阿里云
IoT Link Rack 一体机
物联网平台

产品简介

产品版本：V1.1.0

文档版本：20200622

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意：** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击**设置** > **网络** > **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	表示参数、变量。	bae log list --instanceid Instance_ID
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig [-all|-t]
{}或者{a|b}	表示必选项，至多选择一个。	switch {active|stand}

目录

1 IoT Link Rack 产品简介

1.1 什么是IoT Link Rack

IoT Link Rack是阿里云IoT推出的一款集成了物联网平台（Link Platform）、物联网边缘计算（Link IoT Edge）、物联网络管理（Link WAN）、IoT设备身份认证（Link ID²）和IoT安全运营中心（Link SOC）共5款云产品的软硬一体机柜，可包含5台~9台服务器。

一体机优势

一体机是端到端的交付解决方案，通过定制软件和硬件相结合，做到预先定制、集成、测试和优化，实现快速部署和交付，简化企业IT架构，并提升后续系统可用性和运维效率。

优势	说明
统一硬件配置	• 一站式交付，即开即用。 • 后期统一维护硬件。
统一软件管控	• 软、硬件协调加速，应用集成调优。 • 全方位软硬件监控，智能运维。
面向客户需求灵活集成	• 弹性可扩展，资源按需配置。 • 一体机支持扩展部署业务应用。

