

# BACnet 网络讲义

苏州科技学院  
电子与信息工程系

2006 年 10 月

# 目 录

第 1 章	BACnet 协议概述.....	1
§1.1	BACnet 协议模型.....	1
1.1.1	BACnet 简介.....	1
1.1.2	BACnet 协议模型.....	1
§1.2	BACnet 协议的体系结构.....	2
§1.3	BAC 网络的拓扑结构.....	5
§1.4	BACnet 的协议栈和数据流.....	6
第 2 章	BACnet 应用层规范.....	8
§2.1	BACnet 协议的应用层规范.....	8
§2.2	BACnet 应用层服务类型.....	9
§2.3	BACnet 应用层报文分析.....	11
2.3.1	应用层接口控制信息.....	11
2.3.2	应用层协议数据单元的编码.....	11
2.3.3	BACnet 报文的分段.....	12
§2.4	BACnet APDU 的传输.....	12
2.4.1	证实请求报文的传输.....	12
2.4.2	分段证实请求报文的传输.....	13
2.4.3	分段复杂回应报文的传输.....	13
2.4.4	分段回应 APDU 的传输.....	14
§2.5	与传输有关的其它问题.....	14
2.5.1	事务状态机制的中止.....	14
2.5.2	重复报文的处理.....	14
2.5.3	资源的回收.....	15
第 3 章	BACnet 网络层规范.....	16
§3.1	BACnet 网络层规范的内容.....	16
3.1.1	BACnet 网络层的服务原语.....	16
3.1.2	BACnet 网络层 PDU 结构.....	17
3.1.3	多播报文和广播报文.....	18
3.1.4	网络层协议报文.....	18
3.1.5	网络层协议运行规程.....	19
§3.2	BACnet 路由器.....	21
§3.3	点到点半路由器.....	22
第 4 章	BACnet 数据链路/物理层规范.....	24
§4.1	数据链路/物理层协议的内容.....	24
4.1.1	BACnet 的以太网规范.....	24
4.1.2	BACnet 的 ARCNET 局域网规范.....	25
4.1.3	BACnet 的主从/令牌传递(MS/TP)局域网规范.....	26
§4.2	BACnet 的点到点(PTP)通信规范.....	28
4.2.1	BACnet 点到点通信工作原理.....	28
4.2.2	服务规范.....	28

4.2.3 帧格式.....	28
§4.3 BACnet 的 LonTalk 局域网规范 .....	29
第 5 章 BACnet 的对象模型.....	31
§5.1 BACnet 的对象模型及其属性.....	31
5.1.1 BACnet 的对象定义.....	31
5.1.2 BACnet 对象的属性.....	32
§5.2 BACnet 对象的分类介绍.....	33
5.2.1 输入输出值对象类型及其属性.....	33
5.2.2 命令对象类型.....	35
5.2.3 时序表和时间表对象类型.....	35
5.2.4 事件登记对象类型.....	35
5.2.5 文件、组和环对象类型.....	35
5.2.6 多态输入输出对象类型.....	36
5.2.7 通知类对象类型.....	36
5.2.8 程序对象类型.....	36
第 6 章 BACnet 的服务.....	37
§6.1 BACnet 的服务定义.....	37
§6.2 BACnet 服务的分类介绍.....	38
6.2.1 报警与事件服务.....	38
6.2.2 文件访问服务.....	39
6.2.3 对象访问服务.....	39
6.2.4 远程设备管理服务.....	39
6.2.5 虚拟终端服务.....	40
6.2.6 网络安全服务.....	41
§6.3 BACnet 协议的一致性描述.....	41
6.3.1 BACnet 协议的一致性类别.....	41
6.3.2 BACnet 协议的功能组.....	41
第 7 章 BACnet/IP---BACnet 互联网.....	43
§7.1 BACnet 互联网的概念.....	43
§7.2 用 PAD 组建 BACnet 互联网.....	43
§7.3 BACnet/IP 网络.....	45
§7.4 BACnet/IP 和 BACnet 设备的混合网络.....	48

# 第 1 章 BACnet 协议概述

本章介绍 BACnet 协议的产生及协议模型，讨论 BACnet 网络的体系结构、拓扑结构、协议栈以及数据流。

## § 1.1 BACnet 协议模型

### 1.1.1 BACnet 简介

BACnet (A Data Communication Protocol for Building Automation and Control Network) 是一种为楼宇自动控制网络所制定的数据通信协议，它由美国冷暖空调工程师协会组织的标准项目委员会 135P (Standard Project Committee: SPC 135P) 于 1995 年 6 月制定。BACnet 标准产生的背景是用户对楼宇自动控制设备互操作性 (Interoperability) 的广泛要求，即将不同厂家的设备组成一个一致的自控系统。BACnet 实现楼宇自控设备的互操作性的思想是这样的，一般楼宇自控设备从功能上讲分为两部分，一部分专门处理设备的控制功能，另一部分专门处理设备的数据通信功能，不同厂商生产的设备使用各自专门的数据通信的方式，所以不同厂商的设备之间没有很好的互操作性。BACnet 就是要建立一种统一的数据通信的标准，用于设备的通信部分，从而使得按这种标准生产的设备，都可以进行通信，实现互操作性。BACnet 标准只是规定了楼宇自控设备之间要进行“对话”所必须遵守的规则，并不涉及如何实现这些规则，各厂商可以用不断进步的技术来开发，从而使得整个领域的技术不断进步。

### 1.1.2 BACnet 协议模型

SPC 征集了各方面的意见，同时参考了国际上各种现已成文的或是事实上的数据通信标准，讨论得出了一个具有以下特性的网络协议模型：

(1) 所有的网络设备，除了主从/令牌传递式从属机 (MS/TP slaves: master-slave/token-passing slaves) 以外，都是对等的 (Peer)。当然某些同等设备可能比其他具有更多的特权 (Privilege) 和职责 (Responsibility)。

(2) 每一个网络设备都称之为是一个“对象” (Object) 的实体 (entity)，这是一个具有网络访问特征的集合模型。每个对象又用一些“属性” (Property) 来描述，这些属性表示了设备的硬件、软件以及操作的各个方面。在不需要了解设备内部设计或配置细节的情况下，对象提供了识别和访问设备信息的方法。尽管该标准规定了广泛的应用对象的类型以及它们的属性，但是一旦需要，利用开发工具仍可以自由地增加新的对象类型。

(3) 通信功能是通过读写某些对象的属性，以及利用其他协议提供的“服务” (Service) 来完成的。尽管该标准规定了一套详尽的服务，但是一旦需要，该标准的机制也同样允许利用开发工具增加新的服务。

(4) 设备的完善性 (Sophistication)，即实现特定服务请求或理解特定对象类型种类的能力，是由设备的“一致性类别” (Conformance Class) 所反映的。每一种类别定义了一个包括服务、对象、属性的最小集合，声明为某一类别的设备必须支持其相应的集合。

(5) 由于该标准遵循了 ISO 的“分层”通信体系结构的概念，因此使用不同的网络访问方法和物理介质可以交换相同的报文。这样可以根据传输速度和吞吐量的要求，采用相宜的开销来配置 BACnet 网络。

(6) 该标准是为暖气、通风、空调、制冷控制设备所设计的，同时它也为其他楼宇控制系统的集成提供了基本原则，例如照明、保安、消防系统等。虽然这些扩展超出了该标准的范围，但实现起来却简单明了。并且，标准中定义的许多对象和服务也可以不加修改地被应用。当然，一旦这些其他类型的楼宇控制功能需要，也可以简单方便地定义新的对象和服务。

(7) 该标准的目的是为暖气、通风、空调、制冷控制设备和其它楼宇自控设备的监控定义数据通信的服务和协议。除此之外，标准还定义了抽象的、面向对象的表示法，用来描述这些设备间的信息通信，以便于在楼宇中使用数字控制技术。

所有的通信协议都是一个解决各种信息交换问题的方案的集合，并且随着时间的推移和技术的进步而不断改变，BACnet 网络同样也不例外。

## § 1.2 BACnet 协议的体系结构

国际标准化组织在制定计算机网络通讯协议标准时定义了一个模型，称为开放式系统互联参考模型（OSI 模型），模型的目的是解决计算机与计算机之间普遍的通信问题，并将这个复杂的问题分解成 7 个小的、易解决的子问题，每个子问题只与某些通信功能相关联，如图 1-1 所示。这样每个子问题便形成了协议体系结构中的一“层”。任何两个遵循该模型及有关标准的设备或系统，都可以实现互连和互操作。

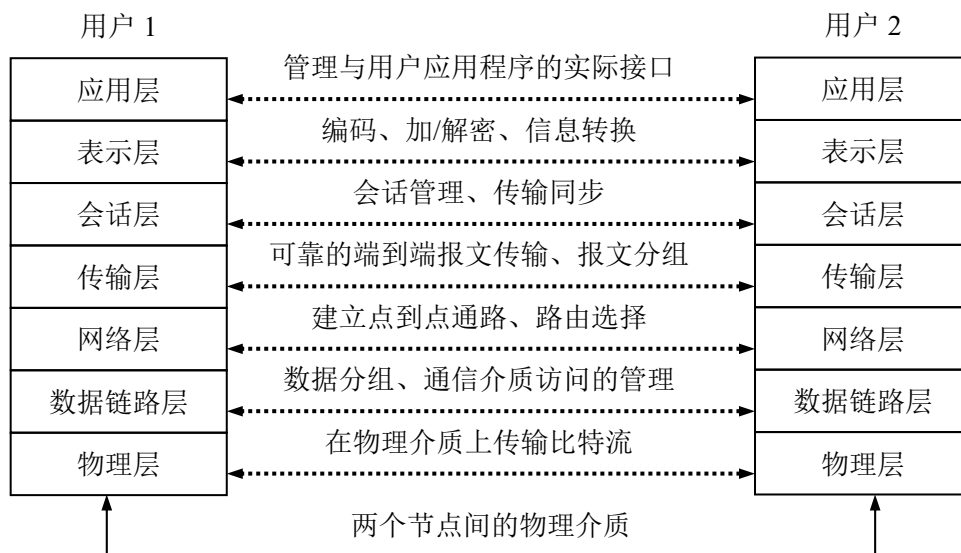


图 1-1 开放式系统互联基本参考模型

SPC 制定 BACnet 标准时，确定 BACnet 作为一种开放性计算机局域网协议，它仍然采用 OSI 模型的“分层”通信体系结构的概念。在确定分层的层数时，考虑了下列两个因素：第一，OSI 模型的实现需要很高的费用，实际上在绝大部分楼宇自控系统应用中也并不需要这么多的层次。但是从 OSI 的功能性方面考虑，经过简化后，OSI 模型仍然是设计楼宇自控协议的一个很好参考，如果只包含 OSI 模型中被选择的层次，其它各层则去掉，这样

减少了报文长度，降低了通信处理开销，同时也会节约楼宇自控工业的生产成本。第二，如果能够充分利用现有的、易用的、广泛使用的局域网技术，如 Ethernet、ARCNET 和 LonTalk，不但可以降低成本，同时也有利于性能的提高。由此，SPC 确定 BACnet 标准协议体系结构为一个包含四个层次的分层体系结构，这四个层次相对于 OSI 模型中的物理层、数据链路层、网络层和应用层，如图 1-2 所示。BACnet 标准定义了自己的应用层和网络层，对于其数据链路层和物理层，提供了以下五种选择方案：

第一种选择是 ISO 8802-2 类型 1 定义的逻辑链路控制（LLC）协议，加上 ISO 8802-3 介质访问控制（MAC）协议和物理层协议。ISO 8802-2 类型 1 提供了无连接不确认的服务，ISO 8802-3 则是著名的以太网协议的国际标准。

第二种选择是 ISO 8802-2 类型 1 定义的逻辑链路控制（LLC）协议，加上 ARCNET（ATA/ANSI 878.1）。

第三种选择是主从/令牌传递（MS/TP）协议加上 EIA-485 协议。MS/TP 协议是专门针对楼宇自控设备设计的，它通过控制 EIA-485 的物理层，向网络层提供接口。

第四种选择是点对点（PTP）协议加上 EIA-232 协议，为拨号串行异步通信提供了通信机制。

第五种选择是 LonTalk 协议。

这些选择都支持主/从 MAC、确定性令牌传递 MAC、高速争用 MAC 以及拨号访问。拓扑结构上，支持星型和总线型拓扑；物理介质上，支持双绞线、同轴电缆、光缆。

BACnet 的协议层次				对应的 OSI 层次
BACnet 应用层				应用层
BACnet 网络层				网络层
ISO 8802-2 (IEEE 802.2)类型 1	MS/TP (主从/令牌传递)	PTP (点到点协议)	LonTalk	数据 链路层
ISO 8802-3 (IEEE 802.3)	ARCNET EIA-485 (RS485)	EIA-232 (RS232)		物理层

图 1-2 BACnet 简化的体系结构层次图

以下详细讨论 BACnet 选择一个四层体系结构的原因。首先仔细考虑 BACnet 网络的独特特征。BACnet 的特征主要有以下两点：

- (1) BACnet 网络是一种局域网。即使在某些应用中，楼宇中设备间远距离的通信必不可少时，这一点仍然是不变的。这种远距离的通信功能，是由电信网来实现。通信过程中要解决的路由、中继、可靠传输等问题，都由电信网来处理。在此电信网可看成是 BACnet 网络外部的部分。
- (2) BACnet 设备是静态的，即在空间上，它们不会经常被移来移去。在要完成的功能上，从某种意义上说也是不变的，即不会今天生产的设备的功能是这样，明天就完全不同了。

在充分了解 BACnet 网络的特征后，就可讨论 OSI 模型的各层在 BACnet 网络中的适用性了。

OSI 模型的物理层提供了设备间的物理连接,以及传输载波信号的方式。显然在 BACnet 协议中,物理层是必不可少的。

OSI 模型的数据链路层,负责将数据组织成帧(Frame)或分组(Packet)、管理通讯介质的访问、寻址(Address),以及完成一些错误校正(Error Recovery)和流量控制。这些都是 BACnet 协议所需要的,因此数据链路层也是必不可少的。

OSI 网络层的功能,包括将全局地址解析为局部地址,在一个或多个网络中进行报文的路由,协调不同类型网络的差异(如不同网络所允许的最大报文长度),序列控制,流量控制,差错控制,以及多路复用。由于 BACnet 网络的拓扑特点,在各个设备之间只存在一条逻辑通路(参见图 3),这样便不需要最优路由的算法。其次,BACnet 网络是由中继器或网桥互联起来的一个或多个网段所组成的网络,它具有单一的局部地址空间。在这样一种单一网络中,许多 OSI 网络层的功能也变得多余,或者与数据链路层相重复。当然在某些 BACnet 网络系统中,网络层也可能是必不可少的。例如,在一个 BACnet 的网际网(internet)中,当两个或多个网络使用了不同的 MAC 层时,便需要区别局部地址和全局地址,这样才能将报文路由到正确的网络上去。在 BACnet 协议中,通过定义了一个包含必要的寻径和控制信息的网络层头部,来完成这种简化了的网络层功能。

传输层主要是负责提供可靠的端到端的报文传输、报文分段、序列控制、流量控制,以及差错校正。传输层的许多功能与数据链路层相似,只是在作用范围上有所不同。传输层提供的是端到端的服务,而数据链路层则提供的是单一网络上点到点的服务。由于 BACnet 支持多种网络的配置,因此协议必须提供传输层端到端的服务。在 BACnet 网络中要提供三个方面的传输层的功能,第一是可靠的端到端传输和差错校正功能,第二是报文分段和端到端的流量控制,第三是实现报文的正确重组,序列控制。由于 BACnet 是建立在无连接的通信模型基础上的,因此所需的服务大大减少,并且可以被高层来实现,所以,传输层的这些功能可以通过 BACnet 应用层来实现,这样,在 BACnet 协议体系中不单独设置传输层,相应的功能放在应用层中完成,从而节省了通信开销。

会话层的功能是在通信双方之间建立和管理长时间对话。包括建立同步标志点,用来在出错时回复到前一个标志点,以避免对话重新开始。但在一个 BACnet 网络中,绝大部分的通信都是很简短的,比如读写一个或一些值,通知某个设备某个警报或事件,或者更改某个设定值。当然长时间的信息交换偶尔也会发生的,比如上载或下载某个设备。由于绝大部分事务处理都是简短的,会话层的服务极少用到,再考虑到带来的开销,因此 BACnet 标准中不包括这层。

表示层为通信双方提供了屏蔽下层传送语法的服务。这种传送语法是用来将应用层中抽象的用户数据表示,变成适合下层传输的字节序列。但当只存在一种传送语法时,表示层的功能便减少到对应用程序的数据进行编码。由于在 BACnet 在应用层中定义了一个固定的编码方案,因此一个独立的表示层也变得不再需要。

协议的应用层为应用程序提供了完成各自功能所需的通信服务。在此基础上,应用程序可以监控 HVAC&R 和其它楼宇自控系统。显然应用层是本协议所必需的。

从以上讨论中,可以得到以下几点:

1. 实现一个完全的 OSI 七层体系结构需要大量的资源和开销,因此它对于目前的楼宇自控系统是不适用的。
2. 根据 OSI 模型,采用现有的计算机网络技术将会带来以下好处:节约成本,便于与其它计算机网络系统集成。
3. 根据楼宇自控系统的环境及要求,可以通过去除 OSI 某些层的功能来简化 OSI 模型。

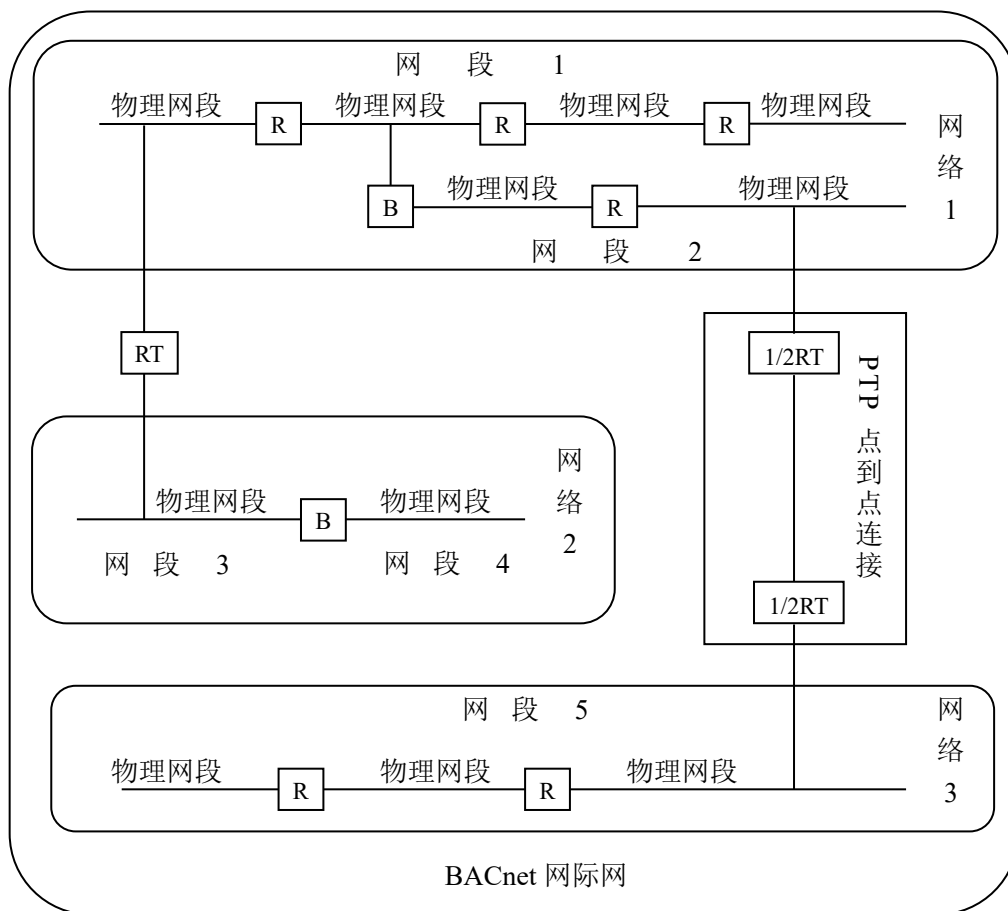
4. 由物理层、数据链路层、网络层和应用层组成的一个简化体系结构，是当今楼宇自控系统的最佳解决方案。

