

Internet Engineering Task Force (IETF)

Request for Comments: 7228

分类: 信息

ISSN: 2070-1721

C. Bormann

Universitaet Bremen TZI

M. Ersue

Nokia Solutions and Networks

A. Keranen

Ericsson

2014年5月

## 《受限节点网络的术语》

### 概述

严重受制于电源，内存和处理器资源的小型设备所组成的网络我们叫做“受限节点网络”。受限节点网络(constrained-node networks)越来越多的开始使用互联网协议簇(Internet Protocol Suite)。这个文档提供了一些基本术语，可以用在“受限节点网络”的标准化制定过程中。

### 备忘录当前状态

这份文档不是一份标准的Internet Standards Track文献;它被发表用作正式信息参考。

这篇文档是Internet Engineering Task Force (IETF)的成果。它代表了IETF社区的一致意见。它已经接受了公开审核并通过了Internet Engineering Steering Group (IESG)的公开发行人许可。并不是所有被IESG批准的文档最终都会成为互联网标准;请查看RFC 5741的第二节。

关于这个文档的当前状态，任何勘误，和如何提供反馈都包含在<http://www.rfc-editor.org/info/rfc7228>中。

### 版权声明

Copyright (c) 2014 IETF Trust和在文档中指定的人都是本文档的作者。我们保留所有的权利。

这篇文档受BCP 78条款和IETF文档中的”Trust’s Legal Provisions”(http://trustee.ietf.org/license-info)合同的约束。请仔细阅读，它们描述了你对于这篇文档的权利和限制。从这篇文档中导出的代码必须遵守《Simplified BSD License》条款中的第4.e节：Trust Legal Provisions，并且保证根据《Simplified BSD License》以免费的方式使用。

—

## 目录

### 1, 介绍

### 2, 核心术语

#### 2.1 受限节点

#### 2.2 受限网络

##### 2.2.1 有缺陷的网络

#### 2.3 受限节点的网络

##### 2.3.1 LLN

##### 2.3.2 LoWPAN, 6LoWPAN

### 3, 受限设备的分类

### 4, 电源术语

#### 4.1 度量单位

#### 4.2 能源受限的分类

#### 4.3 使用电力进行通讯的策略

### 5, 安全考虑

### 6, 鸣谢

### 7, 正式参考

—

## 1, 介绍

所谓的“受限设备”，就是指只有有限的CPU，内存和电源资源的小型设备(通常用作传感器/驱动器, *Smart Objects*, 或者智能设备)。它们可以组成一个网络，在这个网络中它们被称做“受限节点”。由“受限设备”组成的这个网络本身可能也是受限的，比如，使用不稳定或容易丢包的信道、有限的和无法预测的带宽，和高度动态的网络拓扑。

受限设备可能负责在多种环境下收集信息，包括自然环境、楼宇和工厂。它们将这些信息发送到一个或多个服务器站点。它们也可能需要在对某些信息做出响应，比如执行一些物理动作，包括显示这些信息。受限设备可能工作在严重的受限资源下，比如有限的电池和计算能力，小内存和无线带宽的不足。网络中的其他实体，比如，一个基站或者控制服务器，可能有更多计算和通讯资源，可以帮助受限设备与传统网络上的应用程序直接进行交互。

当今，各种有着不同资源和能力的受限设备正在逐渐连接起来。移动个人配件，办公自动化设备，蜂窝手机，设备到设备(M2M)装置等设备开始与附近或互联网上的"things"的交互中受益。因此，IoT开始成为现实，并通过唯一ID和可以被寻址到的对象(things)来构建的。连接互联网的受限设备在下个10年会增长为非常大的数量[FIFTY-BILLION]，这将会极大增加互联网的大小和范围。

这个文档提供一系列在受限网络的标准化工作中的常用基本术语。文档的目标并不是彻底覆盖这些领域，而是要保证在不同的组织和公司中对核心术语的使用是一致的。

在这篇文档中，术语“byte”与“octet”在当今语境中是同义词。半导体内存的大小被提到时，前缀kibi被合并成“byte”to“kibibyte”，简短称作“KiB”，用作1024bytes[ISQ-13]。

在计算机行业中，术语“power”被经常使用在“计算power”或者“处理power”，用作CPU性能。在本文中，除非有特别声明，“power”指电源。“主电源(Main-powered)”是永久连接到稳定电源网络的缩写。