适用场景

适用一体机的用户包含政府、高校、医院、运营商、银行、能源企业等。

一体机可满足以下场景：

- 需要建设自己的物联管理平台。
- 本地核心数据不能上云。
- 对部署成本控制有具体要求。
- 希望软硬一体交付运维。

1.2 产品架构

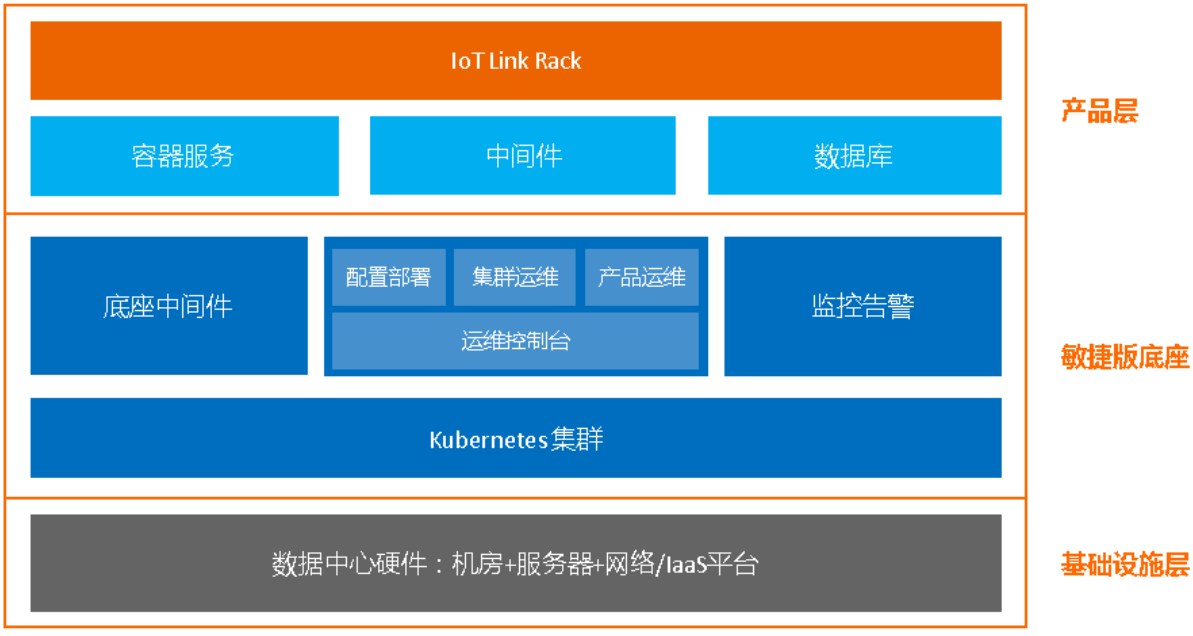
本章节介绍一体机的产品架构。

一体机产品架构如下图所示。

1.3 部署架构

本章节介绍一体机整体的部署架构。

一体机的部署架构如下图所示。



1.4 硬件配置清单

本章节介绍一体机所需的硬件配置。

配置	型号	数量	是否必选	说明
服务器	PN67M1P1.2B	5~9	是	• 使用AOC线缆，设备无需配置光模块。 • 机柜里已包含导轨和电源线，无需额外配置。
交换机	CN61108PC-V-H	2	是	N/A
交换机	S5560-24TQ-AC	1	是	N/A

具体配置清单：

硬件	配置	数量
PN67M1P1.2B	• CPU：6230*2 • 内存：32G × 12 • 硬盘：所需硬盘规格和数量说明如下。 - 3.5''，SATA 6G，SATA，7200rpm，8T × 9 - 2280，SATA 6G，m.2，RI，0.24T × 2 - 2.5''，nvme，u.2，RI，0.96T × 2 • 网卡：2*GE+2*10GE • 配件：无额外配件	5~9
CN61108PC-V-H	支持48口10G SFP+ 光口、6口40G QSFP+光口、双电、冗余风扇（端口侧进风，后出风）。	2
S5560-24TQ-AC	支持24口千兆RJ45电口，4个10G SFP+光口，配置电源、风扇、console线	1
AOC线缆	SFP-10GB-AOC3M= 10G SFP+ 有源光缆3M-橙色	服务器数量×2
RJ45网线	6类千兆网线-RJ45-3M-红色	服务器数量+8
40G交换机堆叠线	QSFP-40GB-AOC0.5M=40G SFP+ 有源光缆0.5M-橙色	2
24U阿里定制机柜	600W*1200D*1230Hmm（含脚轮支脚），内部可用空间24U，阿里定制外观、前门定制、后门网孔双开门，带机柜附件盒、带加固包材、安装辅材	1
机柜配件	32A/220V输入，12口C13-10A插口-黑色	2

硬件	配置	数量
	2A/220V电源线，C13-C14-1m黑色	服务器数量+3
	32A/220V电源线，C13-C14-1m黄色	服务器数量+3
	理线器	3
	盲板-1U	18-服务器数量*2
整机柜服务	维保服务	可选： • 3年 • 5年 • 5*8*NBD • 7*24*4H **说明：** 目前PDU仅支持5*8*NBD维保。
	整机柜集成服务	1
	整机柜运输服务（推到指定位置）	1
	整机柜现场现场实施服务	1

1.5 软件配置清单

本章节介绍一体机的软件配置。

类别	产品	描述	是否必选	数量	单位
专有云底座	敏捷PaaS版底座	敏捷专有云部署必备，提供容器、应用管理和常用中间件。	是	1	套
	敏捷标准版底座	需要控制台部署和账号体系时选择，包含天基。	否	1	套
依赖云产品	Kafka	消息队列，用于各模块之间的消息流转。	是	1	套

类别	产品	描述	是否必选	数量	单位
	HBase	NoSQL存储，用于存储设备相关的实时和历史上报数据。	是	≥48	C
	ElasticSearch	搜索引擎，用于系统和租户日志的全文搜索。	是	≥48	C
	容器服务ACK	需要部署IoT基础产品外的行业和ISV的应用时必选。	否	1	套
IoT产品	物联网平台	LP，提供各种类型设备接入和管理运维的能力，是IoT产品的底座。	是	1	套
	物联网边缘计算	LE，提供边缘网关接入、配置规则下发和远程运维的能力。	否	1	套
	物联网络管理	LW，提供LoRa网关、节点设备接入和快速组网覆盖的能力。	否	1	套
	IoT设备身份认证	ID^2，提供设备认证连接、数据加密和密钥管理的可信接入能力	否	1	套
	IoT安全运营中心	SOC，提供识别和消除IoT系统中潜在安全风险的能力。	否	1	套