## § 1.3 BAC 网络的拓扑结构

为了应用的灵活性，BACnet 并没有严格规定网络的拓扑结构。BACnet 设备可以通过专线或拨号异步串行线，与四种局域网之一进行物理相连。而这些网络可以通过 BACnet 路由器或一对半路由器进一步互联。

在 BACnet 网络中，定义了如下这样一些拓扑结构：

1. 物理网段（Physical Segment）：直接连接一些 BACnet 设备的一段物理介质。
2. 网段（Segment）：多个物理网段通过“中继器”在物理层连接，所形成的网络段。
3. 网络(Network)：多个 BACnet 网段通过“网桥”互连而成，每个 BACnet 网络都形成一个单一的 MAC 地址域。这些在物理层和数据链路层上连接各个网段的设备，可以利用 MAC 地址实现报文的过滤。
4. 网际网（Internetwork）：将使用不同 LAN 技术的多个网络，用 BACnet “路由器”互联起来，便形成了一个 BACnet “网际网”。在一个 BACnet 网际网中，任意两个节点之间恰好存在着一报文通路。这些概念如图 1-3 所示。



其中：B = 网桥，RT = 路由器，R = 中继器，1/2RT = 半路由器

图 1-3 BACnet 网际网结构图



## § 1.4 BACnet 的协议栈和数据流

在 BACnet 中，两个对等应用进程间的信息交换，依然按照 OSI 技术报告中关于 ISO 的服务惯例（ISO TR 8509），被表示成抽象的服务原语的交换。BACnet 定义了四种服务原语：**请求、指示、响应和证实原语**，用来传递某些特定的服务参数。而包含这些原语的信息，又是由 BACnet 标准中定义的各种协议数据单元（PDU：Protocol Data Unit）来传递的。

当应用程序需要同远地的应用进程通讯时，它通过调用 API 访问本地的 BACnet 用户单元（应用层中为用户应用程序提供服务的访问点）。API 的某些参数，如接收服务请求的设备的标志号（或地址）、协议控制信息等，将直接下载到网络层或数据链路层。而其余参数将组成一个应用层服务原语，通过 BACnet 的用户单元传到 BACnet 的应用服务单元（应用层中利用下层服务完成应用层服务的部分）。

从概念上来讲，由应用层服务原语产生的应用层协议数据单元（APDU），构成了网络层服务原语的数据部分，并通过网络层服务访问点下载到网络层。同样，这个请求将进一步下载到本地设备协议栈的以下各层。整个过程如图 1-4 所示（见下一页）。

于是，报文就这样被传送到远地的设备，并在远地设备协议栈中逐级上传，最后指示原语看起来似乎是直接从远地的 BACnet 应用服务单元上传到远地的 BACnet 用户单元。任何从远地设备发回的响应，也是以该方式回传给请求设备的。

BACnet 协议采用的分层思想，来源与一个简单的科学原理——分层原理（Layering Principle）。即“在目标计算机上的第 N 层软件必须恰好接收由在发送计算机上的第 N 层软件所发送的数据”。换句话说，在数据发送前，协议进行的任何转换在接收时必须被完全地逆转换。如果在发送计算机上的一个特定层将一个头部放入帧中，在接收计算机的相应层必须除去该头部。分层思想简化了协议的设计和测试，避免了一层协议软件引入其它层可见的改变。这样，每一层的发送和接收软件可独立于其它层进行设计、实现、测试。

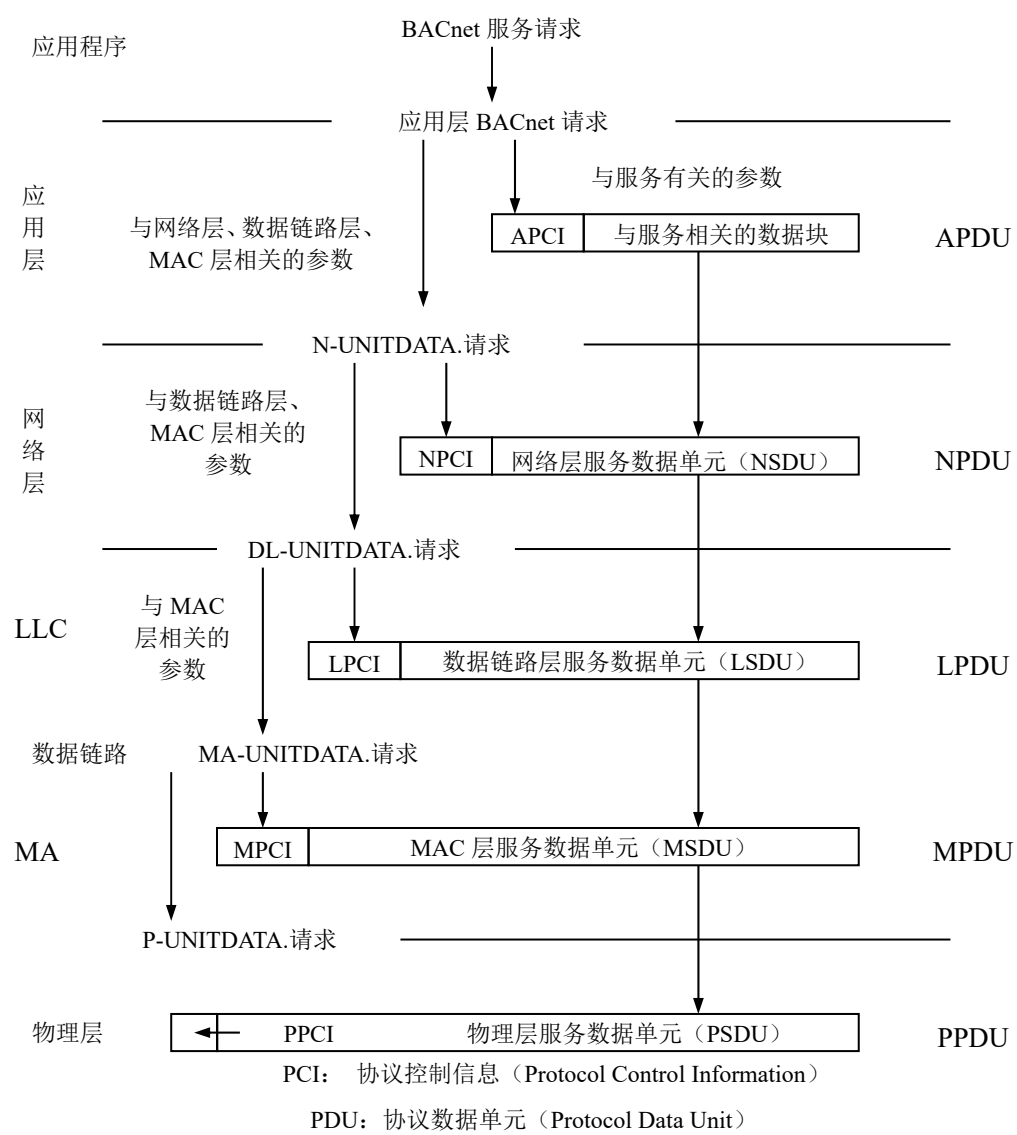


图 1-4 BACnet 协议栈及数据

## 第 2 章 BACnet 应用层规范

本章介绍 BACnet 的应用层规范的原理和运行机制, 概要介绍 BACnet 应用层的模型、主要的服务原语以及应用层报文的结构, 并讨论 BACnet 各种报文的传输过程以及与报文传输相关的其它问题。

### § 2.1 BACnet 协议的应用层规范

BACnet 网络的应用层协议要解决三个问题, 向应用程序提供通信服务的规范, 与下层协议进行信息交换的规范, 和与对等的远程应用层实体交互的规范。首先对一些相关的概念进行说明。

应用进程是指, 为了实现某个特定的应用 (例如, 节点设备向一个远端的温度传感器设备请求当前温度值) 所需要的进行信息处理的一组方法。一般来说, 这是一组计算机软件。

应用进程分为两部分, 一部分专门进行信息处理, 不涉及通信功能, 这部分称为**应用程序**。另一部分处理 BACnet 通信事务, 称为**应用实体**。应用程序与应用实体之间通过应用编程接口(API)进行交互。**BACnet 应用层协议只对应用实体进行规范**, 不涉及应用程序和应用编程接口。但在具体实现过程中, 应用编程接口一定是某个函数、过程或子程序的调用。

图 2-1 示出了这些概念, 图中阴影部分是应用进程位于 BACnet 应用层中的部分。

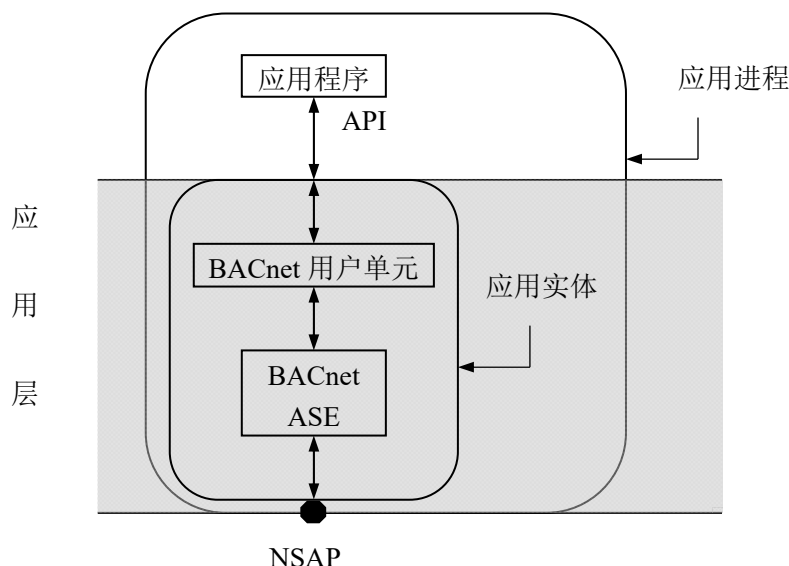


图 2-1 BACnet 应用进程模型

应用实体本身又由两部分组成, 分别是 **BACnet 用户单元**和 **BACnet 应用服务单元 (ASE)**。应用服务单元是一组特定内容的应用服务, 这些应用服务包括: 报警与事件服务, 文件访问服务, 对象访问服务, 远程设备管理服务, 虚拟终端服务, 和网络安全。用户单元的功能是支持本地 API, 负责保存事务处理的上下文信息, 产生请求标志符 (ID), 记录标志符所对应的应用服务响应, 维护超时重传机制所需的超时计数器, 以及将设备的行

为要求映射成为 BACnet 的对象。我们将在后续的文章中介绍这些应用服务和对象的内容。

“BACnet 设备”是指任何一种支持用 BACnet 协议进行数字通信的真实的或者虚拟的设备。一个 BACnet 设备有且只有一个“设备对象”，而且被一个网络号和一个 MAC 地址唯一确定。在大多数情况下，一个物理设备就是一个 BACnet 设备，例如一个支持 BACnet 协议通信的温度传感器就是一个 BACnet 设备。但是也可能有一个物理设备具有多个“虚拟的” BACnet 设备的功能，在 BACnet 标准的附件 H 中对此进行了详细规范。

当一个 BACnet 设备中的应用程序需要与网络中其它 BACnet 设备中的应用程序进行通信时，应用程序只需通过调用 API 访问本地的 BACnet 用户单元来实现。例如，一个 BACnet 设备的应用程序要向一个远地设备的应用程序发送一个请求服务信息，它调用 API，并将相应的参数填入 API 中。API 中的某些参数，如服务请求接收设备的标志号（或地址）、协议控制信息等，将直接下载到网络层或数据链路层；其余参数则组成一个应用层服务原语，通过 BACnet 用户单元传到 BACnet 应用服务单元（ASE），形成应用层协议数据单元（APDU）。APDU 则通过网络层的服务访问点（NSAP）下载到网络层，成为网络层服务原语的数据部分。这个请求将进一步下载到本地设备协议栈中的下层，最终由物理层传送到远地设备，并通过远地设备协议栈逐级上传到远地用户单元。从远地设备看起来，指示原语似乎是直接从它自己的 BACnet 应用服务单元传到其 BACnet 用户单元的。同样，任何从远地设备发回的响应，也是以相同方式回传给请求设备。

BACnet 应用层协议包含了 OSI 模型中的应用层到传输层中的相应内容，所以除了应用层服务的功能外，还要有端到端可靠传输的功能。因此，BACnet 应用层规范就是为了保证 BACnet 设备的应用程序能够与网络中远地 BACnet 设备的应用程序进行端到端可靠通信而制定的一组规则，其主要内容包括：BACnet 应用层提供的服务类型，上下层之间交换的接口控制信息，和对等层协议数据单元的传输机制。

## § 2.2 BACnet 应用层服务类型

BACnet 的应用层提供两种类型的服务，分别是“证实服务”和“非证实服务”。在 BACnet 中，两个对等应用进程间的信息交换，根据 ISO 的服务惯例，被表示成抽象的服务原语的交换。BACnet 定义了四种服务原语：请求（Request）、指示（Indication）、响应（Response）以及证实（Confirm）原语，可以用来传递某些特定的服务参数。而包含这些原语的信息，又是由标准中定义的各种协议数据单元（PDU）来传递的。下面列出各种服务原语：

CONF\_SERV.response CONF\_SERV. Confirm CONF\_SERV. Request CONF\_SERV.  
indication

UNCONF\_SERV.request UNCONF\_SERV. indication

SEGMENT\_ACK.request SEGMENT\_ACK. request

ERROR.request ERROR. indication

REJECT.request REJECT. indication

ABORT.request ABORT. indication

CONF\_SERV 的标识表明使用的是 BACnet 证实服务 PDU。UNCONF\_SERV、SEGMENT\_ACK、ERROR、REJECT 和 ABOUT，分别表明使用的是非证实服务 PDU、分段回应 PDU、出错 PDU、拒绝 PDU 和放弃 PDU，后面这些都是非证实服务类型。

证实服务是建立在客户/服务器通信模型的基础上的，客户端通过某个服务请求实例，

向服务器请求服务，而服务器则通过响应请求来为客户端提供服务，如图 2-2 所示。在交互过程中，担当客户角色的 BACnet 用户，称为请求方 BACnet 用户；担当服务器角色的 BACnet 用户，称为响应方 BACnet 用户。

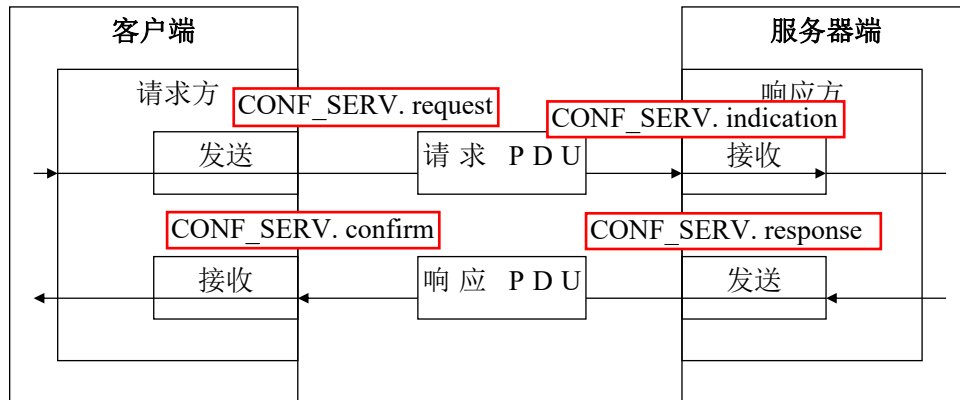


图 2-2 客户与服务器的关系

证实服务的具体过程如下：由请求方 BACnet 用户发出的一个 CONF\_SERV. request 原语，形成请求 PDU 发送给响应方 BACnet 用户。当该请求 PDU 到达响应方 BACnet 用户时，响应方 BACnet 用户则收到一个 CONF\_SERV. indication 原语。同样，由响应方 BACnet 用户发出的一个 CONF\_SERV. response 原语，形成响应 PDU 回传给请求方 BACnet 用户。当响应 PDU 到达请求方 BACnet 用户时，请求方 BACnet 用户则收到一个 CONF\_SERV. CONF\_SERV. confirm 原语。因此，整个过程中请求方 BACnet 用户和响应方 BACnet 用户都要接收和发送 PDU。

在非证实服务中，不存在上述客户/服务器模型、“请求方 BACnet 用户”和“响应方 BACnet 用户”等概念，只有“发送方 BACnet 用户”和“接收方 BACnet 用户”。前者指的是发送 PDU 的 BACnet 用户，后者指的是当一个 PDU 到达时，接收到一个指示（indication）或证实（confirm）的 BACnet 用户。图 2-3 为正常的证实服务报文传递的示意图，图 2-4 为正常的非证实服务报文传递的示意图。

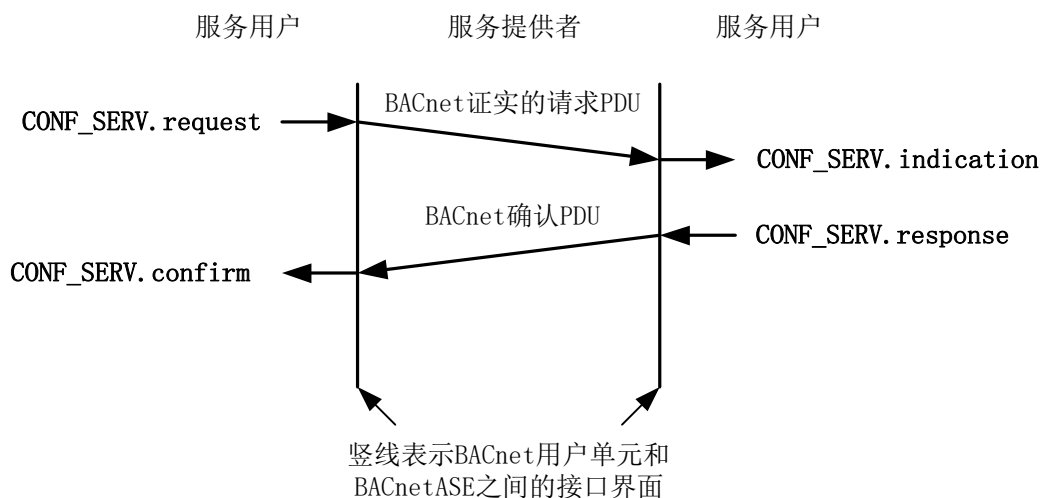


图 2-3 正常的证实服务报文传递时序图

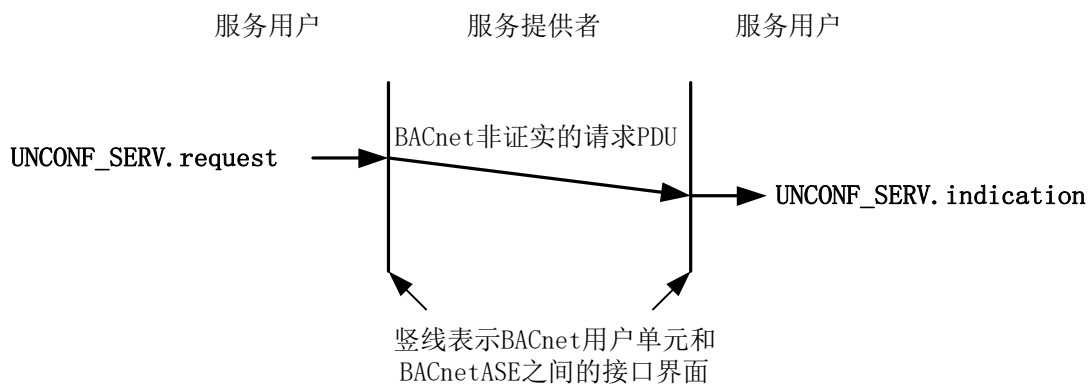


图 2-4 正常的非证实服务报文传递时序图

## § 2.3 BACnet 应用层报文分析

### 2.3.1 应用层接口控制信息

除了服务原语和服务参数外，应用实体还通过 API 与应用程序交换各种接口控制信息（ICI）参数，其具体内容取决于服务原语的类型。应用实体接收到的 ICI 参数将下传到下面各层，以便于各层 PDU 的构建。而应用实体回传给应用程序的 ICI 参数，则包含了其以下各层从各自的 PDU 中得到的信息。