## 2, 核心术语

IoT有两个重要扩展方向：

- 使用不昂贵的节点将传统互联网的技术向上扩展到一个很大的量级，同时
- 向下扩展这些节点的能力和网络，让它们向上扩张更加经济和物理上更加可行。

向下扩展所需要的特性构成了所谓的“受限节点”。

## 2.1, 受限节点

对比一些常见的传统互联网节点可以得到“受限节点”的术语定义。

受限节点：一个节点它的一些属性在写的时候是不能够达到，这通常是因为成本受限和或者物理受限所导致的一些特性：比如尺寸，重量，可用的电源和能量。电源，内存和处理资源有限，导致了状态存储，代码空间和处理循环的硬性限制。这使得在所有的设计需求中，电源优化和网络带宽使用都是主要考虑的目标。同时，“受限节点”可能缺乏一些二层服务，比如完全连接和广播/多播。

虽然这不是一个严格的定义，它定义的比较模糊，但清楚地区分了“受限节点”与服务系统、桌面或笔记本电脑、强大的移动设备如智能手机等设备。这些受限可能有很多是在设计时引入的，包括售价，尺寸，重量和其他扩展因素。

导致节点受限的因素很多。这些因素通常会同时出现的，比如：

- 受限于最大代码复杂度(*ROM/Flash*)，
- 受限于状态空间大小和缓存(*RAM*)，
- 在一定时间里面完成计算的可行性上受限，处理能力弱，
- 受限于可用电源方面，
- 受限于用户界面和部署方面(有能力去设置*keys*，更新软件等)。

第三节用前两个因素作为标准将“受限节点”进行了一个分类(“class-N”，N=0, 1, 2)。在可用电源方面，[RFC6606]区分了“供电充足”节点(主电源或者常规充电)与“供电受限”节点。“供电充足”节点，它们可以从主电池或者使用能源收集器来获得能源；更多有关电源的术语在第四节中会详细介绍。

使用受限节点组成网络通常会导致网络也是受限的。但是，网络受限原因可能与这些节点是没有关系的。我们随后将会辨别“受限网络”和“受限节点的网络”。

## 2.2, 受限网络

我们也使用同样的方法来定义“受限网络”：

受限网络：它的一些特性与传统互联网的链路层是一样的。但是，在一定时间里面是不能写入的。

可能包括下面的受限因素：

- 可以达到的比特率/吞吐量低(包括周期性循环的限制)，
- 包丢失率高和包丢失的可能性高(到达率)，
- 高的不对称的链接特性，
- 使用比较大的数据包会有严重后果(例如，因为链路层分片而导致高的包丢失率)，
- 数据到达率可能会受时间影响(一些设备会关闭电源，但是定期可以会唤醒，然后进行通讯一阵子)，
- 缺乏(或者严重受限于)一些高级服务，比如IP多播。

我们说“受限网络”的时候，通常在网络中的受限节点展现出这样的特性：

另外，可以有一些原因是针对这个：

- 在网络上的经费有限，
- 节点是受限的，
- 物理受限(比如，电源受限，环境受限，媒介受限比如在水下操作，用在非常高的分辨率的有限频谱，电磁兼容性)，
- 监管受限。比如有非常有限的频谱可用性(比如在辐射能力和周期性循环)或者防爆，
- 技术受限，比如依然在使用更老的和更低速技术，可能需要用很长时间。

### 2.2.1, 有缺陷的网络

受限网络并不一定是“缺陷网络”[FALL]:

缺陷网络：应用程序希望使用端对端的IP传输模型，但是网络有很难去完成。举例来说：

- 不能提供一个端对端IP链接，
- 在端对端IP链接显示出严重中断的特点，
- 严重延迟，并超出TCP定义的最大段生存时间(MSL)[RFC0793]

某种意义上，所有缺陷网络是受限网络。但是不是所有的受限网络是缺陷网络。在这两个网络中没有一个非常明确的边界。针对缺陷网络已经有了处理方法：延迟容忍网络(DTN)[RFC4838]。

### 2.3, 受限节点的网络

受限节点网络：这个网络的特点会主要被“受限节点”的特性影响。

一个受限节点网络通常是一个受限网络。因为节点受限导致网络也受限和堵塞。另外，“受限节点网络”也可能有其他方面的受限。

在本章的其他段中描述在受限节点网络使用中的两个额外术语。不需要额外去定义它们：LLN和(6)LoWPAN。

### 2.3.1, LLN

术语LLN已经被描述成IETF ROLL工作小组的目标，它指“低功耗和有损网络”(LLN:Low-Power and Lossy Network)。ROLL(Routing over Low-Power and Lossy)术语文档[RFC7102]中对LLNs做出了如下定义：