2 物联网平台

2.1 什么是物联网平台

阿里云物联网平台为设备提供安全可靠的连接通信能力，向下连接海量设备，支撑设备数据采集上云；向上提供云端API，服务端通过调用云端API将指令下发至设备端，实现远程控制。

物联网平台也提供了其他增值能力，如设备管理、规则引擎、边缘计算等，为各类IoT场景和行业开发者赋能。

物联网平台提供以下主要能力。

设备接入

物联网平台支持海量设备连接上云，设备与云端通过IoT Hub进行稳定可靠地双向通信。

- 提供设备端SDK、驱动、软件包等帮助不同设备、网关轻松接入阿里云。
- 提供2G/ 3G /4G/5G、NB-IoT、LoRaWAN、Wi-Fi等不同网络设备接入方案，解决企业异构网络设备接入管理痛点。
- 提供MQTT、CoAP等多种协议的设备端SDK，既满足长连接的实时性需求，也满足短连接的低功耗需求。
- 开源多种平台设备端代码，提供跨平台移植指导，赋能企业基于多种平台做设备接入。

设备管理

提供完整的设备生命周期管理功能，支持设备注册、功能定义、数据解析、在线调试、远程配置、固件升级、远程维护、实时监控、分组管理、设备删除等功能。

- 提供设备物模型，简化应用开发。
- 提供设备上下线变更通知服务，方便实时获取设备状态。
- 提供数据存储能力，方便用户海量设备数据的存储及实时访问。
- 支持OTA升级，赋能设备远程升级。
- 提供设备影子缓存机制，将设备与应用解耦，解决不稳定无线网络下的通信不可靠痛点。

安全能力

阿里云物联网平台提供多重防护有效保障设备云端安全。

- 身份认证
  - 提供芯片级安全存储方案（ID²）及设备密钥安全管理机制，防止设备密钥被破解。安全级别很高。
  - 提供一机一密的设备认证机制，降低设备被攻破的安全风险。适合有能力批量预分配设备证书（ProductKey、DeviceName和DeviceSecret），将设备证书信息烧入到每个芯片的设备。安全级别高。
  - 提供一型一密的设备认证机制。设备预烧产品证书（ProductKey和ProductSecret），认证时动态获取设备证书（包括ProductKey、DeviceName和DeviceSecret）。适合批量生产时无法将设备证书烧入每个设备的情况。安全级别普通。
- 通信安全
  - 支持TLS（MQTT\CoAP）数据传输通道，保证数据的机密性和完整性，适用于硬件资源充足、对功耗不是很敏感的设备。安全级别高。
  - 支持设备权限管理机制，保障设备与云端安全通信。
  - 支持设备级别的通信资源（Topic等）隔离，防止设备越权等问题。