通过 API 与各种服务原语交换信息的 ICI 参数包括：

1. “目的地址”（DA:）：将要接收服务原语设备的地址。其格式（如设备名称、网络地址等）只与本地有关。这个地址也可以是多播地址、本地广播地址或全局广播地址类型。
2. “源地址”（SA:）：发送服务原语的设备的地址。其格式只与本地有关。
3. “网络优先权”（NP:）：表示网络优先权的参数。
4. “需回复数据”（DER:）：一个逻辑值参数，用来指明某个服务是否需要一个回复服务原语来确认。

### 2.3.2 应用层协议数据单元的编码

在 BACnet 中，使用应用层协议数据单元(APDU)来传递包含在应用服务原语和相应的参数中的信息。BACnet 选择 ISO Standard 8824 规范中的方法来表征 BACnet 服务的数据内容。并且，BACnet 规定了 APDU 的编码内容，这些编码内容在 BACnet 标准中的有关章节中进行了详细的描述。

BACnet 的 APDU 由协议控制信息(PCI)和用户数据两部分组成。PCI 中包含进行应用层协议操作所需要的数据，这些数据包括：APDU 的类型，匹配服务请求和服务响应的信息，执行分段报文重组的信息。这些信息包含在报文的头部，也称为 APDU 的固定部分。用户数据中包含每种服务请求和服务响应的具体信息，这部分也称为 APDU 的可变部分。

### 2.3.3 BACnet 报文的分段

为了实现长报文（长度大于通信网络、收/发设备所支持的长度）的传输，有必要对报文进行分段。在 BACnet 体系结构中，不存在单独的传输层，因此报文分段不是由传输层实现，而是由应用层来完成。并且，在 BACnet 中只有 Confirmed-Request 和 Complex-ACK 报文可能需要分段，因此分段还是 BACnet 的一个可选特性。

#### 1. 报文分段的原则

每个由 BACnet 报文编码而成的数据流序列，按下面规则进行分段，然后再在网上传输。

- ① 一个完整的报文尽可能作为一个 APDU 发送。
- ② 当一个完整的报文不可能作为一个 APDU 发送时，则应分段成最少个数的多个 APDU 发送。
- ③ 一个报文分段的长度（以 bit 为单位）应是 8 的整数倍，即对报文进行分段时，字节是最小的分割单位。

#### 2. BACnet APDU 最大长度的确定

在 BACnet 中，APDU 的长度也是没有固定的，而是定义了一个确定 APDU 最大长度的原则，即 APDU 最大长度应是以下长度值中的最小值：

- ① 设备所能发送的 APDU 的最大长度。一般与本地设备的缓冲区大小等本地因素有关。
- ② BACnet 网际网所能传输到远地设备的 APDU 的最大长度。一般由本地、远地，以及中间传输网络的数据链路所决定。
- ③ 远地设备所能接收的 APDU 的最大长度，其值不能小于 50 个字节。

#### 3. 与分段有关的协议控制信息（PCI）

为了支持报文分段，BACnet 协议在 BACnet-Confirmed-Request-PDU 和 BACnet-ComplexACK-PDU 的头部，定义了四个与分段有关的协议控制信息参数。其中两个是布尔型参数，另两个是八位二进制无符号整数。这些参数可以使接收方对到达的分段进行正确的重组，从而保证端到端的可靠传输。

## § 2.4 BACnet APDU 的传输

BACnet 的 APDU 收发协议的详细细节，包含在 BACnet 复杂的事务状态机制（TSM: Transaction State Machine）中，以下的讨论旨在对几种主要 APDU 的传输过程有整体的认识。

### 2.4.1 证实请求报文的传输

客户端设备在传输了一个完整未分段的证实请求报文（Confirmed-Request Message）后，或在等待接收分段证实请求报文最后一个分段所对应的确认信息时，将启动一个计时器。该计时器用来计量对请求报文回应的时间。一旦收到了针对该请求报文所发的出错 APDU、拒绝 APDU、放弃 APDU、简单回应 APDU 或复杂回应 APDU，则停止计时，同时通知客户应用程序。如果计时器的时间值超出了客户设备对象的 APDU\_TimeOut 属性值，则整个报文重新发送，计时器重新计时。所有报文的超时重传均按此过程进行，直至重传次数超

出了客户端设备对象“APDU 重传次数”属性所规定的次数。若超出规定值仍未收到响应，该报文将被丢弃，同时通知客户应用程序。

## 2.4.2 分段证实请求报文的传输

客户端设备在发送分段证实请求（Segmented Confirmed-Request Message）PDU 的第一个分段之前，首先选择一个预设窗口值，以表示它在收到一个分段回应之前，一次准备发送的报文分段最大个数。它通常由报文分段的“建议窗口尺寸”参数表示，取值范围为 1 至 127，在该处其具体取值只与客户端有关。在传输完第一个分段后，客户端设备将启动一个计时器，用来计量对报文分段回应的时间。一旦收到了针对该报文分段所发的拒绝 APDU、放弃 APDU 或分组回应 APDU，则停止计时，同时通知客户应用程序。如果计时器的时间值超出了客户设备对象的 APDU\_Segment\_TimeOut 属性值，则这个分段将重新发送，计时器重新计时。所有报文分段的超时重传均按此过程进行，直至重传次数超出了客户端设备对象中“APDU 重传次数”属性所规定的次数。若超出规定值仍未收到响应，该报文将被丢弃，同时通知客户应用程序。

当服务端设备收到分段证实请求 PDU 的第一个分段后，将会选择一个实际窗口值，以表示它在发送一个分段回应前，一次准备接收的报文分段最大个数。同样，该值的取值范围也规定在 1 至 127 之间，同时它还不能大于证实请求 PDU 中的预设窗口值，在该处其具体取值只与服务器端有关。

在收到第一个分组回应 APDU 后，客户端设备从中得到服务器端设备的实际窗口值，并将该值设置成它的实际窗口值。这样，客户端设备和服务器端设备的实际窗口值大小一致。客户端便可以在收到一个分段回应 APDU 之前，一次发送多个分段；服务器端也可以在发送一个分段回应 APDU 之前，一次接收多个分段。客户端发送完整个报文或发送了窗口值个数的多个分段后，将启动一个计时器，用来计量对这些报文分段回应的时间。一旦收到了针对这些报文分段所发的拒绝 APDU、放弃 APDU 或分组回应 APDU，则停止计时。如果计时器的时间值超出了客户设备对象的 APDU\_Segment\_TimeOut 属性值，则这些分段将重新发送，计时器重新计时。所有报文分段的超时重传均按此过程进行，直至重传次数超出了客户端设备对象中“APDU 重传次数”属性所规定的次数。若超出规定值仍未收到响应，该报文将被丢弃，同时通知客户应用程序。

客户端在发送分段的过程中，可能会收到拒绝 APDU、放弃 APDU 或分段回应 APDU。在这种情况下，收到拒绝 APDU 或放弃 APDU 将会中止请求的传输；收到分段回应 APDU，将会作为序号等于或小于该 APDU 中分段数参数值的所有分段的确认，而那些没有被确认的分段将按上述过程重传。

## 2.4.3 分段复杂回应报文的传输

分段复杂回应报文（Segmented ComplexACK Message）的传输过程与分段证实请求报文的传输过程相类似，主要不同之处在于：

- ① 在分段复杂回应报文的传输过程中，由服务器端设备发送复杂回应报文的分段，由客户端设备接收并发送分段回应 APDU
- ② 在分段复杂回应报文的传输过程中，客户端设备只能回应放弃 APDU 或分段回应 APDU，而不能回应拒绝 APDU。



## 2.4.4 分段回应 APDU 的传输

分段回应 APDU 是分段接收方设备用来回应发送方的信息。在以下四种情况下，设备需传输一个 SegmentACK。

- ① 设备收到报文的第一个分段。
- ② 设备收到未确认的、有序的、数量为实际窗口值的多个报文分段构成的序列。
- ③ 设备收到一个乱序分段报文（可能表明丢失了某个分段）。
- ④ 设备收到报文的最后一个分段。

## § 2.5 与传输有关的其它问题

### 2.5.1 事务状态机制的中止

在一个证实请求的服务过程中，客户端与服务器端都将创立各自的事务状态机制，以便针对各种情况分别进行处理。该事务状态机制的终止由一些条件所决定。

对于客户端，当出现以下几种情况时，事务处理终止，同时结束该事务状态机制。

- ① 当收到服务器端设备发来的简单回应、不分段复杂回应、出错、拒绝或放弃 APDU 时。
- ② 收到服务器发来的分段复杂回应 APDU 的最后一个分段，并发送了相应的分段回应 APDU 后。
- ③ 当超时重传次数用尽后。
- ④ 在向服务器发送了包含该事务处理过程标志符的放弃 APDU 后。

对于服务器端当出现以下几种情况时，将终止事务处理，同时结束该事务状态机制。

- ① 当向客户端设备发送完简单回应、不分段复杂回应、出错、拒绝或放弃 APDU 后。
- ② 当收到客户端设备发来的针对分段复杂回应 APDU 的最后一个分段的回应 APDU 后。
- ③ 当接收到客户端发来的包含该事务处理过程标志符的放弃 APDU 后。
- ④ 在传输一个分段复杂回应 APDU 的过程中，超时重传次数达到规定值仍未成功时。

### 2.5.2 重复报文的处理

在一个事务处理过程中，由于使用了 BACnet 的出错重传机制，设备不可避免的会接收到重复的报文或报文分段。对此，BACnet 协议中是按以下各种可能出现的情况分别处理的。

① 服务器接收到一个重复的证实请求报文。这时，如果服务器具有识别重复证实请求报文的能力，则该重复报文将被服务器丢弃。否则，服务器仍会响应这个重复的证实请求报文。这样的话，客户端应当根据响应中的标志符不与任何一个当前的事务状态机制绑定，来忽略该重复响应。

② 服务器接收到一个重复的证实请求报文分段，即已经收到该分段并发送了分段确认。

在这种情况下，服务器应忽略该重复分段并回传一个适当的分段回应 APDU。判断分段是否重复的依据是：任何一个分段都可以由其对等方地址、标志符以及分段序号唯一确定。

③ 客户端接收到一个重复的复杂回应分段，即该分段已经收到并确认了。客户端应忽略该重复分段并回传一个适当的分段回应 APDU。

④ 设备接收到一个重复的分段确认 APDU。这时，该设备应忽略重复的分段确认 APDU。

### 2.5.3 资源的回收

上述 BACnet 的出错重传过程，其具体实现需要客户和服务器两端提供一定的资源。这些资源通常是事务处理的各个细节，包括事务状态机制(TSM)、计时器以及 APDU 或 APDU 分段缓冲区等。当出错重传过程失败时，这些相关的资源也变得失效，应被释放掉。资源释放的具体细节取决于系统的具体设计。作为建议，BACnet 协议给出了资源失效而应释放的依据：

- ① 客户端收到对一个证实请求 APDU 的完整响应后。
- ② 在客户端，当一个证实请求 APDU 被重发了“APDU 重发次数”属性所规定的次数，但仍未成功时。
- ③ 在客户端，当一个证实请求 APDU 分段被重发了“APDU 重发次数”属性所规定的次数，但仍未成功时。
- ④ 在服务器端，当发送了对某个证实请求 APDU 的响应并收到相应的分段回应后。

## 第 3 章 BACnet 网络层规范

本章介绍 BACnet 协议网络层的原理和运行机制,包括 BACnet 网络层的功能、主要的服务原语以及网络层报文的结构,并简要介绍 BACnet 路由器的运行规程。

### § 3.1 BACnet 网络层规范的内容

BACnet 网络层的目的是提供一种方法,使用这种方法,不用考虑网络所使用的 BACnet 数据链路技术,可以将报文从一个 BACnet 网络传递到另一个 BACnet 网络。数据链路层提供将报文在本局域网内传递到某个设备或者广播到所有设备的能力,而网络层则提供将报文直接传递到一个远程的 BACnet 设备、广播到一个远程 BACnet 网络、或者广播到所有的 BACnet 网络中的所有 BACnet 设备的能力。一个 BACnet 设备被一个网络号码和一个 MAC 地址唯一确定。

我们将那些使用不同的数据链路层技术的局域网称为异类网络,例如,以太网、ARCNET 网络和 Lonworks 网络等就是异类网络。网络层的功能就是实现连接两个异类的 BACnet 局域网。实现异类网络连接的设备称为“BACnet 路由器”。从协议的观点看,网络层的功能是向应用层提供同一的网络服务平台,屏蔽异类网络的差异。同时,BACnet 网络层协议也建立路由器建立和维护它们的路由表的方法,这将使得路由器自动配置和报文在路由器之间的流动成为可能。

#### 3.1.1 BACnet 网络层的服务原语

BACnet 网络层向应用层提供的服务是不确认的无连接形式的数据单元传送服务。与这种交互相关的原语是 N-UNITDATA 请求和指示,其参数如下:

N-UNITDATA.request (destination\_address, data, network\_priority, data\_expecting\_reply)  
N-UNITDATA.indication (source\_address, destination\_address, data, network\_priority,  
data\_expecting\_reply)

“目标地址”和“源地址”参数提供下列事物的逻辑连续配置:1)一个可选择的网络号码,2)适合于下层 LAN 技术的 MAC 地址,3)链路服务接入点。网络号码 X ‘FFFF’表示此报文广播到目前能够到达的所有网络的所有设备。目前能够到达的网络是指那些在 BACnet 互联网中已经具有一条有效连接的网络。“数据”参数是从应用层传递过来的网络服务数据单元(NSDU),其中包含一个完全编码的 BACnet APDU。“网络优先级”参数是一个数字值,由 BACnet 路由器中的网络层用来确定任何可能的优先于先进先出排队等待规则的情况。“data\_expecting\_reply”参数指出对于正在传送的数据单元是否期待有一个应答的数据单元。

当网络层从应用层收到一个 N-UNITDATA.request 请求原语后,就用网络层规范所表述的方式发送一个网络层服务数据单元 NSDU。当一个网络实体收到从一个对等网络实体发来的 NSDU 后,它作如下处理:1)通过一个直接连接的网络将 NSDU 发送到目的地,2)将 NSDU 发送到下一个 BACnet 路由器后再路由到目的地,3)如果 NSDU 的地址与它自己的应用层中的某个实体的地址匹配,则向这个实体发送一个 N-UNITDATA.indication 原语,通知有一个 NSDU 到达。

### 3.1.2 BACnet 网络层 PDU 结构

图 3-1 给出了 BACnet 网络层协议数据单元的分组格式。下面对相应的域进行说明：

版本	1个字节
控制	1个字节
DNET	2个字节
DLEN	1个字节
DADR	可变字节
SNET	2个字节
SLEN	1个字节
SADR	可变字节
Hop Count	1个字节
网络层报文类型	1个字节
Vendor ID	2个字节
APDU	N个字节

图 3-1 BACnet 网络层协议数据单元格式

#### 1. 协议版本号

每个 NPDU 的第一个字节是一个 8 比特的无符号整数，标识 BACnet 协议的版本号。  
目前的 BACnet 协议的版本号是(1)。

#### 2. 网络层协议控制信息

NPDU 的第二个字节是控制字节，表示后面的某个特殊 NPCI 域的存在。控制字节中每个比特的作用如下：

比特位	意义	比特值	比特值的含义
比特 7	标志报文类型	0	表示 NPDU 传送的是一个包含 BACnet APDU 的数据报文，报文类型域不存在。
		1	表示 NPDU 传送的是一个网络层报文，报文类型域存在。
比特 6	保留	0	目前置 0。
比特 5	目标指示器	0	DNET, DLEN, DADR, Hop Count 不存在
		1	DNET, DLEN, Hop Count 存在 DLEN = 0 表示广播 MAC，DADR 不存在 DLEN > 0 规定了 DADR 域的长度
比特 4	保留	0	目前置为 0。
比特 3:	源指示器	0	SNET, SLEN, SADR 不存在
		1	SNET, SLEN, SADR 存在 SLEN = 0 无效 SLEN > 0 规定了 SADR 域的长度
比特 2	N-UNITDATA 中的 data_expect_reply 参数	0	存在一个网络层报文期待的应答 (除 BACnet-Confirmed-Request-PDU, BACnet-ComplexACK-PDU 段外)。
		1	存在一个 BACnet-Confirmed-Request-PDU，一个 BACnet-ComplexACK-PDU 段，或者一个网络层报文期待的应答。
比特 1, 0	网络优先级	11	关于楼宇安全性的报文。
		10	关于楼宇关键设备的报文。
		01	紧急报文。
		00	一般报文。

### 3. 特殊域的内容

DNET: 最终目标网络号, 2 个字节。

DLEN: 最终目标的 MAC 层地址的长度, 1 个字节, 0 表示对目标网络的广播。

DADR: 最终目标的 MAC 层地址。

SNET: 初始源网络号, 2 个字节。

SLen: 初始源的 MAC 层地址的长度, 1 个字节。

SADR: 初始源的 MAC 层地址。

Hop Count: 递减计数器值, 用来防止报文不被循环路由。1 个字节, 初始化为 X 'FF'。当报文通过每个路由器时, 其值被至少减一。如果路由器发现该值已为 0, 则丢弃此报文。

### 4. 网络层报文类型

如果控制域中的比特 7 为 1, 这表示此报文是一个网络层报文, 其报文类型域存在。这是个 1 字节的域, 其内容表示报文携带的各种网络层的控制信息。

### 5. 生产商专有网络层报文

如果控制域的比特 7 为 1 和报文类型域的值在 X '80' 至 X 'FF' 时, Vendor ID 域存在, 生产商可以有 2 个字节来编码自己的专有网络层报文类型。

## 3.1.3 多播报文和广播报文

BACnet 使用多播地址和广播地址来支持多个目标的报文传输。多播是指一个报文被传送给一组目标设备, 而广播是指一个报文被传送给某个局域网中的所有设备、一个远程网络中的所有设备、或者所有 BACnet 网络中的所有设备。BACnet 网络层处理两种报文, 一种是包含有 APDU 的数据报文, 另一种是关于网络层本身控制信息的网络层协议报文。对于数据报文, 只有 BACnet 非证实请求协议数据单元(BACnet-Unconfirmed-Request-PDU)的报文可以被多播或广播。而网络层协议报文都可以被多播或广播, 使用多播地址或者广播地址进行。

## 3.1.4 网络层协议报文

在 BACnet 中, 有十种网络层协议报文, 它们的作用是进行路由器自动配置, 路由表的维护, 和网络层拥塞控制。下面介绍这十种报文。

### 1. Who-Is-Router-To-Network 报文

格式为: 网络报文类型域是 X '00', 后面有 2 个字节的网络号。作用是: ①节点用来确定通达某目标网络的下一个路由器; ②帮助路由器更新路由表。当省略 2 字节的网络号时, 接收此报文的路由器要返回其所有可通达的目标网络的列表。