LLN：低功耗和有损网络。通常很多嵌入式设备使用有限电源，内存和处理资源组成了一个连接，比如IEEE 802.15.4或者低功耗Wi-Fi。很多大范围的应用程序用作LLN，包括工业监控，建筑自动化(加热，空气流通和空调，灯光，访问控制，或灾报警)，连接家庭，健康，环境健康，城市传感网络，能源管理，资产追踪，冷链。

TODO 在这些之上，LLN通常表现出在物理层上的一些丢失，使用明显变量在传递速率，一些短时间的不可达，配合一些长时间的稳定，让它在构建直接无环图，是中等属于稳定，用作路由，和做测量在，比如ETX[RFC6551]。并不是所有的LLN由低功耗节点组成；这个导致操作模式的设计，比如“无存储模式”由RPL设计(IPV6路由协议用作低功耗和丢失网络[RFC6550])。所有，在这个当前文档的术语中，一个LLN是一个受限节点网络使用一定网络特性，包括在网络上受限。

### 2.3.2, LoWPAN, 6LoWPAN

一个受限网络的有趣的类型被用作受限节点网络是“LoWPAN”[RFC4919]，一个术语由IEEE802.15.4工作小组所定义的(LR-WPANs)。解释LoWPAN是，“低功耗无线个人区域局域网”，包含一个很难去界定的词“个人”，因为IEEE 802工作小组在定义的时候有一个目标是定义LoWPAN是围绕个人设计的。准确的说，LoWPANs已经被建议成城市监控，大楼控制和工业控制程序，所以”个人“这个词可以被认为是过时了。偶尔，术语又被称为低功耗无线网络[WEI]。通常关注于IEEE 802.15.4，“LoWPAN”指在受限网络下的链路层网络技术[V6-BTLE][V6-DECT-ULE][V6-G9959]

## 3, 受限设备种类

尽管，绝大部分与互联网链接的设备可以被想象的，它可能是值得的去对不同类型的受限设备有一些简洁的术语定义。在这个文档中，表1中的文章，可能会用在一个相对开放的设备能力定义：

名称	大小的数据（例如， <b>RAM</b> ）	代码的大小（例如，闪存）
0类，C0	< < 10 KIB	< < 100 KIB
1类，C1	~ 10 KIB	~ 100 KIB
2类，C2	~ 50 KIB	~ 250 KIB

表1：受限设备类型（KiB = 1024字节）

作为本文件的写作，这些特征可以区分商业芯片集群和为受限设备的设计核心。虽然预计，这些类的边界会随着时间的推移，摩尔定律往往是在嵌入式空间比个人计算设备不太有效：取得可用晶体管数量的增加和密度更容易投入的成本和功耗的要求比减少到计算能力的不断提高。

0类设备是非常受限的传感器。他们是如此的严重受限的存储和处理能力，以至于不具有可以与互联网直接的、安全的沟通所需的资源。0类设备与互联网通信需要更大的设备来帮忙比如代理，网关，或服务器。0类设备通常不能安全或者进行复杂的管理。他们最可能是使用一个非常小的数据集预先配置好了（然后很少再配置）。为了管理的目的，他们可以响应keepalive信号发送/关闭或基本健康指标。

1类设备在代码空间和处理能力相当的限制，使得它们不能很容易地与其他网络节点沟通，采用一个完整的协议栈，如使用HTTP，传输层安全（TLS），及相关的协议和基于XML的数据表示。然而，他们有足够的力量来使用一个协议栈，专为受限节点设计的协议（如使用UDP的受限的应用协议CoAP），在没有网关节点的帮助下进行一定的通讯。特别是，他们可以提供大型网络所要求的安全功能的支持。因此，他们可以集成到IP网络，但他们需要简单的状态存储，代码空间，并经常耗电的协议和应用程序使用。

2类设备的限制较少，基本上能够支持大多数相同的协议栈上使用笔记本电脑或服务器。然而，即使这些设备可以由轻质、节能协议和消耗更少的带宽效益。此外，使用较少的网络资源留下更多的可用资源的应用。因此，利用协议栈更受限的设备，对2类设备的定义可能会降低开发成本和提高互操作性。

受限的设备和能力显然超越2类设备存在。他们不太苛刻的标准发展点，他们可以在很大程度上利用现有的协议不变。本文件，因此不做任何尝试定义类超过2类。这些设备仍然可以通过有限的能源供应的限制。

4， 电源术语

设备不只可以从它们的计算能力上进行区分，也可以在可用电源和(或)能量上进行区分。在可用电源和能量这个层面上很难去找到可量化的分类方法，但引入一些通用术语还是非常有用的。