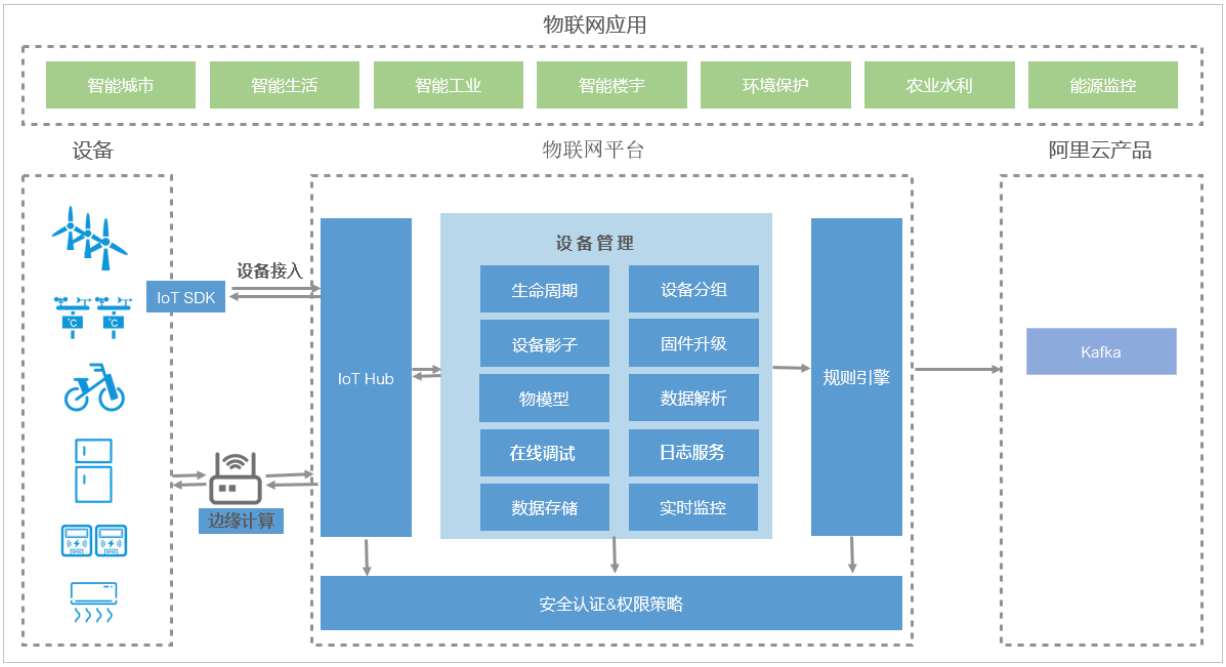
规则引擎

规则引擎提供数据流转和场景联动功能。配置简单规则，即可将设备数据无缝流转至其他设备，实现设备联动；或者流转至其他云产品，获得存储、计算等更多服务。使用规则引擎，您可以：

- 将数据转发至另一个设备的Topic中，实现设备与设备之间的通信。
- 将数据转发到消息队列（Kafka）中，实现消息的高可靠流转。
- 将数据转发到AMQP服务端订阅消费组，您的服务器通过AMQP客户端监听消费组中的消息。

2.2 产品架构

设备连接物联网平台，与物联网平台进行数据通信。物联网平台可将设备数据流转到其他阿里云产品中进行存储和处理。这是构建物联网应用的基础。



IoT SDK

物联网平台提供IoT SDK，设备集成SDK后，即可安全接入物联网平台，使用设备管理、数据流转等功能。

只有支持TCP/IP协议的设备可以集成IoT SDK。

具体请参见《物联网平台用户指南》文档中**设备接入 > 下载设备端SDK**。

IoT Hub

IoT Hub帮助设备连接阿里云物联网平台服务，是设备与云端安全通信的数据通道。IoT Hub支持PUB/SUB与RRPC两种通信方式，其中PUB/SUB是基于Topic进行的消息路由。

IoT Hub具有下列特性：

- 高性能扩展：支持水平动态扩展，架构可以支撑亿级设备连接。
- 全链路加密：整个通信链路以RSA，AES加密，保证数据传输的安全。
- 消息实时到达：当设备与IoT Hub成功建立数据通道后，两者间将保持长连接，以减少握手时间，保证消息实时到达。
- 支持数据透传： IoT Hub支持将数据以二进制透传的方式传到自己的服务器上，不保存设备数据，从而保证数据的安全可控性。

- 支持多种通信模式：IoT Hub支持RRPC和PUB/SUB两种通信模式，以满足您在不同场景下的需求。
- 支持多种设备接入协议：支持设备使用MQTT和CoAP协议接入物联网平台。

设备管理

物联网平台为您提供功能丰富的设备管理服务，包括：生命周期、设备分组、设备影子、物模型、数据存储、在线调试、固件升级、远程配置等，具体请参见《物联网平台用户指南》文档中**设备管理**的章节