### 2. I-Am-Router-To-Network 报文

格式为: 网络报文类型域是 X '01', 后面有 2 个字节的网络号。作用是列出通过发送此报文的路由器可以到达的网络号。

### 3. I-Could-Be-Router-To-Network 报文

格式为: 网络报文类型域是 X '02', 后面有 2 个字节的网络号和 1 个字节的性能指标。作用是响应包含有特定网络号的 Who-Is-Router-To-Network 报文, 由能够建立到达特定目标网络的点到点连接的半路由器使用, 其网络号就是所响应的报文中包含的特定网络的网络号。性能指标表明这种连接的质量。

### 4. Reject-Message-To-Network 报文

格式为: 网络报文类型域是 X '03', 后面有 1 个字节的原因说明和 2 个字节的网络号。

作用是一个拒绝报文，直接发给生成被拒绝的报文的节点，网络号就是被拒绝报文中的网络号。在拒绝原因字节中是一个无符号的整数，其值所表示的意义如下：

(0): 其它差错。

(1): 本路由器不能直接连接到所指示的目标网络以及不能发现任何一个能够连接到所指示的目标网络。

(2): 本路由器忙，目前不能接收关于所指示目标网络的报文。

(3): 这是一个不可识别的网络层报文类型。

(4): 报文太长，不能路由到所指示的目标网络。

#### 5. Router-Busy-To-Network 报文

格式为：网络报文类型域是 X ‘04’，后面是可选的 2 个字节的网络号。作用是被路由器用来通知停止接收通过本路由器向某特定目标网络或者所有网络发送的报文。此报文通常用广播 MAC 地址发向相应的网络。如果没有可选的 2 个字节的网络号，则表示到所有网络的报文都不接收。

#### 6. Router-Available-To-Network 报文

格式为：网络报文类型域是 X ‘05’，后面是可选的 2 个字节的网络号。作用是被路由器用来通知开始或者重新开始接收通过本路由器向某特定目标网络或者所有网络发送的报文。此报文通常用广播 MAC 地址发向相应的网络。如果没有可选的 2 个字节的网络号，则表示到所有网络的报文都可接收。

#### 7. Initialize-Router-Table 报文

格式为：网络报文类型域是 X ‘06’。作用是初始化一个路由器的路由表或者查询当前路由表的内容。此报文有一个数据段，包含有初始化路由表的信息。

#### 8. Initialize-Router-Table-Ack 报文

格式为：网络报文类型域是 X ‘07’。作用是对初始化路由表报文的应答，表示路由器的路由表已经改变，或者已被查询。此报文的数据段具有与它应答的初始化路由表报文相同的格式。

#### 9. Establish-Connection-To-Network 报文

格式为：网络报文类型域是 X ‘08’，后面有 2 个字节的网络号和 1 个字节的“中止时间值”。作用是命令一个半路由器创建一个通达指定网络的点到点连接。2 个字节的网络号指出要半路由器连接的目标网络。1 个字节的“中止时间值”规定了在没有 NPDU 到达的情况下，连接保留的时间。当此值为 0 时，表示连接永久保留。

#### 10. Disconnect-Connection-To-Network 报文

格式为：网络报文类型域是 X ‘09’，后面有 2 个字节的网络号。作用是命令一个路由器释放所建立的点到点连接。

### 3.1.5 网络层协议运行规程

本节介绍 BACnet 路由器和节点进行本地和远程数据传输所遵循的网络层协议运行规程。所谓“本地”是指源设备和目标设备都在同一个 BACnet 网络中，而所谓“远程”是指源设备和目标设备分处不同的 BACnet 网络之中。

#### 1. 本地数据发送的网络层协议规程

当网络层实体收到来自应用层的一个 N-UNITDATA.request 原语时，它先检查“目标地址”参数中的 DNET 字段。如果不存在此字段，表明目标设备与本身源设备位于同一个 BACnet 网络中。在 NPCI 控制字节中应该包含有“网络优先级”参数的值和指明不存在 DNET、DADR、Hop Count、SNET 和 SADR 的字节。NPCI 加在 N-UNITDATA.request 原

语中的“数据”参数（就是 NSDU）的前面，形成 NPDU，传送给数据链路层，作为数据链路层原语中的“数据”参数。同时向数据链路层发送一个 DL-UNITDATA 数据链路请求原语。

## 2. 接收本地数据的网络层协议规程

当网络层实体收到来自数据链路层的一个 NPDU 时，它先检查第二个字节，这是控制 NPCI。如果此字节的比特 7 为值“0”，表示此报文中包含有 APDU。否则，比特 7 的值为“1”时，这表明此报文是网络层报文。对于两种类型的报文，其处理方式不同。①对于 APDU 报文，当不存在 DNET 域或者存在 DNET 域而同时包含有全球广播地址 X ‘FFFF’ 时，网络实体查找 BACnet 应用层实体。如果网络实体找到相应的应用层实体，就将来自于数据链路层的报文中的 NPCI 部分去掉，将其后的作为“数据”参数的部分作为一个 N-UNITDATA.indication 原语传送给应用层实体。如果网络层实体不能找到相应的应用层实体并且网络层实体本身位于非路由器节点，则丢弃此报文。当存在 DNET 域且不是全球广播地址 X ‘FFFF’ 时，非路由器节点中的网络层实体丢弃此报文，路由器中的网络层实体的行为在后面介绍。②对于本地网络层报文，当不存在 DNET 域或者存在 DNET 域而同时包含有全球广播地址 X ‘FFFF’ 时，网络层实体解读此报文。如果报文不可解读，就向源设备发送一个 Reject-Message-To-Network 报文。当存在 DNET 域且不是全球广播地址 X ‘FFFF’ 时，非路由器节点中的网络层实体丢弃此报文，路由器中的网络层实体的行为在后面介绍。

## 3. 远程数据发送的网络层协议规程

当网络层实体收到来自应用层的一个 N-UNITDATA.request 原语时，它先检查“目标地址”参数中的 DNET 字段。如果存在此字段，表明目标设备位于与本身源设备不同的 BACnet 网络中。在 NPCI 控制字节中指明存在 DNET、DADR、Hop Count 域，但是不存在 SNET 和 SADR 域。在“网络优先级”域中，网络层实体填入提供的参数。接着填写相应的地址域。NPCI 加在 N-UNITDATA.request 原语中的“数据”参数（就是 NSDU）的前面，形成 NPDU，传送给数据链路层，作为数据链路层原语中的“数据”参数。同时向数据链路层发送一个 DL-UNITDATA 数据链路请求原语。传递到数据链路层的“目标地址”参数的 DA 段应该是对应 DNET 参数的 BACnet 路由器的 MAC 地址，或者如果不知道路由器 MAC 地址，此段就是一个广播地址。当然，如果 DNET 是全球广播网络号，DA 也是广播地址。

对于某个特定的 DNET，有四种建立相应 BACnet 路由器地址的方法。分别是：①在配置设备时人工设定。②通过发送一个 Who-Is 请求报文，并且读取应答的 I-Am 报文中的“源地址”SA 段而得到。③使用网络层报文 Who-Is-Router-To-Network 来获得。④向一个远程 DNET 上的设备发送具有本地广播 MAC 地址的报文，然后读取远程设备的响应报文中的 SA 而获得。

## 4. 接收远程数据的网络层协议规程

当网络层实体收到来自数据链路层的一个 NPDU 时，它先检查第二个字节，这是控制 NPCI。对于非路由器的 BACnet 设备中的网络层实体，如果发现此字节表示存在 DNET 域且其值不为 X ‘FFFF’，则丢弃此报文。对于路由器中的网络层实体，如果发现此字节表示存在 DNET 域，则根据其优先级将此报文置于它的报文队列中。在相同优先级时，报文按先进先出的顺序排队。如果 NPCI 的控制字节表示 NPDU 包含一个网络层报文，则网络层实体还需进一步查看“报文类型”域。如果此域表示存在一个 Reject-Message-To-Network 报文，则网络层实体要执行专门的针对此报文的规程。如果存在 SNET 和 SADR 域，表示报文来自一个对等的路由器；而如果不存在 SNET 和 SADR 域，表示报文来自于与路由器直接连接的网络。对于后一种情况，路由器根据路由表所示的报文来自网络的网络号，将

SNET 和 SADR 添加到 NPCI 中。SADR 域设置成等于到达报文的 SA。

存在三种可能性：①收到报文的路由器直接与 DNET 所指示的网络相连接，则网络层实体去掉 NPCI 中的 DNET、DADR 和 Hop Count 域，将 DA 设置为等于 DADR，然后将报文直接发送给目标设备。②收到报文的路由器不直接与 DNET 所指示的网络相连接，网络层实体先将报文的 Hop Count 域的值减 1，如果此值仍然大于 0，就将报文沿着目标网络方向传给下一站路由器。如果不知道下一站路由器的位置，就发送一个 Who-Is-Router-To-Network 报文来确定其位置。如果 Hop Count 域值为 0，则丢弃此报文。③DNET 表示的是全球广播网络号并且 Hop Count 域的值大于 0，收到报文的路由器使用适合于每种数据链路的广播地址，向除了报文来自于的网络以外的所有连接的网络广播此报文。如果 Hop Count 域的值为 0，则丢弃此报文。

## § 3.2 BACnet 路由器

我们将连接两个或者多个 BACnet 网络从而形成 BACnet 互联网的设备称为 BACnet 路由器。在 BACnet 路由器中可以有 BACnet 应用层功能，也可以没有此功能。BACnet 路由器使用 BACnet 网络层协议报文来维护路由表。以下介绍 BACnet 路由器运行规程。

### 1. 路由表

路由器是连接至少两个 BACnet 网络的设备，在路由器中将每个连接处称为一个“端口”。路由表中包含端口的下列项目：①此端口所连接的网络的 MAC 地址；②2 个字节的关于所连接网络的网络号；③通过此端口可通达网络的网络号列表每个这些网络的可通达的状态。

### 2. 启动规程

路由器在启动时，向每个端口广播一个 I-Am-Router-To-Network 报文，其中包含有每个可通达网络的网络号。这使其它路由器可以根据报文内容建立或者更新其路由表中的条目。

### 3. 路由器的运行

图 3-2 给出了路由器运行的流程图。



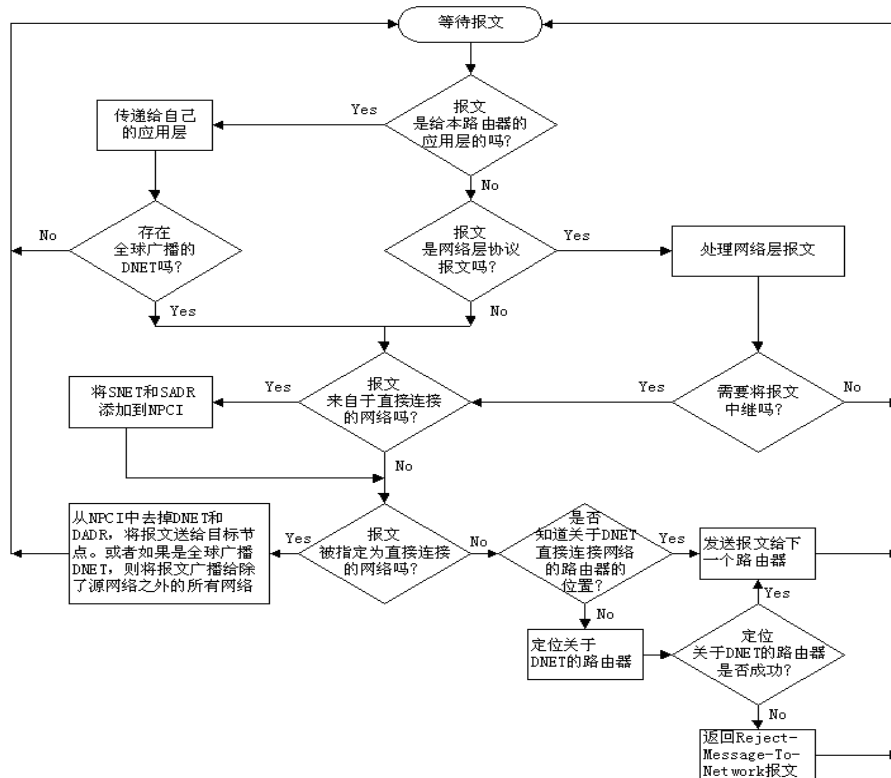


图 3-2 BACnet 网络路由器运行流程图

#### 4. 路由器流量控制

在路由器接收报文时，如果流量大于它的处理速度，其缓存器可能会溢出，这将造成数据的丢失。路由器要有一种功能，当它的缓存器将要溢出时，它能够通知源设备暂停发送数据或者放慢发送的速度。在 BACnet 网络中，路由器使用 Router-Busy-To-Network 报文和 Router-Available-To-Network 报文来实现流量控制的功能。

### § 3.3 点到点半路由器

在 BACnet 网络中，将两个网络通过广域网（例如公共电话网络）进行连接的设备是半路由器。半路由器创建路由和同步路由的规程与路由器的不相同。点到点连接总是需要在两个半路由器之间建立连接从而形成一个完整的路由器，图 3 表示了点到点连接的示意图。

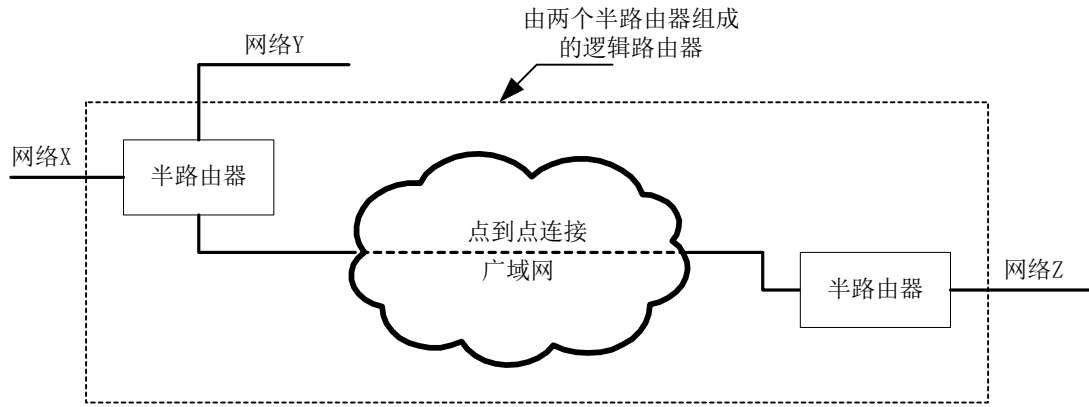


图 3-3 由两个半路由器组成的点到点连接

在 BACnet 的标志规范中，定义了 5 个网络层报文，用于点到点半路由器建立链路、中止链路和路由学习功能等。I-Could-Be-Router-To-Network 报文是半路由器用来通知网络该设备能够建立到所请求的网络的连接，但是目前还没有建立此连接。Establish-Connection-To-Network 报文用来请求半路由器建立一个连接。Disconnect-Connection-To-Network 报文请求中止一个连接。Initialize-Router-Table 和 Initialize-Router-Table-ACK 报文用来进行路由器的初始化工作，然后，不论是否有活动的点到点连接存在，半路由器都使用与其它活动路由器相同的规程来维护其路由表。

总之，BACnet 网络层向应用层实体提供了进行网络之间互相通信的同一的平台。BACnet 使用路由器作为连接异类网络的设备，并且对于路由器的运行规程进行了详细的规范，从而保证了 BACnet 网络的成功运行。随着因特网的普及，因特网的网络层规范 IP 协议也成为事实上的标准。ASHRAE 不失时机地制定了 BACnet 标准附件 Annex J，BACnet/IP，将使用 TCP/IP 协议进行通信的设备纳入到 BACnet 网络之中，使得 BACnet 网络可以进行因特网上的全球通信。我们将在后续章节中对 BACnet/IP 予以介绍。

## 第 4 章 BACnet 数据链路/物理层规范

本章介绍 BACnet 的五种数据链路/物理层的规范, 并介绍 BACnet 数据链路/物理层的功能、主要服务原语以及帧结构。

### § 4.1 数据链路/物理层协议的内容

为了保证由通信链路连接的两个计算机设备之间能够可靠和有效地传递数据, 已经发展起来多种技术, 计算机网络中的数据链路层和物理层的协议就是对于如何使用这些技术建立网络的通信链路进行规范。用同一种技术建立起来的通信链路连接的一组计算机设备就称为一个类型的计算机网络。例如, 用载波侦听多路访问/冲突检测技术建立的网络称为以太网; 而用 LonTalk 协议技术建立的网络称为 LonWork 网络。不同技术所建立的网络在数据传输速率、传输的数据帧格式、设备使用介质的方式等等方面都不相同。这些网络之间一般不能直接连接通信。这些技术各有特长, 分别适应不同的应用环境。

BACnet 标准目前将五种类型的数据链路/物理层技术作为自己所支持的数据链路/物理层技术进行规范, 形成其协议。这五种类型的网络分别是: Ethernet(ISO8802-3)局域网, ARCNET 局域网, 主从/令牌传递(MS/TP)局域网, 点到点(PTP)连接, 和 LonTalk 局域网。BACnet 选择这些局域网技术的原因是从实现协议的硬件的可用性、数据传输速率、与楼宇自控系统的兼容性和设计的复杂性等几个方面考虑的。本文分别讨论这些协议规范。

#### 4.1.1 BACnet 的以太网规范

以太网是目前在计算机网络中使用的最普遍的局域网技术, 其协议包括逻辑链路控制协议(LLC), 载波侦听多路访问/冲突检测 (CSMA/CD) 协议和相应的物理介质协议等。BACnet 将 ISO 8802-2 中的 Class I LLC 和类型 1 不确认的无连接模式服务以及 ISO 8802-3 的所有规范, 包括将来的扩展, 作为自己的标准。

##### 1. BACnet 网络对 ISO 8802-2 逻辑链路控制协议(LLC)的使用

BACnet 网络使用 LLC 的数据链路服务来传送 BACnet 链路服务数据单元(LSDU)。一个 LSDU 包含一个 NPDU。使用 ISO 8802-3 局域网技术的 BACnet 设备遵守 LLC Class I 的要求, 提供不确认的无连接服务。同时, 使用 DL-UNITDATA 原语传送 LLC 参数。

##### 2. LLC 原语所要求的参数

DL-UNITDATA 原语中的参数是源地址、目标地址、数据和优先级。源地址和目标地址各自分别是一个 6 字节由网络接口硬件确定的介质访问控制(MAC)地址和 1 字节的链路服务访问点(LSAP)参数组成。LSAP 的值都为 X '82', 表示本 LSDU 内包含有 BACnet 数据。数据参数就是来自网络层的 NPDU。因为 ISO 8802-3 MAC 层运行在只有一个服务类别的单优先级模式下, 所以在此标准中没有优先级参数的规范。

##### 3. MAC 原语所要求的参数

ISO 8802-3 MAC 层原语是 MA-DATA.request 和 MA-DATA.indication。这些是用源节点和目标节点的 MAC 地址封装的 LLC 数据的帧结构, 图 1 是这种帧的数据结构图。其中, APDU 是应用层协议数据单元, NPCI 是网络层协议控制信息。DSAP 和 SSAP 分别是目标节点和源节点的链路服务访问点参数, 在此情况下, 其值都为 X '82', 表示帧内包含有