4.1， 度量单位

一个设备可用电源或可用能量的计量单位可能是不同的，从千瓦到毫瓦，从基本无限制到上百微焦耳。

我们使用国际标准单位(SI单位)简单陈述下可用电源或可用能量，而不是定义一个类和簇。在表2中定义了一个或两个相似值。

名字	定义	国际标准度量
Ps	可持续平均功率可用用在设备上，当它被调用	W(Watt)
Et	全部电量当电量来源被消耗后所有电源能量	J(Joule)

表 2: 有关电源和能量的度量

TODO 值Et可能需要在与时间的价值时间指示结合解释了；见4.2节。

TODO 一些设备在可用能量耗尽之前会进入“low-power”模式。对于这些设备，Ps需要为每个给定的模式/步骤。

4.2， 能源限制的分类

正如上面所讨论的，一些设备是有限的可用能源作为反对（或除了）是可用电源有限公司。在没有有关存在的局限性，对能量的装置，分为E9。能量限制可以在设备的使用寿命总有效能量（例如，一种装置，被丢弃时不可替代的原电池耗尽），分为E2。在相关的限制是为一个特定的时期，该装置分为E1，例如，太阳能装置与有限数量的可用于夜间的能量，一个是手动连接到充电器和充电装置之间的一段时间，或用一个



周期性的装置（初级）电池更换间隔。最后，有可能是一个有限的能量可用于一个特定的事件，例如，在能量收集光开关按下一个按钮；这样的设备分为E0。需要注意的是，在某种意义上，许多设备也E2 E1，为可再充电电池具有有限数量的有用的充电周期。

表3提供上述分类的总结。

名称	能量限制的类型	电源来源示例
E0	事件能量受限	定期收集能量
E1	定期能量受限	电池，需要定期充电或更换
E2	生命周期能量受限	一次性，无需更换电源
E9	对可用能量没有直接的配额限制	主电源

表 3: 能量限制的级别

4.3，使用电力进行通讯的策略

特别是当使用无线传输的时候，无线电通常会占到设备总耗电量的很大一部分。设计参数，比如可用频谱，所需的范围和目标比特率，都在传输和接受的过程中影响电量消耗；传输和消耗的间隔(包括潜在的接受)也会影响全部的总消耗能量。

基于不同的能源来源(比如电池和主电源供电)和设备需要通讯的频率，可能会使用不同的电源使用和网络连接策略。

通常电源使用的策略可以描述如下：

**Always-on**：如果没有节能的要求，这种策略是最适用的。设备可以在所有的时间都以正常状态工作。可能会使用省电的硬件或者限制一定数量的无线传输，CPU速度和其他为了常用的省电和散热要求的手段，但是设备需要一直连接到网络。

**Normally-off**：在这个策略下，设备一次会休眠很长时间。一旦它醒来，它不会假装它已经连接到网络中：设备会在它被唤醒的时候重新连接网络。主要优化目标是减少重连的时候所需要的努力和由此产生的任何应用程序的通信。

如果设备休眠很长一段时间，需要的沟通不是很频繁，在重连过程中的能量消耗相对增加可能也是可以接受的。

**Low-power:** 这种策略通常适用与需要在低功耗，但仍需进行一个相对频繁通讯的设备。这意味着，超低功耗的解决方案需要使用在这些硬件上，和链路层选择机制等等。通常情况下，相比它们的休眠时间，传输只使用了很短的时间，这些设备依然保持某种形式可以连接到网络。用于减少网络通信电源使用的技术包括唤醒后减少重新建立连接的能耗和调整的通信频率（包括“周期性循环”，其中在一个循环周期中，组件交换在有规律的循环和关闭）和其他适当的参数。

下表4提供使用电源进行通讯的策略

名称	策略	通讯时机
P0	Normally-off	当需求的时候连接
P1	Low-power	看似连接
P9	Always-on	始终连接

请注意，上述讨论的是在设备层面；类似的考虑也适用于通信接口层。这个文档没有定义后面的术语。

一个经常使用的术语来描述的省电方法是“周期性循环(Duty Cycle)”。这描述了各种形式的周期性开关一些功能。

[RFC7102]只能区分两个级别，定义一个非休眠的节点始终保持在在完全供电状态（一直醒着），它有能力执行通信（P9）和一个休眠的节点，有时可能会进入睡眠模式（低功耗状态，以节省电力）和暂时中止协议通信（P0）；没有明确提及P1。