规则引擎

当设备基于Topic进行通信时，您可以编写SQL对Topic中的数据进行处理，然后配置转发规则将数据转发到其他Topic或阿里云服务上进行存储和处理。例如：转发到另一个Topic中实现M2M通信。

安全认证&权限策略

安全是IoT的重要话题。阿里云物联网平台提供多重防护保障设备云端安全。

- 物联网平台为每个设备颁发唯一证书，设备使用证书进行身份验证连接物联网平台。
- 针对不同安全等级和产线烧录的要求，物联网平台为开发者提供了多种设备认证方式。
- 授权粒度精确到设备级别，任何设备只能对自己的Topic发布、订阅消息。

2.3 名词解释

本章主要介绍物联网平台中相关的名词解释。

产品名词解释

名词	描述
产品	设备的集合，通常指一组具有相同功能的设备。物联网平台为每个产品颁发全局唯一的ProductKey。每个产品下最多可以包含50万个设备。
设备	归属于某个产品下的具体设备。物联网平台为设备颁发产品内唯一的证书DeviceName。设备可以直接连接物联网平台，也可以作为子设备通过网关连接物联网平台。
分组	物联网平台支持建立设备分组，分组中可包含不同产品下的设备。通过设备组来进行跨产品管理设备。
网关	能够直接连接物联网平台的设备，且具有子设备管理功能，能够代理子设备连接云端。
子设备	本质上也是设备。子设备不能直接连接物联网平台，只能通过网关连接。

名词	描述
设备证书	设备证书指**ProductKey**、**DeviceName**、**DeviceSecret**。 • **ProductKey**：是物联网平台为产品颁发的全局唯一标识。该参数很重要，在设备认证以及通信中都会用到，因此需要您保管好。 • **DeviceName**：在注册设备时，自定义的或系统生成的设备名称，具备产品维度内的唯一性。该参数很重要，在设备认证以及通信中都会用到，因此需要您保管好。 • **DeviceSecret**：物联网平台为设备颁发的设备密钥，和DeviceName成对出现。该参数很重要，在设备认证时会用到，因此需要您保管好并且不能泄露。
ProductSecret	由物联网平台颁发的产品密钥，通常与ProductKey成对出现，可用于一型一密的认证方案。该参数很重要，需要您保管好，不能泄露。
Topic	Topic是UTF-8字符串，是发布（Pub）/订阅（Sub）消息的传输中介。可以向Topic发布或者订阅消息。
Topic类	同一产品下不同设备的Topic集合，用${productkey}和${deviceName}通配一个唯一的设备，一个Topic类对一个ProductKey下所有设备通用。
发布	操作Topic的权限类型，对应的英文名称为Pub。可以往此类Topic中发布消息。
订阅	操作Topic的权限类型，对应的英文名称为Sub。可以从此类Topic中订阅消息。
RRPC	全称：Revert-RPC。RPC（Remote Procedure Call）采用客户机/服务器模式，用户不需要了解底层技术协议，即可远程请求服务。RRPC则可以实现由服务端请求设备端，并能够使设备端响应的功能。
标签	标签分为产品标签、设备标签和分组标签。 • 产品标签：描述同一个产品下，所有设备所具有的共性信息。 • 设备标签：通常根据设备的特性为设备添加的特有标记，您可以自定义标签内容。 • 分组标签：描述同一个分组下，所有设备所具有的共性信息。
Alink协议	阿里云定义的设备与云端之间的通信协议。
物模型	是对设备在云端的功能描述，包括设备的属性、服务和事件。物联网平台通过定义一种物的描述语言来描述物模型，称之为 TSL（即 Thing Specification Language），采用JSON格式，您可以根据TSL组装上报设备的数据。
属性	设备的功能模型之一，一般用于描述设备运行时的状态，如环境监测设备所读取的当前环境温度等。属性支持 GET 和 SET 请求方式。应用系统可发起对属性的读取和设置请求。