BACnet 数据。整个帧由物理介质传送到目标节点设备。

#### 4. 物理介质

完全采用 ISO 8802-3 标准及其附件中对物理介质的规范。

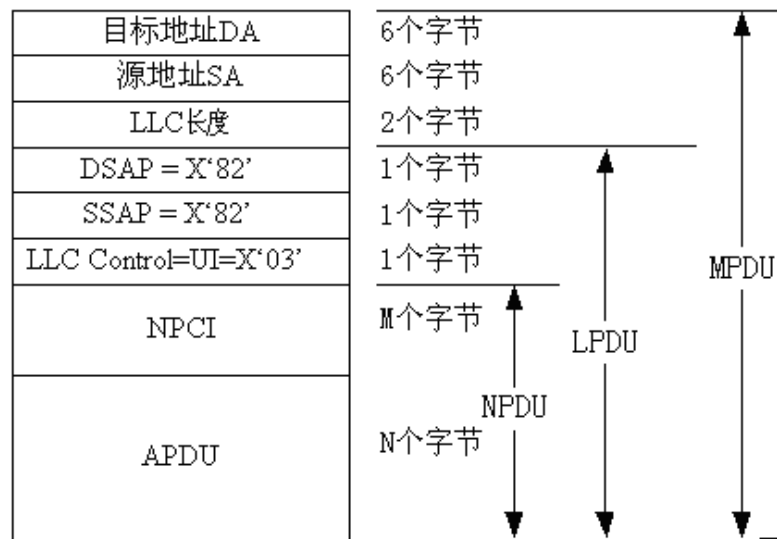


图 4-1 BACnet 的以太网 MPDU 格式

### 4.1.2 BACnet 的 ARCNET 局域网规范

ARCNET 目前是美国国家标准(ATA/ANSI 878.1)。这是一种很成熟的局域网技术，数据传输率为 2.5Mbps。这种网络的特点是使用令牌传递协议作为设备访问介质的方式，因此每个设备可以设置等待发送报文时间的最大值，这对有些应用非常有用。BACnet 将 ATA/ANSI 878.1 ARCNET 局域网标准，包括将来的扩展，作为自己的标准。同时，仍然使用 ISO 8802-2 中的 Class I LLC 和类型 1 不确认的无连接模式服务作为逻辑链路控制协议。

#### 1. LLC 原语所要求的参数

BACnet 网络仍然使用 LLC 的数据链路服务来传送 BACnet 链路服务数据单元(LSDU)。同时，使用 DL-UNITDATA 原语传送 LLC 参数。DL-UNITDATA 原语中的参数是源地址、目标地址、数据和优先级。源地址和目标地址各自分别是一个 1 字节的由网络接口硬件确定的介质访问控制地址，1 字节的链路服务访问点和 1 字节的系统代码(SC)参数组成。LSAP 的值都为 X '82'，表示本 LSDU 内包含有 BACnet 数据。SC 的值为 X 'CD'，表示此数据结构是一个 BACnet 帧。数据参数就是来自网络层的 NPDU。因为 ARCNET MAC 层运行在只有一个服务类别的单优先级模式下，所以在此标准中没有优先级参数的规范。

#### 2. 将 LLC 原语映射到 ARCNET 的 MAC 层

类型 1 不确认的无连接 LLC 服务直接映射成 ARCNET 的 MAC 原语 MA-DATA.request。没有指示原语传递给 LLC 子层，但是从目标 MAC 子层有一个确认返回。ARCNET 不允许其 MSDU 的长度为 253、254 或者 255 字节。长度为 0—252 字节的 BACnet LPDU 作为 ARCNET MPDU 帧的整个 MSDU，其中 MPDU 中具有 1 个字节的信息长度(IL)域。长度为 253—504 字节的 BACnet LPDU 作为 ARCNET MPDU 的 MSDU 的前部分，后面加上 3 个不确定数值的字节，长度达到 256—507 字节，其中 MPDU 中具有 2 个字节的信息长度域。在接收方，如果检测到 ARCNET 的 MPDU 的信息长度域有 2 个字节，则要去掉 MSDU 中的最后 3 个字节。ARCNET 中不能传输长度超过 504 字节的 LPDU。

#### 3. MAC 原语所要求的参数

ARCNET 的 MAC 层原语是 MA-DATA.request、MA-DATA.indication 和

MA-DATA.confirmation。这些是用源节点和目标节点的 MAC 地址封装的 LLC 数据的帧结构，图 2 是这种帧的数据结构图。其中，APDU 是应用层协议数据单元，NPCI 是网络层协议控制信息。DSAP 和 SSAP 分别是目标节点和源节点的链路服务访问点参数，在此情况下，其值都为 X‘82’，表示帧内包含有 BACnet 数据。整个帧由物理介质传送到目标节点设备。

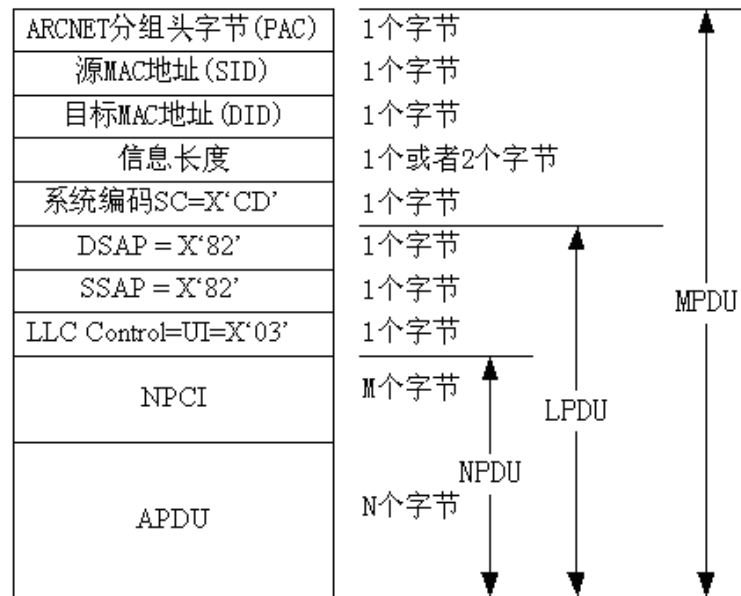


图 4-2 BACnet 的 ARCnet 局域网 MPDU 格式

#### 4. 物理介质

完全采用 ARCNET 标准及其附件中对物理介质的规范。

### 4.1.3 BACnet 的主从/令牌传递(MS/TP)局域网规范

BACnet 的主从/令牌传递局域网技术的基础是使用 EIA-485 标准。EIA-485 标准是电子工业协会开发的物理层的数据通信标准，广泛应用在楼宇设备控制系统中。由于 EIA-485 标准只是一个物理层标准，不能解决设备访问传输介质的问题，BACnet 定义了主从/令牌传递(MS/TP)协议，提供数据链路层功能。

在 MS/TP 网络中有一个或者多个主节点，主节点在逻辑令牌环路中是对等的。每个主节点可以有一些从节点，从节点只有在主节点的请求下才能传送报文。如果网络全部是由主节点组成，就形成一个对等网络。如果网络是由单主节点和所有其它从节点组成，就形成一个纯主从网络。

#### 1. MS/TP 网络工作原理

MS/TP 网络使用一个令牌来控制设备对网络总线的访问。当主节点掌握令牌时，它可以发送数据帧。凡是收到主节点请求报文的主节点和从节点都可以发送响应报文。一个主节点在发送完报文之后，就将令牌传递给下一个主节点。但是，如果主节点有许多报文要发送，当它一次掌握令牌期间最多只能发送  $N_{\max\_info\_frames}$  个数据帧，就必须将令牌传递给下一个主节点，其它数据帧只能在它再一次掌握令牌时，才能发送。传递令牌帧不需确认，但是，发送令牌的节点侦听接收令牌的节点是否开始使用令牌。侦听的方法是在发送完令牌帧的最后一个字节之后的  $T_{usage\_timeout}$  时间内收到  $N_{min\_octets}$  字节。大多数令牌总线型网络都不区分请求帧和响应帧，它们都以相同的方式访问总线，只有掌握令牌的节点可以发送。

由于 MS/TP 网络定义了从节点不能掌握令牌，因此规定所有节点，不论是否握有令牌，都必须对请求报文作出响应。发出请求报文的主节点在收到应答之前不释放令牌。收到请求报文的从节点要立即发回应答报文，而收到请求报文的主节点可以选择发回应答报文或者发送一个“延迟应答”报文，告知它将延迟应答到它自己掌握令牌时再发送。

## 2. 服务规范

MS/TP 网络提供两个数据链路层服务原语，向网络层提供服务，这两个服务原语分别是 DL-UNITDATA.request 和 DL-UNITDATA.indication。前者由网络层传递给 MS/TP 实体，请求使用不确认的无连接方式向一个或者多个远程节点的网络层实体发送一个网络层协议数据单元(NPDU)。后者由 MS/TP 实体传递给网络层，通知有一个来自远程实体的 NPDU 的到达。

## 3. 物理层介质

MS/TP EIA-485 网络使用屏蔽双绞线作为信号传输介质，特征阻抗为 100—130 欧姆。EIA-485 节点有三种类型，分别是：具有网络偏置电阻的节点，具有本地偏置电阻的节点和无偏置电阻的节点。

## 4. 帧格式

MS/TP 网络的帧格式如图 3 所示。帧类型域用来区别不同类型的 MAC 帧。目标地址和源地址都是 1 字节，目标地址域值为 255(X ‘FF’)表示此帧为广播帧，而源地址域的值不允许为 255。地址值 0—127 可用来表示主节点和从节点，而地址值 128—254 只能用来表示从节点。长度域以字节表示数据域的长度。如果长度域的值 0，即两个字节都为 0，则不存在数据域和数据校验域。数据域的长度为 0—501 字节。

前导码	2个字节前导码：X ‘55’，X ‘FF’
帧类型	1个字节
目标地址	1个字节
源地址	1个字节
长度	2个字节
帧头校验	1个字节
数据	0-501个字节，只在“长度”字节不为0时才存在
数据校验	2个字节，只在“长度”字节不为0时才存在
填充	可选的，最长为1个字节，其值为：X ‘FF’

图 4-3 BACnet 的 MS-TP 局域网的帧格式

帧类型域值表示的帧类型如下：

- 00：令牌
- 01：主节点轮询帧
- 02：响应主节点轮询帧
- 03：测试请求帧
- 04：测试响应帧
- 05：BACnet 数据期待响应帧
- 06：BACnet 数据不期待响应帧
- 07：响应延迟帧
- 8—127：保留为 ASHRAE 所用帧

128—255: 生产商定义的专用帧

## § 4.2 BACnet 的点到点(PTP)通信规范

为了使两个 BACnet 设备能够使用各种点到点通信机制进行通信, BACnet 定义了一种数据链路层协议, 称为 BACnet 点到点通信规范。这个协议的功能是: 使两个 BACnet 网络层实体建立点到点数据链路连接, 可靠地交换 BACnet PDU, 和使用已建立的物理连接执行 BACnet 点到点连接的有序终止。对应的物理连接方式有: EIA-232 连接调制解调器, 线路驱动器, 或者其它数据通信设备。

### 4.2.1 BACnet 点到点通信工作原理

BACnet 点到点通信协议只适用于半路由器设备之间的通信, 具有全双工通信、通信的断续性和通信速率慢的特点。当呼叫设备和被叫设备之间建立起物理连接之后, 两个 BACnet 设备之间交换一系列的信息帧, 以建立一个 BACnet 连接。一旦这种连接成功建立之后, 两个设备就可以透明地交换 BACnet PDU。不论呼叫设备还是被叫设备都可以启动释放连接过程, 而只有每个设备都发送了终止请求之后, 连接才会终止。点到点协议是面向连接的协议, 这与其它 BACnet 数据链路层协议不同。点到点协议还充分利用了物理连接的全双工特征, 使两个设备可以同时发送报文。

### 4.2.2 服务规范

BACnet 点到点通信协议向网络层提供了八个数据链路层服务原语, 这些原语的形式和功能如表 4-1 所示。

表 4-1 BACnet 点到点通信协议数据链路层服务原语和功能

原 语	功 能
DL-UNITDATA.request	由网络层传递给 PTP 实体, 请求使用不确认的无连接方式向一个或者多个远程节点的网络层实体发送一个网络层协议数据单元(NPDU)。
DL-UNITDATA.indication	由 PTP 实体传递给网络层, 通知有一个来自远程实体的 NPDU 的到达。
DL-CONNECT.request	由网络层传递给 PTP 实体, 请求建立一个逻辑链路连接。
DL-CONNECT.indication	由 PTP 实体传递给网络层, 指出已经建立一个逻辑链路连接。
DL-CONNECT.confirm	由 PTP 实体传递给网络层, 证实已经建立一个逻辑链路连接。
DL-DISCONNECT.request	由网络层传递给 PTP 实体, 请求释放建立的逻辑链路连接。
DL-DISCONNECT.indication	由 PTP 实体传递给网络层, 指出已经释放了逻辑链路连接。
DL-DISCONNECT.confirm	由 PTP 实体传递给网络层, 证实已经释放了逻辑链路连接。

### 4.2.3 帧格式

PTP 的数据链路帧格式如图 4 所示。其中前导码域、帧类型域、长度域和帧头校验域组成帧的“头段”; 数据域和数据校验域组成帧的“数据段”。

前导码	2个字节前导码: X '55FF'
帧类型	1个字节
长度	2个字节, 表示数据域的长度, 不包括CRC域
帧头校验	1个字节
数据	0-501个字节, 只在“长度”字节不为0时才存在
数据校验	2个字节, 只在“长度”字节不为0时才存在

图 4-4 BACnet 的 PTP 通信的帧格式

帧类型域值表示的帧类型如下:

- X '00': 心跳帧, 不含数据段, 通知对等设备数据链路仍有效, 但本地设备还不能接收数据帧。
- X '01': 心跳帧, 不含数据段, 通知对等设备数据链路有效并可以接收数据帧。
- X '02': 数据帧, 包含数据 NPDU, 数据域长度为 0—501 字节, 对应传输序列号 0。
- X '03': 数据帧, 包含数据 NPDU, 数据域长度为 0—501 字节, 对应传输序列号 1。
- X '04': 肯定确认帧, 不包含数据段, 确认已接收序列号 0 的数据帧, 不能接收后续帧。
- X '05': 肯定确认帧, 不包含数据段, 确认已接收序列号 1 的数据帧, 不能接收后续帧。
- X '06': 肯定确认帧, 不包含数据段, 确认已接收序列号 0 的数据帧, 可以接收后续帧。
- X '07': 肯定确认帧, 不包含数据段, 确认已接收序列号 1 的数据帧, 可以接收后续帧。
- X '08': 否定确认帧, 不包含数据段, 确认不能接收序列号 0 的数据帧, 不能接收后续帧。
- X '09': 否定确认帧, 不包含数据段, 确认不能接收序列号 1 的数据帧, 不能接收后续帧。
- X '0A': 否定确认帧, 不包含数据段, 确认不能接收序列号 0 的数据帧, 可以接收后续帧。
- X '0B': 否定确认帧, 不包含数据段, 确认不能接收序列号 1 的数据帧, 可以接收后续帧。
- X '0C': 连接请求帧, 不包含数据段, 由被叫设备发送, 请求建立一个 BACnet 连接。
- X '0D': 连接响应帧, 数据域中为一个密码, 由响应连接请求帧的设备发送。
- X '0E': 释放连接请求帧, PTP 通信中的任何设备都可发送, 其数据域中的数据表示释放连接的原因, 长度为 1 个字节, 分别是: X '00' 表示已经没有要传输的数据了, X '01' 表示对等进程正在运行, X '02' 表示收到的密码无效, X '03' 表示其它原因。
- X '0F': 释放连接响应帧, 不包含数据段, 确认已经收到释放连接请求帧, 并且表示接收释放连接的请求。
- X '14': 测试请求帧, 启动 PTP 传输路径的环路测试, 其数据域长度为 0—501 字节。
- X '15': 测试响应帧, 对测试请求帧的响应, 其数据域长度为 0—501 字节。

## § 4.3 BACnet 的 LonTalk 局域网规范

LonTalk 是由美国 Echelon 公司开发的数据通信协议, 较为广泛地应用于控制网络的数据通信中。BACnet 支持使用 LonTalk 协议的服务来传输 BACnet 报文的功能, 为此制定本规范。BACnet 将 LonTalk 协议规范, 包括将来的扩展, 作为自己的标准。同时, 仍然使用 ISO 8802-2 中的 Class I LLC 和类型 1 不确认的无连接模式服务作为逻辑链路控制协议。在产品实现中, 要将 BACnet 的 DL-UNITDATA 原语映射为 LonTalk 应用层接口。

### 1. LLC 原语所要求的参数

BACnet 网络仍然使用 LLC 的数据链路服务来传送 BACnet 链路服务数据单元(LSDU)。



同时，使用 DL-UNITDATA 原语传送 LLC 参数。DL-UNITDATA 原语中的参数是源地址、目标地址、数据和优先级。每个源地址和目标地址由 LonTalk 地址、链路服务访问点(LSAP)和报文代码(MC)组成。LonTalk 地址的长度可变，由 BACnet 设备的构造确定。MC 为 1 个字节，其值为 X‘4E’，表示此数据结构是一个 BACnet 帧。由于 LonTalk 报文代码识别 BACnet 网络层，所以不用 LSAP。数据参数就是来自网络层的 NPDU。

## 2. 将 LLC 原语映射到 LonTalk 的应用层

类型 1 不确认的无连接 LLC 服务原语 DL-UNITDATA.request 映射为 LonTalk 的 msg\_send 请求原语，DL-UNITDATA.indication 映射为 LonTalk 的 msg\_receive 请求原语。LonTalk 网络中不能传输长度超过 228 字节的 LPDU。

## 3. LonTalk 应用层原语所要求的参数

LonTalk 应用层原语是 msg\_send 和 msg\_receive。这些是用目标节点的 LonTalk 地址和 BACnet 报文代码封装的 LLC 数据的帧结构，图 5 是这种帧的数据结构图。整个帧由物理介质传送到目标节点设备。

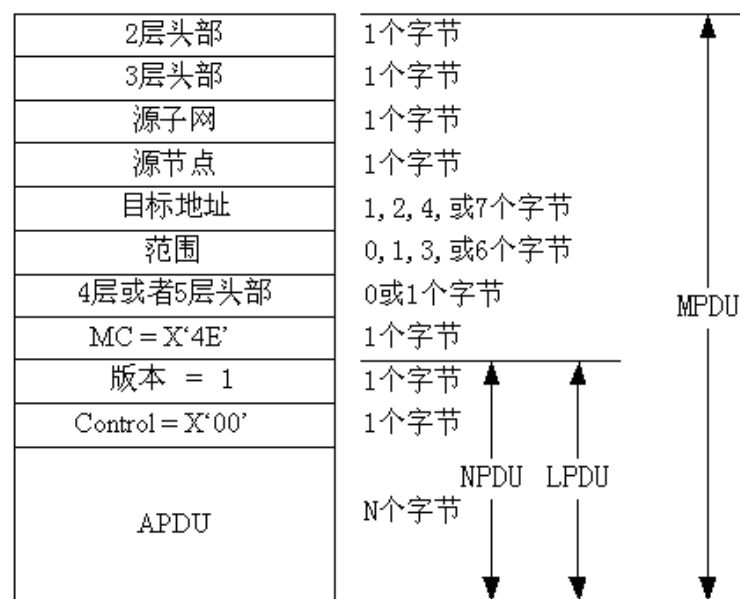


图 4-5 BACnet 的 Lontalk 局域网 MPDU 格式

## 4. 物理介质

完全采用 Lontalk 标准及其附件中对物理介质的规范。

## 第 5 章 BACnet 的对象模型

本章介绍 BACnet 定义的对象模型及模型中的 18 个对象类型,并对每一类对象的内容进行介绍。对象模型构建了网络设备之间通信的“共同语言”,这些对象具有广泛性,楼宇自控系统中的每个单元设备都可以由一个或者几个对象来描述。

### § 5.1 BACnet 的对象模型及其属性

在楼宇自控网络中,各种设备之间要进行数据交换,为了能够实现设备的互操作,所交换的数据必须使用一种所有设备都能够理解的“共同语言”。BACnet 的最成功之处就在于采用了面向对象的技术,定义了一组具有属性的对象(Object)来表示任意的楼宇自控设备的功能,从而提供了一种标准的表示楼宇自控设备的方式。在 BACnet 中,所谓对象就是在网络设备之间传输的一组数据结构,对象的属性就是数据结构中的信息,设备可以从数据结构中读取信息,可以向数据结构写入信息,这些就是对对象属性的操作。BACnet 网络中的设备之间的通信,实际上就是设备的应用程序将相应的对象数据结构装入设备的应用层协议数据单元(APDU)中,按照前面几篇文章中所叙述的规范传输给相应的设备。对象数据结构中携带的信息就是对象的属性值,接收设备中的应用程序对这些属性进行操作,从而完成信息通信的目的。

