU208
Model Name	AAC20	Model Name	DAC_606E	Model Name	ECY-S1000 R
Model Name	AAM-Router	Model Name	DCU 2	Model Name	ECY-S1000 R
Model Name	ACM-GC	Model Name	DD 1.0	Model Name	ECY-TU203 R
Model Name	AE-200/AE-5	Model Name	DDC420	Model Name	ECY-VAV Rev
Model Name	AGZ	Model Name	DENT PS3037	Model Name	EMBAS
Model Name	AS	Model Name	DSC-1212	Model Name	ENC-SW
Model Name	AS-B 24 Han	Model Name	DSC-1212E	Model Name	ENS
Model Name	AS-B 36 Han	Model Name	DSC-1280E	Model Name	ENS-1
Model Name	AS-P	Model Name	DSC-1616E	Model Name	ENS-1 - pow
Model Name	ASDEPRM	Model Name	DSC1616	Model Name	ES
Model Name	ASM-24E	Model Name	DSC1616E	Model Name	ETHER-Link
Model Name	ASM_24E	Model Name	DSC_1146E	Model Name	ETOS
Model Name	ASM_24E-MOD	Model Name	DSC_1146E-E	Model Name	EY-AS521F00
Model Name	BAC-5051E	Model Name	DSC_1146E-M	Model Name	EY-AS521F00
Model Name	BAC-5901CE	Model Name	DSC_1180E	Model Name	EY-AS524F00
Model Name	BAC-A1616BC	Model Name	DSC_1180E-M	Model Name	EY-AS525F00
Model Name	BAC0 Script	Model Name	DSC_1212E	Model Name	EY-AS525F00
Model Name	BACnet Adva	Model Name	DSC_1212E-M	Model Name	EY-RC500F00
Model Name	BACnet Dire	Model Name	DSC_1280E	Model Name	EY-RC502F00
Model Name	BACnet Serv	Model Name	DSC_1280E-M	Model Name	EY-RC504F00
Model Name	BACnet/IP t	Model Name	DSC_1280E-M	Model Name	EY-RC504F10
Model Name	BACnet4J	Model Name	DSC_1616E	Model Name	EY-RC504F20
Model Name	BACport	Model Name	DSC_1616E-M	Model Name	Eagle
Model Name	BAS920	Model Name	DSC_1616E-M	Model Name	EcoSmart
Model Name	BASRT-B	Model Name	DSC_606E	Model Name	Excel Web

Figure 2: Model names of devices supporting the BACnet protocol

A number of indicators have been presented in this article to highlight the different ways to fingerprint BACnet devices on the Internet. Fingerprinting of BACnet devices is necessary to obtain visibility into the nature of the device that is required to map the complete security posture of the device.

Contributing author: Srinivas Akella, CTO, WootCloud.