名词	描述
服务	设备的功能模型之一，设备可被外部调用的能力或方法，可设置输入参数和输出参数。相比于属性，服务可通过一条指令实现更复杂的业务逻辑，如执行某项特定的任务。
事件	设备的功能模型之一，设备运行时的事件。事件一般包含需要被外部感知和处理的通知信息，可包含多个输出参数。例如，某项任务完成的信息，或者设备发生故障或告警时的温度等，事件可以被订阅和推送。
数据解析脚本	针对采用透传格式/自定义数据格式的设备，需要在云端编写数据解析脚本，将设备上报的二进制数据或自定义的JSON数据，转换为物联网平台支持的Alink JSON数据格式；将平台下发的Alink JSON格式数据，转换为设备支持的格式。
设备影子	是一个JSON文档，用于存储设备或者应用的当前状态信息。每个设备都会在云端有唯一的设备影子。无论该设备是否连接到Internet，您都可以使用设备影子通过MQTT协议或HTTP协议获取和设置设备的状态。
规则引擎	通过创建、配置规则，以实现数据流转和场景联动。
数据流转	物联网平台规则引擎的数据流转功能，可将Topic中的数据转发至其他Topic或其他阿里云服务进行存储或处理。
场景联动	场景联动是一种开发自动化业务逻辑的可视化编程方式。您可以通过可视化的方式定义设备之间联动规则，并将规则部署至云端或者边缘端。
一型一密	同一产品下所有设备可以烧录相同产品证书（即ProductKey和ProductSecret）。设备发送激活请求时，物联网平台进行产品身份确认，认证通过，下发该设备对应的DeviceSecret。
一机一密	每个设备烧录其唯一的设备证书（ProductKey、DeviceName和DeviceSecret）。当设备与物联网平台建立连接时，物联网平台对其携带的设备证书信息进行认证。
期望属性值	通过期望属性值功能，设置您希望的设备属性值。若设备在线，将实时更新属性值；若设备离线，期望属性值将缓存在云端。设备上线后，获取期望属性值，并更新属性值。

2.4 产品优势

企业基于物联网，通过运营设备数据实现效益提升已是行业趋势和业内共识。然而，物联网转型或物联网平台建设过程中往往存在各类阻碍。针对此类严重制约企业物联网发展的问题，阿里云物联网平台提供了一系列解决方案。

以下是传统开发与基于阿里云物联网平台开发的对比表。

-	传统开发	基于阿里云物联网平台的开发
设备接入	需要搭建基础设施，联合嵌入式开发人员与云端开发人员共同开发。 开发工作量大、效率低。	提供设备端SDK，快速连接设备上云，效率高。 同时支持全球设备接入、异构网络设备接入、多环境下设备接入和多协议设备接入。
性能	自行实现扩展性架构，极难做到从设备粒度调度服务器、负载均衡等基础设施。	具有亿级设备的长连接能力、百万级并发处理能力，架构支撑水平性扩展。
安全	需要额外开发、部署各种安全措施，保障设备数据安全是个极大挑战。	提供多重防护，保障设备数据安全。 • 设备认证保障设备安全与唯一性。 • 传输加密保障数据不被篡改。 • 云盾护航和权限校验保障云端安全。
稳定	需自行发现宕机，并完成迁移。迁移时服务会中断。稳定性无法保障。	服务可用性高达99.9%。去中心化，无单点依赖。拥有多数据中心支持。
简单易用	需要购买服务器搭建负载均衡分布式架构，需要花费大量人力物力开发”接入 + 计算 + 存储”一整套物联网系统。	一站式设备管理、实时监控设备场景、无缝连接阿里云产品。可灵活简便地搭建复杂物联网应用。

2.5 使用限制

物联网平台设置了以下使用限制。

产品与设备

限制项	描述	限制
标签个数	单个产品、设备或分组最多可以添加的标签数。	100
产品数量	单账号最多可以创建的产品数。	1,000
设备数量	单产品最多可以添加的设备数。	500,000
	单账号最多可以添加的设备数。	与购买规格相关
网关与子设备	单个网关下最多添加的子设备数。	1,500
物模型功能定义	单个产品最多可添加的功能数。	200
	struct类的属性，最多可添加的参数个数。	10
	当功能的数据类型为enum时，枚举项最多不超过100个。	100