#### 5.1.1 BACnet 的对象定义

BACnet 目前定义了 18 个对象,表 5-1 给出了这些对象的名称和应用举例。

表 5-1 BACnet 定义的对象及其它们的应用实例

对象名称	应用实例
模拟输入 Analog Input	传感器输入
模拟输出 Analog Output	控制输出
模拟值 Analog Value	设置的阈值或其它模拟控制系统参数
数字输入 Binary Input	开关输入
数字输出 Binary Output	继电器输出
数字值 Binary Value	数字控制系统参数
时序表 Calendar	为按事件执行程序定义的日期列表
命令 Command	为完成诸如日期设置等特定操作而向多设备的多对象写多值
设备 Device	其属性表示设备支持的对象和服务以及设备商和固件版本
事件登记 Event Enrollment	描述可能处于错误状态的事件(例如“输入超出范围”),或者其它设备需要的报警。该对象可直接通知一个设备,也可用通知类(Notification Class)对象通知多对象
文件 File	允许读写访问设备支持的数据文件
组 Group	提供在一个读单一操作下访问多对象的多属性
环 Loop	提供标准化地访问一个“控制环”

多态输入 Multi-state Input	表述一个多状态处理程序的状况，如冰箱的开、关和除霜循环等
多态输出 Multi-state Output	表述一个多状态处理程序的期望状态，如冰箱的开始冷却时间、开始除霜时间等
通知类 Notification Class	包含一个设备列表，其中包括如果一个事件登记对象确定有一个警告或报警报文需要发送则将要送给的那些设备
程序 Program	允许设备中的一个程序开始，停止，装载，卸载，以及报告程序当前状态等
时间表 Schedule	定义一个按周期的操作时间表

每个对象都有一组属性，属性的值描述对象的特征和功能。在 BACnet 中，对于每个对象来说，属性分为必需的和可选的两种。用三个字母表示属性的类型，其意义分别是：O 表示此属性是可选的，R 表示此属性是必需的且是用 BACnet 服务可读的，W 表示此属性是必需的且是用 BACnet 服务可读和可写的。

## 5.1.2 BACnet 对象的属性

BACnet 要求每个 BACnet 设备都要有一个“设备对象”，“设备对象”包含此设备和其功能的信息。当一个 BACnet 设备要与另一个 BACnet 设备进行通信时，它必须要获得该设备的“设备对象”中所包含的某些信息。表 2 给出“设备对象”的属性描述。

表 5-2 “设备对象”的属性

属性标识符		属性的意义	特征
原意	中文意译		
Object_Identifier	对象标识符	一个用来标识对象的数字代码	R
Object_Name	对象名称	标识对象名称的字符串	R
Object_Type	对象类型	表示对象的类型，值为 DEVICE	R
System_Status	系统状态	表示设备的物理和逻辑状态	R
Vendor_Name	设备商名	标识生产厂商的字符串	R
Vendor_Identifier	设备商标识符	由 ASHRAE 分配的生产商标识代码	R
Model_Name	型号名称	由生产商分配的表示设备型号的字符串	R
Firmware_Revision	固件版本	由生产商分配的表示安装在设备中的固化软件的版本	R
Application_Software_Version	应用软件版本	表示安装在设备中的应用软件的版本	R
Location	位置	表示设备的物理位置的字符串	O
Description	描述	表示设备功能的字符串	O
Protocol_Version	协议版本	表示设备所支持的 BACnet 协议的版本	R
Protocol_Conformance_Class	协议一致类别	表示设备支持的一组标准协议服务和对象类型	R
Protocol_Service_Supported	协议服务支持	表示设备的协议实现所支持的标准协议服务	R
Protocol_Object_Types_Supported	协议对象类型支持	表示设备的协议实现所支持的标准对象类型	R
Object_List	对象列表	列出设备中的可被 BACnet 服务访问的所有对象的标识符	R
Max_APDU_Length_Accepted	最大应用层协议数据单元长度支持	表示在一个应用层协议数据单元所能装载的最大的字节数	R

Segmentation_Supported	分段支持	表示设备是否支持报文分段，分段传输和分段接收	R
VT_Classes_Supported	虚拟终端类型支持	设备支持的终端类型	O
Active_VT_Sessions	活动虚拟终端会话	表示任何给定时间活动的网络可访问的虚拟终端	O
Local_Time	本地时间		O
Local_Date	本地日期		O
UTC_Offset	时差	本地时间与国际标准时间的时差	O
Daylight_Savings_Status	夏令时状态	是否是夏令时	O
APDU_Segment_Timeout	APDU 分段超时	以毫秒表示对 APDU 分段超时重传的等待时间	O
APDU_Timeout	APDU 超时	以毫秒表示对 APDU 超时重传的等待时间	R
Number_Of_APDU_Retries	APDU 重传次数	表示重传 APDU 的最大次数	R
List_Of_Session_Keys	会话密钥列表	用于与其它 BACnet 设备进行通信的密钥列表	O
Time_Synchronization_Recipients	时间同步容器	表示设备使用时间同步服务的限制	O
Max_Master	最大主节点数	表示在 MS/TP 网络中的最大主节点数	O
Max_Info_Frame	最大信息帧数	表示在 MS/TP 网络中节点在掌握令牌时能够发送的信息帧的最大数量	O
Device_Address_Binding	设备地址捆绑	对象标识符与设备地址捆绑的列表	R

从表 5-2 中可以看到，虽然“设备对象”的属性很多，但是大部分是在出厂时就写定了的，且是只读属性。另一点要注意的是，“设备对象”的“对象标识符”属性中的设备实例号必须是在整个 BACnet 互联网中唯一的，这样才能在安装系统时标识设备。

表中的前三项属性，即“对象标识符”，“对象名称”和“对象类型”是 BACnet 设备中的每个对象必须具有的属性。“对象标识符”是一个 32 位的编码，用来标识对象的类型和其实例标号，这两者一起可以唯一地标识对象；“对象名称”是一个字符串，BACnet 设备可以通过广播某个“对象名称”而建立与包含有此对象的设备的联系，这将使整个系统的设置大为简化；“设备对象”的属性向 BACnet 网络表述了设备的全部信息。例如，“对象列表”属性提供了设备中包含的每个对象的列表。

下面分类介绍 BACnet 标准中定义的 18 个对象和它们的属性。

## § 5.2 BACnet 对象的分类介绍

### 5.2.1 输入输出值对象类型及其属性

在楼宇自动控制系统中，设备的输入输出值是一类基本的参数。BACnet 定义了 6 个输入输出值对象，分别是：模拟输入对象，数字输入对象，模拟输出对象，数字输出对象，模拟值对象和数字值对象。这些对象全面地定义了 BACnet 设备之间交换关于与控制单元有关的信息时所采用的“共同语言”。模拟输入和数字输入是物理设备或者硬件的输入信号参数，模拟输出和数字输出是物理设备或者硬件的输出信号参数，模拟值和数字值是存储在 BACnet 设备中的控制系统参数。表 3 给出了这些对象的属性描述。

表 5-3 输入输出值对象的属性

属 性		模拟 输入	模拟 输出	模拟 值	数字 输入	数字 输出	数字 值
属性标识	标识含义						
Object_Identifier	对象标识符	R	R	R	R	R	R
Object_Name	对象名称	R	R	R	R	R	R
Object_Type	对象类型	R	R	R	R	R	R
Present_Value	当前值	R	W	W	R	W	R
Description	描述	O	O	O	O	O	O
Device_Type	设备类型	O	O	×	O	O	×
Status_Flags	状态标志	R	R	R	R	R	R
Event_State	事件状态	R	R	R	R	R	R
Reliability	可靠性	O	O	O	O	O	O
Out_Of_Service	脱离服务	R	R	R	R	R	R
Update_Interval	更新间隔	O	×	×	×	×	×
Units	单位	R	R	R	×	×	×
Min_Pres_Value	最小值	O	O	×	×	×	×
Max_Pres_Value	最大值	O	O	×	×	×	×
Resolution	分辨率	O	×	×	×	×	×
Priority_Array	优先值数组	×	R	O	×	R	O
Relinquish_Default	释放缺省	×	R	O	×	R	O
COV_Increment	COV 增量	O	O	O	×	×	×
Polarity	极性	×	×	×	R	R	×
Inactive_Text	非活动文本	×	×	×	O	O	O
Active_Text	活动文本	×	×	×	O	O	O
Change_Of_State_Time	状态改变时间	×	×	×	O	O	O
Change_Of_State_Count	状态改变次数	×	×	×	O	O	O
Time_Of_State_Count_Reset	改变时间置 0	×	×	×	O	O	O
Elapsed_Active_Time	现值活动累计	×	×	×	O	O	O
Time_Of_Active_Time_Reset	活动时间置 0	×	×	×	O	O	O
Minimum_Off_Time	非活动最小值	×	×	×	×	O	O
Minimum_On_Time	活动最小值	×	×	×	×	O	O
Time_Delay	时间延迟	O	O	O	O	O	O
Notification_Class	通知类	O	O	O	O	O	O
High_Limit	高值极限	O	O	O	×	×	×
Low_Limit	低值极限	O	O	O	×	×	×
Deadband	极限宽度	O	O	O	×	×	×
Limit_Enable	极限使能	O	O	O	×	×	×
Alarm_Value	报警值	×	×	×	O	O	O
Event_Enable	事件使能	O	O	O	O	O	O
Acked_Transition	要求变换	O	O	O	O	O	O
Notify_Type	通知类型	O	O	O	O	O	O

图 5-1 是一个模拟输入对象的举例，它描述一个气体温度传感器的模拟传感输入信号。这个对象可能驻留在连接传感器的节点设备中，也可能驻留在作为 BACnet 设备的智能传感器中。如何实现这些是各生产厂家自己解决的问题。图 1 表示网络设备可以通过 5 个属性访问该对象，其中描述、设备类型和单位属性值是在设备安装时设定的，而当前值和脱离服务属性值表示设备的当前状态。还有一些属性（模拟输入对象最多可以有 25 个属性）没有在此图中显示出来，它们的值可能是在设备出厂时设定的。图中还表示通过网络有一个询问此对象当前值的请求和此设备的应答，这些就是对属性的操作。

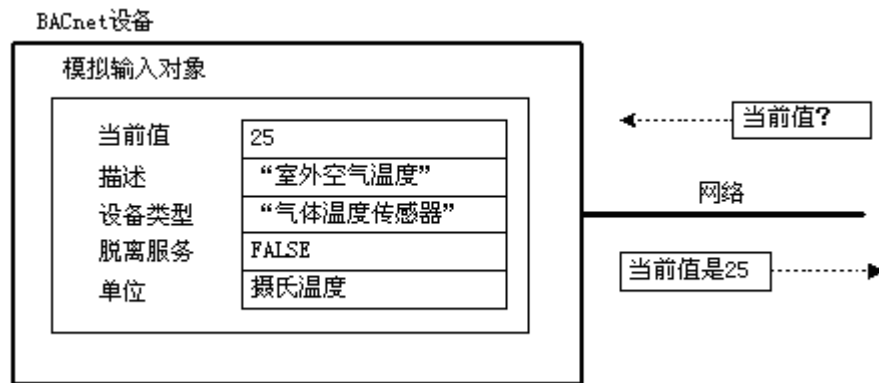


图 5-1 BACnet 的模拟输入对象举例

## 5.2.2 命令对象类型

命令对象根据其 Present\_Value 属性中的“操作代码”向一组对象的属性写入一组值。命令对象的 Action 属性是一个数组，其中包含有一个操作列表，对应着一系列的操作值。当 Present\_Value 属性被写入新值时，命令对象就根据此值所对应的 Action 属性中的列表内容，向某个 BACnet 设备的某个对象的某个属性写入某个特定值。

## 5.2.3 时序表和时间表对象类型

时序表对象用来表示一个日期列表，可以包含一些有特定事件发生的日期，例如节假日等。

时间表对象用来表示一个周期性的时间表，在每个时间表内，都进行相同的操作。此对象也可用作周期性地向某个对象的某个属性写入某特定值。

## 5.2.4 事件登记对象类型

将任何一个对象的任何一个属性的值发生偏离预设值的变化称为事件。事件登记对象包含在 BACnet 系统中管理事件所要求的信息。这些信息包括事件的定义和当该事件发生时将要通知的设备以及通知报文的内容等。

## 5.2.5 文件、组和环对象类型

文件对象表示用 BACnet 文件服务可以访问的数据文件的性质，它的一个重要的属性是文件访问方式属性，其值有记录访问，流访问，记录与流访问。

组对象用来简化 BACnet 设备之间信息交换的处理过程，其方法是使用一种简记的方

式来标识一个组中的所有成员。一组中可以包含各种对象类型。

环对象表示任何形式的反馈控制环路。

### 5.2.6 多态输入输出对象类型

多态输入对象表示对象所驻留的 BACnet 设备中的一个运算程序的结果。例如，多态输入对象的状态（用它的当前值属性表示）可以是多个二进制输入值的逻辑和，或者是一个或多个模拟输入的阈值，或者是一个数学计算的结果。

多态输出对象表示对象所驻留的 BACnet 设备中一个或者多个物理输出或处理程序的期望的状态。当前值属性是一个无符号整数，表示对象的状态。例如，某个状态可以代表某些物理输出的活动/非活动情况，或者某个模拟输出的值。

### 5.2.7 通知类对象类型

通知类对象包含在 BACnet 系统中分发事件通知所需要的信息。对于那些事件激励对象来说，这个对象特别有用，它提供了如何处理通知、怎样规划通知目标、以及怎样获得确认的方式。

### 5.2.8 程序对象类型

程序对象表示在 BACnet 设备中运行的应用程序的外部可见特征。程序对象的属性向网络提供了一个应用程序的一些参数的表征。在程序对象的属性中有两个属性特别重要，它们是程序状态(Program\_State)属性和程序改变(Program\_Change)属性。程序状态属性反映该对象所表示的应用程序执行过程的逻辑状态。程序状态属性有六个属性值，分别是：IDLE（程序没有执行），LOADING（正在装载应用程序），RUNNING（正在执行应用程序），WAITING（运行的程序正在等待某个外部事件），HALTED（由于某个错误导致运行程序中止）和 UNLOADING（运行程序按要求被终止）。程序改变属性用来请求改变该对象所表示的程序的运行状态。程序改变属性有六个属性值，分别是：READY（这是正常状态，表示准备接收改变请求并执行），LOAD（如果还没有装载应用程序，则请求装载应用程序），RUN（如果还没有运行应用程序，则请求应用程序开始执行），HALT（请求应用程序暂停执行），RESTART（请求应用程序从初始点开始重新运行）和 UNLOAD（请求应用程序终止运行并且卸载）。

归纳 BACnet 对象模型，可以看出：在传统自动控制工业领域中，一直使用“点”这个通用术语来描述诸如传感器输入，控制输出，或者控制值等这些参数类型，而且不同厂家的设备对这些参数特征的表示也使用各自不同的方法。BACnet 定义一个标准对象集合表示楼宇自控网络中参数类型，每个 BACnet 设备中都具有一些（至少一个）对象。每个对象有一个标准属性集合，向网络中的其它设备描述对象和其当前状态。其它 BACnet 设备通过操作属性实现对象控制，从而达到信息交换和分布控制的目的。

BACnet 设备的功能决定于该设备内驻留的对象类型和数量，BACnet 标准并不要求在所有的 BACnet 内要有所有的对象。但每个 BACnet 设备必须要有“设备对象”，其中的对象列表属性提供了该设备内包含的所有对象的一个列表。

另外，BACnet 标准允许厂家根据需要自己定义专用对象，但是 BACnet 标准并不提供与专用对象的接口，所以，其它设备一般不能访问专用对象。

## 第 6 章 BACnet 的服务

本章介绍 BACnet 定义的 35 个服务，服务提供了用于访问和操作这些信息的命令，并提供 BACnet 设备之间通信所需要的获取信息的方法。

### § 6.1 BACnet 的服务定义

在楼宇自控网络中，各种设备之间要进行数据交换，BACnet 的**对象提供了网络设备进行信息通信的“共同语言”**。除此之外，BACnet 设备之间还要有进行信息传递的手段，例如，一个设备要求另一个设备提供信息，命令另一个设备执行某个动作，或者向某些设备发出信息通知已经发生某事件，等等。在面向对象技术中，与对象相关联的是属性和方法，属性用来说明对象，而方法是外界用来访问或作用于对象的手段。在 BACnet 中，把对象的方法称为服务(Service)，对象提供了对一个楼宇自控设备的“网络可见”部分的抽象描述，而服务提供了用于访问和操作这些信息的命令。

服务就是一个 BACnet 设备可以用来向其它 BACnet 设备请求获得信息，**命令其它设备执行某种操作或者通知其它设备有某事件发生的方法**。在 BACnet 设备中要运行一个“应用程序”，负责发出服务请求和处理收到的服务请求。这个应用程序实际上就是一个执行设备操作的软件。例如，在操作工作台，应用程序负责显示一系列传感器的输入信号，这需要周期性地向相应的目标设备中的对象发送服务请求，以获得最新的输入信号值；而在监测点设备中，它的应用程序则负责处理收到的服务请求，并返回包含有所需数据的应答。**实现服务的方法就是在网络中的设备之间传递服务请求和服务应答报文**。图 6-1 是一个 BACnet 设备接收服务请求和进行服务应答的示意图。

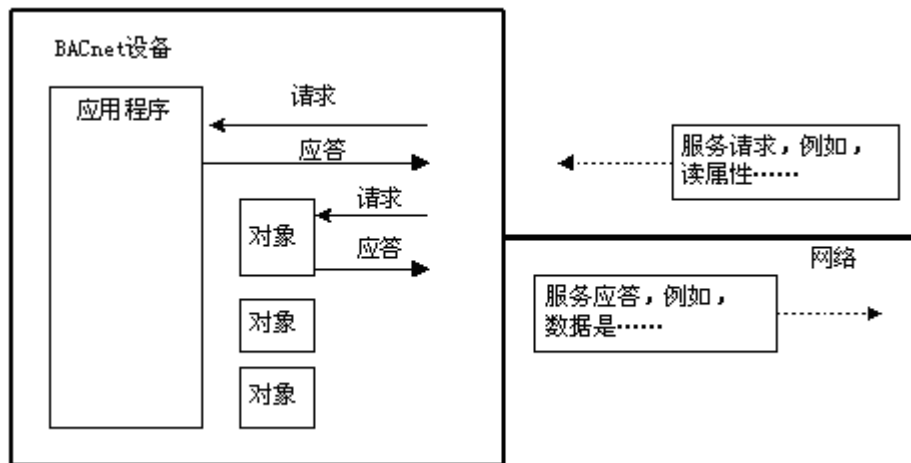


图 6-1 BACnet 服务请求和应答

BACnet 定义了 35 个服务，并且将这 35 个服务划分为 6 个类别。这 6 个服务类别分别是：报警与事件服务(Alarm and Event Services)，文件访问服务(File Access Services)，对象访问服务(Object Access Services)，远程设备管理服务(Remote Device Management Services)，虚拟终端服务(Virtual Terminal Services)，和网络安全性(Network Security)。这些服务又分为两种类型，一种是确认服务(Confirmed，简单标记为“C”)，另一种是不确认服务(Unconfirmed，简单标记为“U”)。发送确认服务请求的设备，将等待一个带有数据