5，安全考虑

本文档介绍了常见的术语，不会增加任何新的安全问题。因为受限所产生的安全方面的考虑需要在特定的协议下进行讨论。例如，[COAP]的11.6节，“受限节点的考虑”，探讨了在受限情况下对使用安全机制的影响。[ROLL-SEC-THREATS]为RPL路由协议提供了安全威胁分析。在[IKEV2-MINIMAL]和[TLS-MINIMAL]有讨论受限节点的安全协议的实现问题。在[IOT-SECURITY]提供如何使受限节点网络更安全的观点。

## 6, 鸣谢

Dominique Barthel and Peter van der Stok提供了有用的意见；Charles Palmer提供一个全面的编辑审查。

Peter van der Stok坚持认为我们应该包含电源的术语，因此出现了第4节。4.3节很大一部分是从以前的一个版本[COAP-CELLULAR]中拿出来的，已被改编为这个文件。

## 7, 正式参考

[COAP] Shelby, Z., Hartke, K., and C. Bormann, “Constrained Application Protocol (CoAP)”, Work in Progress, June 2013.

[COAP-CELLULAR] Arkko, J., Eriksson, A., and A. Keranen, “Building Power-Efficient CoAP Devices for Cellular Networks”, Work in Progress, February 2014.

[FALL] Fall, K., “A Delay-Tolerant Network Architecture for Challenged Internets”, SIGCOMM 2003, 2003.

[FIFTY-BILLION] Ericsson, “More Than 50 Billion Connected Devices”, Ericsson White Paper 284 23–3149 Uen, February 2011,  
<http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf>.

[IKEV2-MINIMAL] Kivinen, T., “Minimal IKEv2”, Work in Progress, October 2013.

[IOT-SECURITY] Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., and R. Struik, “Security Considerations in the IP-based Internet of Things”, Work in Progress, September 2013.

[ISQ-13] International Electrotechnical Commission, “International Standard – Quantities and units – Part 13: Information science and technology”, IEC 80000–13, March 2008.

[RFC0793] Postel, J., “Transmission Control Protocol”, STD 7, RFC 793, September 1981.

[RFC4838] Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant Networking Architecture", RFC 4838, April 2007.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J.P., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC6551] Vasseur, J.P., Kim, M., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, March 2012.

[RFC6606] Kim, E., Kaspar, D., Gomez, C., and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing", RFC 6606, May 2012.

[RFC7102] Vasseur, J.P., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, January 2014.

[ROLL-SEC-THREATS] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)", Work in Progress, December 2013.

[RPL-DEPLOYMENT] Vasseur, J., Ed., Hui, J., Ed., Dasgupta, S., and G. Yoon, "RPL deployment experience in large scale networks", Work in Progress, July 2012.

[TLS-MINIMAL] Kumar, S., Keoh, S., and H. Tschofenig, "A Hitchhiker's Guide to the (Datagram) Transport Layer Security Protocol for Smart Objects and Constrained Node Networks", Work in Progress, March 2014.

[V6-BTLE] Nieminen, J., Ed., Savolainen, T., Ed., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "Transmission of IPv6 Packets over BLUETOOTH Low Energy", Work in Progress, May 2014.

[V6-DECT-ULE] Mariager, P., Ed., Petersen, J., and Z. Shelby, “Transmission of IPv6 Packets over DECT Ultra Low Energy”, Work in Progress, July 2013.

[V6-G9959] Brandt, A. and J. Buron, “Transmission of IPv6 packets over ITU-T G.9959 Networks”, Work in Progress, May 2014.

[WEI] Shelby, Z. and C. Bormann, “6LoWPAN: the Wireless Embedded Internet”, ISBN 9780470747995, 2009.

### **Authors' Addresses**

Carsten Bormann

Universitaet Bremen TZI

Postfach 330440

D-28359 Bremen

Germany

Phone: +49-421-218-63921

Email: [cabo@tzi.org](mailto:cabo@tzi.org)

Mehmet Ersue

Nokia Solutions and Networks

St.-Martinstrasse 76

81541 Munich

Germany

Phone: +49 172 8432301

Email: mehmet.ersue@nsn.com

Ari Keranen

Ericsson

Hirsalantie 11

02420 Jorvas

Finland

Email: ari.keranen@ericsson.com

### *翻译贡献声明*

WildDog技术小组(github:WildDogTeam)对此文档进行了翻译。翻译后的内容不得用于任何商业用途。文档维护者联系方式: github:macliu010, mac.liu@wilddog.com。

本文采用Markdown语言, 使用IA Writer Pro编辑器并生成PDF。

在此对IETF和此文的原作者表示致敬。