限制项	描述	限制
	当功能的数据类型为text时，数据长度不超过2,048字符。	2,048字符
	当功能的数据类型为为array时，数组内的元素不超过128个	128
	服务中可添加的入参和出参分别不超过20个。	20
	事件中可添加的出参不超过50个。	50
	导入物模型时，文件大小不超过256 KB。	256 KB
设备分组	一个阿里云账号下最多可有1,000个分组，包括父分组和子分组。	1,000
	单个分组内最多添加20,000个设备。	20,000
	一个设备最多可以被添加到10个分组中。	10
数据解析	数据解析脚本文件大小不能超过48 KB。	48 KB
远程配置	远程配置文件，仅支持JSON格式，大小不能超过64 KB。	64 KB
数据存储时间	产品运行时，产生的属性、事件、服务数据存储时间为30天。超出30天的数据不再保存。	30天
固件升级	一个阿里云账号下最多可包含的固件数量。	500
	单个固件文件大小限制。	500MB

连接通信

限制项	描述	限制
设备接入限制	使用同一个设备证书信息（相同的Productkey、DeviceName）。在同一时间，只能和物联网平台服务器建立一个连接。	1
连接次数	单账号每秒最大MQTT连接请求数。	500
	单设备每分钟最大连接请求次数。	5
设备订阅数	单设备的最大订阅数。 超过订阅数的请求将会被直接拒绝。设备端可以通过验证SUBACK消息，确认请求是否成功。	100
请求数量	单账号每秒由设备端向物联网平台发送的请求数。	与购买规格相关
	单账号每秒由物联网平台向设备端发送的请求数。	与购买规格相关
规则引擎接收消息数	单账号每秒到达规则引擎数据流转的消息数量。	与购买规格相关
服务端订阅限流	单账号每秒通过服务端订阅可接收的最大消息数。	与购买规格相关

限制项	描述	限制
消息通信限流	单设备每秒最多可上报的消息数量。 **说明：** MQTT的Pub上报消息限流，协议上没有任何应答。您可以通过日志服务发现设备被限流的警告。	• QoS 0：30条/秒 • QoS 1：10条/秒
	单设备接收下行消息的最大限制为50条/秒，同时受限于网络环境。 如果网络tcp write buffer拥堵，将直接返回错误。通过Pub接口发指令给设备，如果设备不能及时处理，将收到限流错误。	50条/秒
带宽	单个连接每秒的吞吐量（带宽）最大限制。	1,024 KB
缓存请求数	物联网平台限制了单客户端的最大未确认入站发布请求数。 达到此限制后，除非返回PUBACK消息，否则服务器不会再接收新的客户端发布请求。	100
消息存储时长	QoS1消息的最大存储时间。 如果最大时间后，未从客户端接收到PUBACK消息，则会丢弃这些发布请求。	7天
MQTT消息长度	MQTT单个发布消息最大长度。超过此大小的发布请求将被直接拒绝。	256 KB
CoAP消息长度	CoAP单个发布消息最大长度。超过此大小的发布请求将被直接拒绝。	1 KB
MQTT保活	MQTT连接心跳时间为30至1,200秒。心跳时间不在此区间内，服务器将会拒绝连接。 建议取值300秒以上。 从物联网平台发送CONNACK响应CONNECT消息时，开始心跳计时。收到PUBLISH、SUBSCRIBE、PING、或 PUBACK消息时，会重置计时器。超过指定1.5倍心跳时间未收到消息（指定心跳时间乘以1.5），服务器将自动断开连接。	30-1,200秒
RRPC超时时间	设备响应RRPC请求的超时时间。	8秒