的服务应答。而发送不确认服务请求的设备并不要求有应答返回。对于每一个确认服务，BACnet 设备或者能够发送服务请求，或者能够处理并应答收到的服务请求，或者两者都能做。对于每一个不确认服务，BACnet 设备或者能够发送服务请求，或者能够处理收到的服务请求，或者两者都能做。BACnet 并不要求每个设备具有执行每个服务的能力，但是有一个服务是每个设备都必须能够处理的，这就是“读属性”服务。下面讨论这六个类别的服务。

## § 6.2 BACnet 服务的分类介绍

### 6.2.1 报警与事件服务

报警与事件服务类别中有 8 种服务，这类服务处理 BACnet 设备感知的环境状态的变化。在 BACnet 中，“事件”表示有预先设置的某个对象的某个属性的值的改变，或者内部状态的改变。BACnet 并没有指定哪个事件应被考虑为“报警”，而是定义了 Notify\_Type 属性，使用户可以用来指定哪个事件应被作为报警。BACnet 提供了三种管理事件的机制：属性值的改变(COV)报告，内部特性报告和算法改变报告。COV 报告允许客户以永久方式或者临时方式预订接收某些参考属性的值的改变的报告。报警与事件服务提供了 BACnet 设备预订请求“值的改变通告”、请求报警或事件的状态摘要、向其它设备发送报警或事件发生的通知、和已经收到报警通知的确认等的方法。表 6-1 列出了报警与事件服务类别中的 8 种服务的功能。

表 6-1 报警与事件服务

服 务	确认性	描 述
确认报警 AcknowledgeAlarm	C	用来告知报警发送方，操作者已收到报警。
确认的“属性值改变”通告 ConfirmedCOVNotification	C	告知“属性值改变”的预订设备，在一个属性中已发生值的改变。
确认的事件通告 ConfirmedEventNotification	C	用来告知发送者，可能发生一个错误。
获得报警摘要 GetAlarmSummary	C	请求设备提供一份“活动报警”列表。
获得注册摘要 GetEnrollmentSummary	C	请求一份（可能错误的）“事件”列表。
预订“属性值改变” SubscribeCOV	C	由一个设备发送的，请求当在一个对象中有属性值改变发生，要被告知。
不确认的“属性值改变”通告 UnconfirmedCOVNotification	U	告知“属性值改变”的预订设备，在某个对象的一个或多个属性中值的改变已发生。
不确认的事件通告 UnconfirmedEventNotification	U	用来告知多个设备，可能发生一个或多个错误。

有九个对象可以具有支持报警与事件服务功能的可选属性，这九个对象是：“模拟输入对象”，“模拟输出对象”，“模拟值对象”，“数字输入对象”，“数字输出对象”，“数字值对象”，“环对象”，“多状态输入对象”，和“多状态输出对象”。内部特性报告用来定义只对某个特定对象的且由该对象的属性单独表示的报警或事件的情况。内部特性事件是基于某种算法的，这种算法是某对象类型特有的并且只与该对象的某个属性相关联。例如，“模拟输入对象”支持“读数超出阈值”事件的内部特性报告，一些可选属性定义了可接受值的阈值(Max\_Pres\_Value and Min\_Pres\_Value)，这个阈值检查只用于“当前值属性”。算法改变报告可用于任何对象的任何属性。BACnet 定义了六个事件算法，分别是：比特流的改

变(Change\_Of\_Bitstring), 状态改变(Change\_Of\_State), 值的改变(Change\_Of\_Value), 命令失败(Command\_Failure), 极限溢出(Floating\_Limit), 和超出阈值(Out\_Of\_Range)。

## 6.2.2 文件访问服务

文件访问服务提供读写文件的方法, 这包括上载和下载控制程序和数据库的能力。表 6-2 列出了文件访问服务类别中的 2 种服务的功能。服务之所以称为“基本读文件”和“基本写文件”, 是因为在对一个文件进行读或写操作时, 不允许同时又进行另外的读或写操作。BACnet 现在的版本还没有定义文件的格式, 但是确实提供了以记录结构(record-structure)格式或者以连续字节流的方式访问文件。

表 6-2 文件访问服务

服 务	确 认 性	描 述
基本读文件 AtomicReadFile	C	请求获得一个“文件对象”文件的部分或全部。
基本写文件 AtomicWriteFile	C	向一个“文件对象”写入部分或全部文件。

## 6.2.3 对象访问服务

对象访问服务类别中有 9 种服务, 提供了读出、修改和写入属性的值以及增删对象的方法。为了将对一个 BACnet 设备中的多个属性的读出和写入操作结合到一个单一的报文中, 提供了读多个属性(ReadPropertyMultiple)和写多个属性(WritePropertyMultiple)服务, 这将减轻网络的负载。条件读属性(ReadPropertyConditional)提供了更复杂的服务, 设备根据包含在请求中的准则来测试每个相关的属性, 并且返回每个符合准则的属性的值。虽然定义了创建对象和删除对象服务, 但是其应用是受限制的。与物理设备本身相关联的对象是不可增删的, 而组对象和事件注册对象以及在某些情况下的文件对象可对其进行增删服务。

表 6-3 对象访问服务

服 务	确 认 性	描 述
添加列表元素 AddListElement	C	向一个列表的属性添加一个或多个项目。
删除列表元素 RemoveListElement	C	从一个列表的属性中删除一个或多个项目。
创建对象 CreateObject	C	用来在本设备中创建一个对象的新实例。
删除对象 DeleteObject	C	用来在本设备中删除某个对象。
读属性 ReadProperty	C	返回一个对象的一个属性的值。
条件读属性 ReadPropertyConditional	C	返回符合条件的多个对象中的多个属性的值。
读多个属性 ReadPropertyMultiple	C	返回多个对象中的多个属性的值。
写属性 WriteProperty	C	向一个对象的一个属性写入值。
写多个属性 WritePropertyMultiple	C	向多个对象中的多个属性写入值。

## 6.2.4 远程设备管理服务

远程设备管理服务类别中有 11 种服务, 提供对 BACnet 设备进行维护和故障检测的工

具。表 6-4 列出了远程设备管理服务类别中的 11 种服务的功能。可以用 Who-Is 和 I-Am 服务来获得 BACnet 互联网中的 BACnet 设备的网络地址。当一个 BACnet 设备需要知道一个或多个其它 BACnet 设备的地址时，它就可向整个 BACnet 互联网广播一个标明有一个“设备对象实例标号”或者一组“设备对象实例标号”的 Who-Is 服务请求报文。需要响应的设备并不是向询问设备发回一个响应，那些具有 Who-Is 报文中标明的“设备对象实例标号”的设备向本地局域网，或者向远程网，或者向整个 BACnet 互联网广播一个包含有其自己的网络地址的 I-Am 服务报文。这样不仅响应了询问的设备，而且也使那些需要知道地址的其它设备得到了信息，限制了网络负载的增加。

Who-Has 和 I-Have 服务具有与 Who-Is 和 I-Am 相似的功能，但是在 Who-Has 中增加了一个“对象标识符”或者“对象名称”，具有相应询问请求的对象的设备广播一个 I-Have 服务报文作为响应。

表 6-4 远程设备管理服务

服 务	确认性	描 述
设备通信控制 DeviceCommunicationControl	C	通知一个设备停止（及开始）接收网络报文。
确认的专用信息传递 ConfirmedPrivateTransfer	C	向一个设备发送一个厂商专用报文。
不确认的专用信息传递 UnconfirmedPrivateTransfer	U	向一个或多个设备发送一个厂商专用报文。
重新初置设备 ReinitializeDevice	C	对接受的设备进行排序，以使可以自引导冷或热启动。
确认的文本报文 ConfirmedTextMessage	C	向另一个设备传递一个文本报文。
不确认的文本报文 UnconfirmedTextMessage	U	向一个或多个设备发送一个文本报文。
时间同步 TimeSynchronization	U	向一个或多个设备发送当前时间。
Who-Has	U	询问 BACnet 设备中哪个含有某个对象。
I-Have	U	肯定应答 Who-Has 询问，广播。
Who-Is	U	询问关于某个 BACnet 设备的存在。
I-Am	U	肯定应答 Who-Is 询问，广播。

## 6.2.5 虚拟终端服务

因为不同厂家生产的楼宇自控设备仍然保持有在其硬件和结构上的专有特性，BACnet 要提供一种工具，使得操作者能够重构这些设备。虚拟终端服务就是这样的工具，它们提供了一种实现面向字符的数据双向交换的机制。操作者可以用虚拟终端服务建立 BACnet 设备与一个在远程设备上运行的应用程序之间的基于文本的双向连接，使得这个设备看起来就象是连接在远程应用程序上的一个终端。

表 6-5 虚拟终端服务

服 务	确认性	描 述
VT-Open	C	与一个远程 BACnet 设备建立一个虚拟终端会话。
VT-Close	C	关闭一个建立的虚拟终端会话。
VT-Data	C	从一个设备向另一个参与会话的设备发送文本。

## 6.2.6 网络安全性服务

安全性服务提供对等实体验证，数据源验证，操作者验证，和数据加密等功能。为了实现安全性功能，在网络中要设置一个设备作为密钥服务器，每个要具有安全性特性的设备都要被分配一个密码，并且支持安全性服务。BACnet 允许支持安全性服务的设备与不支持安全性服务的设备混合运行，是否运行安全性服务由具体的事务决定。

表 6-6 安全性服务

服 务	确 认 性	描 述
验证 Authenticate	C	验证密码。
请求密钥 RequestKey	C	申请一个密钥。

## § 6.3 BACnet 协议的一致性描述

BACnet 从满足分布式楼宇自控系统对所有控制通信的要求出发，定义了一组广泛的对象类型和服务。实际上，对于一个具体的楼宇自控系统来说，没有必要所有的设备都支持所有的 BACnet 功能。为此，BACnet 协议定义了 6 个一致性类别和 13 个功能组。

### 6.3.1 BACnet 协议的一致性类别

一致性类别的编号是 1—6，是分级结构，最低级别的是一致性类别 1。每个类别都规定了设备要实现的最小的服务子集，且包含有比它低一级别的类别的所有服务。随着一致性类别的级别的提高，不断增加设备应能够响应的服务请求和能够启动的服务请求的数量。一致性类别 1 的 BACnet 设备只要求具有一个“设备对象(Device Object)”及能够响应读属性服务请求。一致性类别 2 的设备要求再增加能够响应写属性服务请求。一致性类别 3 的设备增加的服务是：启动 I-Am 和 I-Have 服务请求，响应读多个属性、写多个属性、Who-Has 和 Who-Is 服务请求。一致性类别 4 的设备再增加的服务是：启动添加列表元素、删除列表元素、读属性、读多个属性、写属性和写多个属性服务请求，响应添加列表元素和删除列表元素服务请求。一致性类别 5 的设备再增加的服务是：启动 Who-Has 和 Who-Is 服务请求，响应创建对象、删除对象和条件读属性服务请求。一致性类别 6，要求设备能够执行全部 32 个服务类型中的 21 个，其中有 20 个必须是该设备能够启动的服务，有 17 个是设备能够响应的服务。一致性类别分类提供了一种评测 BACnet 设备通信能力的方法。

### 6.3.2 BACnet 协议的功能组

功能组规定了为实现特定的楼宇自动控制功能而需要的对象与服务的组合。已经定义了 13 个功能组。时钟功能组提供与具有时钟有关的一般能力。便携工作站功能组提供与便携式工作站设备有关的能力。PC 工作站功能组提供与主操作工作站有关的能力。事件启动功能组提供定义报警和事件、检测报警或事件的产生以及启动通告报警或事件发生的通知报文的能力。事件响应功能组提供对通告报警或事件发生的通知报文的响应能力。COV 事件启动功能组提供启动通知报文通告已发生值改变事件的能力。COV 事件响应功能组提供预订和接收通告已发生值改变事件的通知报文的能力。文件功能组提供读、写、上载和下载文件的能力。重初始化功能组表示能被远程设备重新初始化的能力。虚拟操作员接口功

能组提供虚拟终端会话操作员端的能力。虚拟终端功能组提供虚拟终端会话的服务器端的能力。设备通信功能组提供启动和中止与某个设备单独通信的能力，从而可以用于网络监测。时间主机功能组提供自动启动时间同步服务的能力。

BACnet 标准要求生产厂商要为每个 BACnet 设备提供标准格式的文件，称为协议实现一致性描述，标识在设备中已实现的 BACnet 标准规范的内容。文件包含的信息有：标识生产厂商和描述设备的基本信息，设备的一致性类别，设备支持的功能组，设备支持的服务，设备支持的对象类型及其属性描述，设备支持的数据链路层技术选择，设备支持的分段请求和响应。

总之，BACnet 标准定义了 BACnet 设备之间进行通信的所有元素。应用面向对象技术，BACnet 定义了 18 个对象，描述楼宇自控系统中所涉及的与控制及通信相关的事物。通过定义 123 个属性和 35 个服务，提供了 BACnet 设备之间通信所要交换的信息和获取信息的通用化方法。

## 第 7 章 BACnet/IP---BACnet 互联网

本文介绍了 BACnet 互联网的概念, 用 PAD 组建 BACnet 互联网, BACnet/IP 网络的规范, BACnet/IP 设备和 BACnet 设备组成的混合网络的工作原理。

### § 7.1 BACnet 互联网的概念

BACnet 互联网是由两个或者多个 BACnet 网络所组成的网络的网络。BACnet 标准最初只是作为一个楼宇范围的自动控制网络通信协议而制定的标准。随着信息社会的发展, 已经有越来越多地要求将 BACnet 系统跨越园区、城市、地区、国家和洲而连接起来。最合适的实现方法就是使用现有的 IP 协议和广域网将 BACnet 系统连接。但是, BACnet 设备和 IP 设备使用的是不同的协议, 不同的语言, 不能将这些设备简单地放置于一个网络中就能使它们在一起工作。为了使网络中的设备能够通信, 网络设备必须使用共同的语言, 称之为协议。对于 BACnet 设备, 协议就是 BACnet 协议。对于 IP 网络设备, 协议就是 TCP/IP 互联网协议。协议定义了设备之间交换的报文分组的格式, 传输帧的格式, 以及包含有目标地址和协议类型的封装格式。将多个网络连接起来就组成互联网(internetwork), 连接互联网中的网络的设备称为路由器, 路由器要与两个以上的网络连接。路由器在接收到一个报文时, 需要确定是否要将这个报文转发到另一个网络中, 因此它必须能够理解帧的协议。BACnet 路由器必须理解 BACnet 帧, IP 路由器必须理解 IP 帧。仅仅由只能够理解 BACnet 帧的路由器连接的 BACnet 互联网称之为直接连接的互联网, 由 IP 路由器将多个直接连接的互联网互连, 组成“超级”互联网。要将 BACnet 网络通过 IP 广域网互连起来, 首先遇到的问题是 IP 路由器不能识别 BACnet 帧。解决这个问题的方法是使用一个也能够理解 IP 协议的特别 BACnet 设备, 这个设备能够将 BACnet 报文封装到一个 IP 帧中, 从而使得 IP 路由器能够识别该帧, 并且通过 IP 互联网进行转发。在目标节点, 有另一个这样的设备用来从 IP 帧中拆装出 BACnet 报文, 并且进行处理。

BACnet 标准目前使用两种技术来实现 IP 互联 BACnet 网络。第一种技术在附件 H 中进行了描述, 称之为“隧道”技术, 其设备称之为 BACnet/IP 分组封装拆装设备, 简称 PAD, 其作用像一个路由器, 将 BACnet 报文通过 IP 互联网传送。第二种技术在附件 J 中进行了描述, 称之为 BACnet/IP 网络技术, 设备称之为 BACnet/IP 设备, 其作用就是直接将 BACnet 报文封装进 IP 帧中进行传输。

### § 7.2 用 PAD 组建 BACnet 互联网

所谓隧道技术是指要实现这样一个过程, 首先将数据封装在一个网络协议的数据包内, 然后使用该协议进行数据传输, 最后在它们到达其目的地时解开封装。为了通过 IP 网络连接 BACnet 网络, 在每一个 BACnet 网络中要配置一个称之为 PAD 的特别类型的路由器, 它的作用是通过 IP 网络将一个 BACnet 网络与另一个 BACnet 网络互连起来。PAD 可以是一个单独的设备, 也可以是楼宇控制设备的一部分功能。PAD 的功能像一个 BACnet 路由器, 当它接收到一个 BACnet 报文时, 如果该报文的目标地址位于一个远程 BACnet 网络, 而且只能通过一个 IP 互联网才能到达目标 BACnet 网络, PAD 将该报文封装进一个 IP 帧中, 给出位于目标 BACnet 网络中的对应的 PAD 的 IP 地址, 作为封装帧的目标 IP 地址,

将此帧发送到 IP 互联网中。接收方的 PAD 从 IP 帧中取出 BACnet 报文，并且将其传送给本地局域网内的目标设备。发送和接收报文的 BACnet 设备本身并不知道为了传送报文会有这么多的特别的操作。它们与 PAD 通信就好像 PAD 是一个连接到 BACnet 网络上的普通的 BACnet 路由器一样。使用隧道传输技术的好处是，在将数据包发往远程目的地之前，PAD 设备可以修改数据包，为此，最常见的用法就是对数据包进行加密，从而形成一个安全的网络。图 7-1 表示用 PAD 组建 BACnet 互联网的工作原理图。

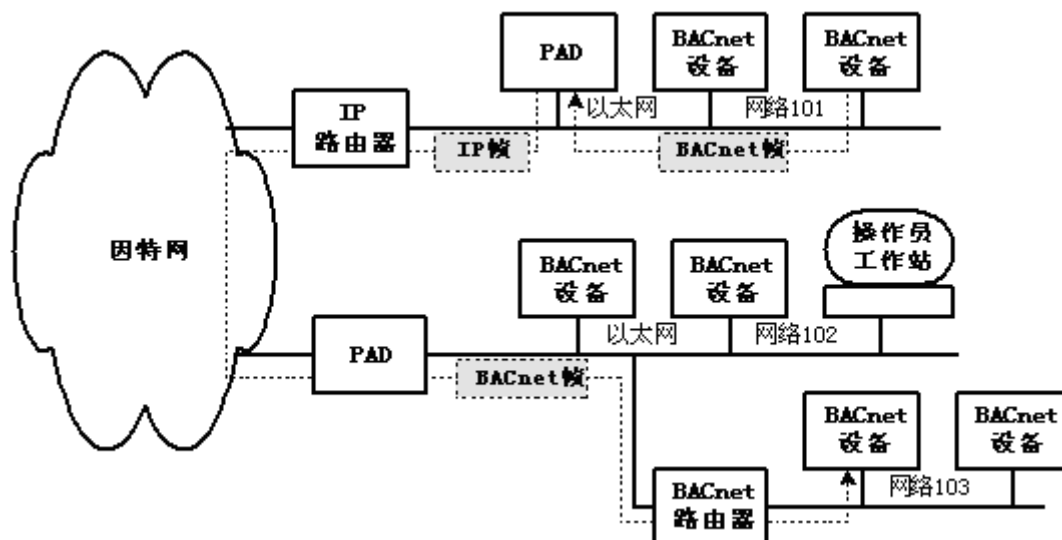


图 7-1 用 PAD 组建 BACnet 互联网

在图 7-1 中，网络 102 和网络 103 由一个 BACnet 路由器连接组成直接连接的互联网，而网络 101 由 IP 路由器通过因特网连接于直接连接互联网，组成“超级”互联网。从图 7-1 中还可以看到，存在两种 PAD 配置。

第一种是 PAD 只有一个物理网络连接端口，比如在网络 101 中，这时，BACnet 帧和 IP 帧都能传输。为了将 IP 帧传送给远程的 PAD，要求在网络中配置一个 IP 路由器。

第二种 PAD 配置，对于 BACnet 帧和 IP 帧有不同的连接端口。IP 端口可以直接连接到 IP 互联网上，这时，PAD 被 IP 互联网认为是一个用 IP 进行通信的设备，而不是一个 IP 路由器。对于 BACnet 设备来说，IP 路由器和因特网都是完全不可见的。

PAD 与 BACnet 路由器的不同点是它们处理全局广播的方式不同。路由器的处理方式是，对于广播报文，路由器将它重新发送给除了报文来自于的那个网络之外的所有网络；而 PAD 却是向每一个对等 PAD 发送一个 IP 帧，这就要求 PAD 保持一个对等 PAD 的 IP 地址表。

在智能小区中应用 BACnet 互联网是一个非常好的应用实例。在园区中，每个楼宇都有它自己的 BACnet 网络，通过园区中的 IP 互联网，将园区中的所有楼宇 BACnet 网络互连组成一个广域的 BACnet 互联网，并且构造成为一个虚拟网络。虚拟网络的概念是这样的，由 IP 网络将若干个 BACnet 网络互连起来组成一个 BACnet 互联网，对于互联网中的 BACnet 设备来说，由于 IP 网络是不可见的，这些 BACnet 设备会将整个 BACnet 互联网中的 BACnet 设备都看成是在一个单独的 BACnet 网络中的设备一样，从这个角度来说，就形成了一个虚拟的网络。将若干个甚至所有的园区 BACnet 互联网通过因特网（因特网是一个全球范围内的 IP 网络）互连，组成“超级” BACnet 互联网，构造为一个超级虚拟网络。图 7-2 表示由两个智能小区互联网所组成的“超级”互联网，其中两个小区各自都有自己的 IP 互联网，并且构造了各自的虚拟网络（标记为虚拟网络 1 和虚拟网络 2），通过

因特网互连构造成为超级虚拟网络（标记为虚拟网络 10）。从图中还可看到，组成超级虚拟网需要增加 PAD 设备。

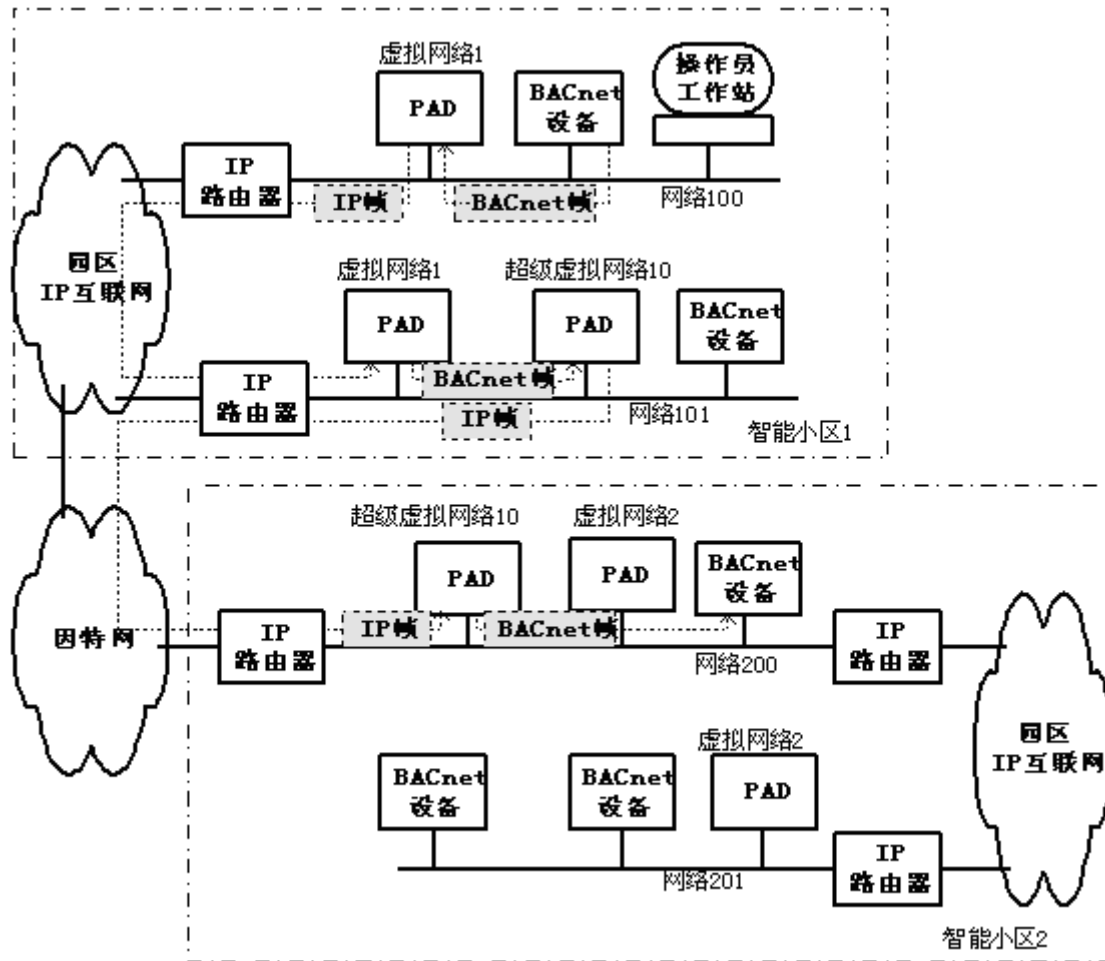


图 7-2 智能小区中的 BACnet 互联网

### § 7.3 BACnet/IP 网络

附件 H 的 PAD 设备是实现在 IP 网络上互连 BACnet 网络的最简单的方法，但是，这种方法有一些不足。其中之一是，不容易从网络中增删设备。如果要重构网络时，必须重新改写每一个 PAD 中的对等 PAD 设备表。为此，SSPC135 开发了一个更有效的协议，称为 BACnet/IP，作为附件 J 加入到 BACnet 标准中。ASHRAE 于 1999 年 1 月正式发布附件 J 作为 BACnet 标准的附件，成为美国国家标准。附件 J 详细规范了使用 TCP/IP 协议通信的设备组建 BACnet 网络的技术，并且将这种网络称之为 BACnet/IP 网络，简称 B/IP。附件 J 中对 BACnet/IP 网络的定义是这样的，BACnet/IP 网络是由一个或者多个 IP 子网络组成的集合，其中整体具有一个单独的 BACnet 网络号。BACnet/IP 规范的内容有七个部分，它们分别是：

- (1) 提出并详细描述由一个或者多个 IP 子网组成的 BACnet 网络的概念。
- (2) 详细描述了使用 BACnet 非确认服务进行在 BACnet/IP 网络和非 BACnet/IP 网络之间的本地、远程和全局广播的管理。
- (3) 定义了一个新设备，称为 BACnet 广播管理设备(BBMD)，用来进行广播管理。
- (4) 通过定义一个新的协议层，称为 BACnet 虚拟链路层(BVLL)，实现 BACnet/IP 通信。



- (5)提供了“外来”设备接入 BACnet/IP 网络的方法。
- (6)规定了在 BACnet/IP 网络和非 BACnet/IP 网络之间的路由。
- (7)规定了多个 BACnet/IP 网络之间的路由。

BACnet/IP 网络是由一个或者多个具有 IP 域名的子网组成的、具有一个单独的 BACnet 网络号的集合网络。BACnet 互联网由两个或者多个 BACnet 网络组成，这里的 BACnet 网络是 BACnet/IP 网络，BACnet 的以太网，BACnet 的 ARCNET 网络，BACnet 的主从/令牌传递网络和 BACnet 的 LonTalk 网络。BACnet/IP 能够比 PAD 设备更有效地处理在 IP 网络上进行 BACnet 广播传输。BACnet/IP 允许设备从因特网的任何地方接入系统，并且支持“纯 IP”的 BACnet 设备，所谓纯 IP 设备是指那些使用 IP 帧而不是 BACnet 帧来装载要传送的 BACnet 报文的单一控制器，这样，它就可以有效地利用因特网甚至是广域网作为 BACnet 局域网。

图 7-3 所示为 BACnet/IP 网络报文格式。MAC 域是下层网络帧的地址。BIP 域分为两部分，前面一部分是 20 个字节的标准 IP 数据报的头部固定部分，包含有各 4 个字节的源和目的 IP 地址，后面一部分是 8 个字节的标准 UDP 数据段的头部，包含有各 2 个字节的源和目的 UDP 端口号。BVLCI 域是 BACnet 虚拟链路控制信息域。NPCI 是网络层协议控制信息域。APDU 是应用层协议数据单元。从因特网的网络层的观点来看，BACnet/IP 网络报文是一个 IP 数据报，从因特网传输层的观点来看，它是一个 UDP 数据段，从而可以在因特网中很好地被传输。

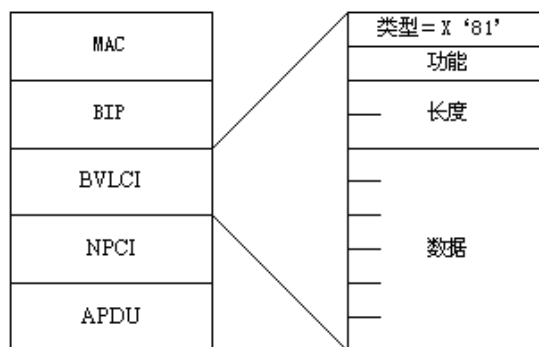


图 7-3 BACnet-IP 网络报文格式

UDP 是极其简单的协议，它仅仅只提供一个 2 字节的数字，称之为“UDP 端口”，用来通知接收系统在下面的 UDP/IP 帧中是什么报文或者什么协议。UDP 端口号 47808 标示 BACnet 报文，也是 PAD 设备使用的 UDP 端口号。BACnet/IP 设备缺省使用这个端口号，但是如果必要，许多设备也可以重构使用其它的端口号。图 7-4 示出了一个 BACnet/IP 报文实例。从图中我们可以看到，BACnet/IP 设备将 BACnet 报文（在本实例中，这个报文是一个远程设备管理服务中的 I-Am 广播应答报文），加上一些控制信息，整体作为 TCP/IP 协议中的 UDP 报文的数据段，封装进入 IP 帧中。每个 BACnet/IP 设备都具有一个 IP 地址，是一个 IP 网络设备，而它的上层应用又是按照 BACnet 协议进行组织的，可以与其它的 BACnet 设备进行数据“对话”。

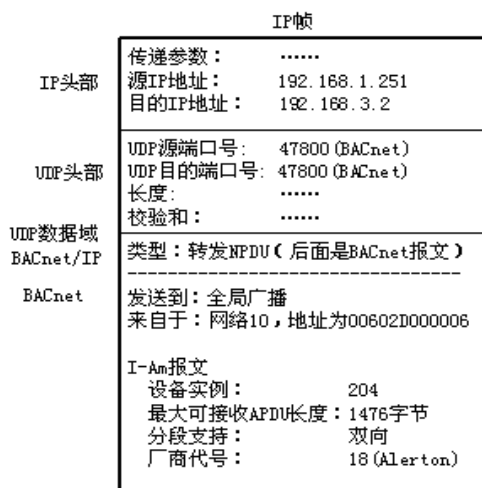


图 7-4 智能小区中的 BACnet 互联网

BACnet/IP 设备在进行读数据值、传输文件、或者其它的设备与设备间通信时，可以在 IP 互联网中直接传输报文。由于 IP 网络本身并不支持 BACnet 类型的广播，BACnet/IP 协议提供两个解决在 IP 网络中进行 BACnet 广播的方法。第一个称之为“组播(multicast)”，第二个称之为“BACnet/IP 广播管理设备”(BBMD)。

组播是一种特殊类型的广播，它标明了那些接收报文的设备。一个组播报文有一个特殊形式的目标地址，称之为组播地址。IP 组播地址范围是 224.0.0.0 到 239.255.255.255。组播报文通过互联网传送，但是只有那些被标明组播地址的设备才接收和处理组播报文。

BBMD 将由一个 BACnet/IP 设备在其子网内发送的 BACnet 广播报文直接传送给其它子网中的 BACnet/IP 设备。这些报文到达目标子网后，在子网内广播。有两种方法可以用于 BBMD 将一个报文广播到一个远程子网，一种是直接广播方法也称为一跳方法。在一跳方法中，报文有一个地址，可以使得连接到目标的 IP 路由器向该子网广播报文。如果路由器没有广播功能，则必须使用两跳方法。报文先被广播到目标子网中的对等 BBMD 中，再被广播到子网中。为了将 BACnet/IP 设备广播报文发送到虚拟网中的所有其它的 BACnet/IP 设备中，每个具有 BACnet/IP 设备的子网都必须有一个 BBMD。BBMD 保持一个列表，称之为广播分配表，其中列出了在虚拟网络中的所有的 BBMD，包括它自己。这个列表在虚拟网中的所有的 BBMD 中都是一样的。

## § 7.4 BACnet/IP 和 BACnet 设备的混合网络

可以在一个 BACnet/IP 网络中同时运行 BACnet、BACnet/IP 和 PAD 设备，但是必须遵守三个规则。

第一个规则是，BACnet 设备和 BACnet/IP 设备不能互相直接进行通信，它们之间的报文必须通过一个 BACnet-to-BACnet/IP 路由器进行路由才能传递给对方。如果 BACnet 设备和 BACnet/IP 设备同时存在于同一个物理网络中，例如以太网，则该网络要有两个 BACnet 网络号，一个为 BACnet 设备所用，另一个为 BACnet/IP 设备所用。

第二个规则是，BACnet/IP 设备不能直接与 PAD 设备进行通信，必须使用一个 BACnet-to-BACnet/IP 路由器连接到 BACnet 互联网中。

第三个规则是，BACnet 关于在任何两个设备之间必须只有一条路径的要求要被满足。

图 7-5 示出了由 BACnet/IP 设备和 BACnet 设备组成的混合网络的工作原理。其中，网络 201 和网络 203 是 BACnet 网络，通过隧道技术(PAD)与其它网络组成 BACnet 互联网。网络 202 和网络 204 是 BACnet/IP 网络，它们的设备向网络上发送的是 IP 帧，它们通过 IP 路由器可以直接连接到因特网中构成 BACnet 互联网。在网段 2 和网段 3 分别都同时存在 BACnet/IP 设备和 BACnet 设备，这两个网段分别都具有两个 BACnet 网络号，而它们各自中的两种设备之间进行数据通信时，需要有 BACnet-to-BACnet/IP 路由器进行链接。

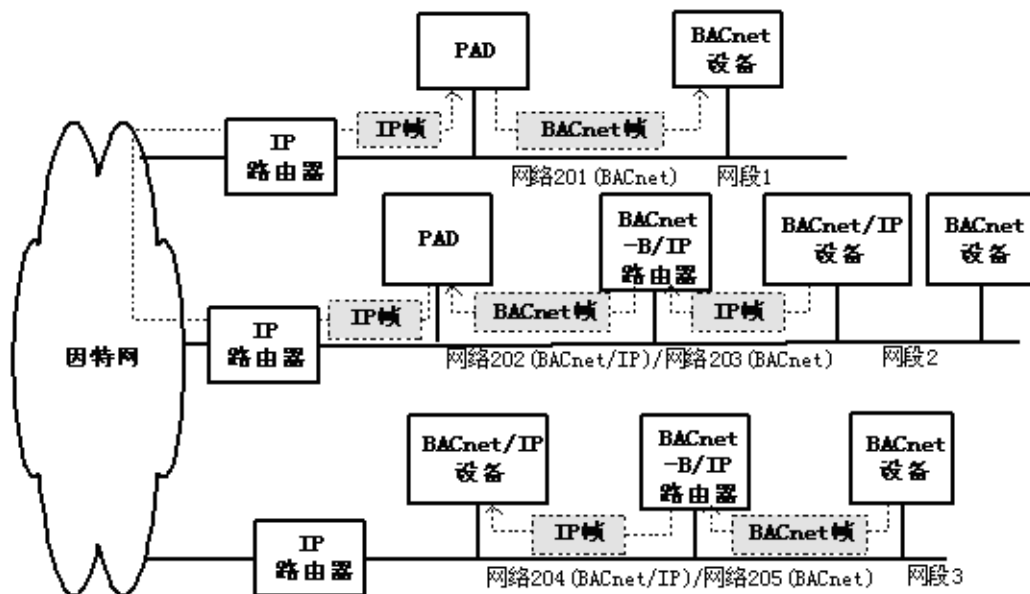


图 7-5 BACnet-IP 与 BACnet 设备组成的混合网络

因特网在世界范围内的广泛使用，使得 IP 网络技术成为目前和今后建立和运行通信网络的主流技术，同时也使得利用因特网建立大范围的 BACnet 系统成为可能。ASHRAE 不失时机地制定出 BACnet 标准附件 H 和附件 J，规范出应用 IP 网络技术和因特网建立扩展的 BACnet 系统的技术，为大规模地应用 BACnet 技术奠定了基础。

## 【主要参考文献】

1. ANSI/ASHRAE Standard 135-1995:BACnet-A Data Communication Protocol for Building Automation and Control Networks, American Society of Heating, Refrigerating, and Air-conditioning Engineer, Atlanta, Georgia, USA. (1995)
2. Bill Swan, Building Wide-Area Networks with BACnet (Part 1), <http://www.bacnet.org/Bibliography/ES-7-99/IPPART1.HTM>
3. Bill Swan, Building Wide-Area Networks with BACnet (Part 2), [www.bacnet.org/Bibliography/ES-7-99/IPPART2.HTM](http://www.bacnet.org/Bibliography/ES-7-99/IPPART2.HTM)
4. Bill Swan, The Language of BACnet-Objects, Properties and Service, [http://www.alerton.com/Products/BACtalk/About\\_Bacnet/Articles/langbac.asp](http://www.alerton.com/Products/BACtalk/About_Bacnet/Articles/langbac.asp)
5. 董春桥编著, 智能楼宇 BACnet 原理与应用, 电子工业出版社, 2003 年 3 月第 1 版
6. Steven T. Bushby, BACnet™ – A standard communication infrastructure for intelligent buildings, *Automation in Construction*, Vol. 6 No.5-6, 1997, p. 529-540
7. Steven T. Bushby, New tools for specifying BACnet, *ASHRAE Journal*, March 2002
8. David G. Holmberg, BACnet Wide Area Network Security Threat Assessment, National Institute of Standard and Technology, U.S DEPARTMENT OF COMMERCE, July 2003
9. Douglas E. Comer Computer Networks And Internets, 清华大学出版社, 1997.11
10. 黄志超, 楼宇自控网 BACnet. 工程设计 CAD 与智能建筑. No.26, 1999
11. 刘贤德, 石岩, 惠晓实, BACnet 的体系结构 BACnet 协议标准技术系列讲座一, 工程设计 CAD 与智能建筑, 1999 年第 9 期
12. 石岩, 刘贤德, 惠晓实, BACnet 应用层规范——BACnet 协议标准技术系列讲座(二), 工程设计 CAD 与智能建筑, 1999 年第 10 期
13. 惠晓实, 刘贤德, 石岩, BACnet 网络层规范 BACnet 协议标准技术系列讲座(三), 工程设计 CAD 与智能建筑, 1999 年第 11 期
14. 惠晓实, 刘贤德, 石岩, BACnet 数据链路/物理层规范 BACnet 协议标准技术系列讲座(四), 工程设计 CAD 与智能建筑, 1999 年第 12 期
15. 惠晓实, 刘贤德, 石岩, BACnet 的服务——BACnet 协议标准技术系列讲座(6), 工程设计 CAD 与智能建筑, 2000 年第 2 期
16. 惠晓实, 刘贤德, 金鑫, BACnet/IP:BACnet 的互联网扩展(上)——BACnet 协议标准技术系列讲座(7), 工程设计 CAD 与智能建筑, 2000 年第 3 期
17. 惠晓实, 刘贤德, 金鑫, BACnet/IP:BACnet 的互联网扩展(上)——BACnet 协议标准技术系列讲座(7), 工程设计 CAD 与智能建筑, 2000 年第 4 期
18. 艾顿 BACTalk 楼宇自控系统应用手册, <http://affaxx.lxwl.cn/soft/show.asp?id=342>