Topic相关

限制项	描述	限制
自定义Topic类数量	一个产品最多可以定义50个Topic类。	50
权限	设备只能对自己的Topic进行消息发布与订阅。	-
Topic长度	Topic长度不能超过128字节， UTF-8编码字符。	128字节
Topic类目	一个Topic中最多可包含多少个层级类目，即Topic中斜杠的最大数量。	7
订阅数	每个订阅请求的最大订阅数。	8
操作生效时间	订阅和取消订阅都是操作10秒后生效，一次订阅永久生效。建议您提前订阅Topic以免漏失信息。 示例：设备向Topic A发送SUB请求，10秒后，订阅生效，设备开始收到实时消息，除非取消订阅，设备将一直接收Topic A的消息。	10秒
广播Topic	一个广播Topic最多可以被1,000个设备订阅。	1,000
	服务端SDK每秒只可发一条广播消息。	1条/秒

设备影子

限制项	描述	限制
JSON层级	设备影子JSON文档的最大层级深度。	5
文件大小	设备影子JSON文档的最大限制。	16 KB
属性数量	设备影子JSON文档的属性数量限制。	128
每秒请求数	每个设备每秒的最大请求数。	20

数据流转

限制项	描述	限制
规则数量	单账号最多可以设置1,000条规则。	1,000
流转目标数量	一条规则中转发数据的操作不能超过10个。	10
限流	在目标云产品实例性能足够的情况下，数据流转为单个阿里云账号提供的数据转发能力与购买规格相关。 如果请求量超出该限制或云产品写入耗时超过1秒，数据转发会被限流。被限流的消息，系统将自动重试转发，重试10分钟仍未成功的，将被直接丢弃。	与购买规格相关

限制项	描述	限制
流转目标要求	数据转发依赖目标云产品，需确保目标云产品实例正常。目标云产品的实例宕机、参数错误（如授权变更、值非法）、配置错误等异常状况将会导致消息流转失败。	无
消息到达次数	数据流转不保证消息只到达一次，在分布式环境下，某些rebalance短暂不一致可能导致一条消息发送多次情况。多次发送的消息ID相同，应用方收到消息后需要根据消息ID去重。	无

3 物联网边缘计算

3.1 什么是物联网边缘计算

物联网边缘计算，又名Link IoT Edge，是阿里云能力在边缘端的拓展。它继承了阿里云安全、存储、计算、人工智能的能力，可部署于不同量级的智能设备和计算节点中，通过定义物模型连接不同协议、不同数据格式的设备，提供安全可靠、低延时、低成本、易扩展、弱依赖的本地计算服务。

同时，物联网边缘计算可以结合阿里云的大数据、AI学习、语音等能力，打造出云边端三位一体的计算体系。

物联网边缘计算的核心功能如下：

边缘实例

边缘实例提供一种类似文件夹的管理功能，您可以通过实例的方式管理边缘端相关的网关、子设备，同时也可以管理场景联动、函数计算、流数据分析和消息路由内容。通过部署实例，将边缘实例中的资源部署至网关中。

设备接入

物联网边缘计算提供多语言设备接入SDK，让设备轻松接入边缘计算节点。

场景联动

场景联动是规则引擎中，一种开发自动化业务逻辑的可视化编程方式，您可以通过可视化的方式定义设备之间联动规则，将规则部署至云端或者边缘端。

拖拽可视化组件即可实现多设备的本地管理、联动及控制，每个人都可以成为面向设备不用编程的程序员。

例如，您可以将“开门”、“开灯”两个操作串联起来，并设置时间区间在18：00至19:00之间，实现在固定时间段，门开灯亮。

边缘应用

边缘应用是一种运行时框架，遵循事件驱动模型，当前产品支持函数计算类型的边缘应用。函数计算是一种运行时（Runtime）框架，可完成设备接入到边缘网关的开发以及基于设备数据、事件的业务逻辑开发。

您可以使用本地函数计算框架，完成设备接入到边缘网关的开发以及基于设备数据、事件的业务逻辑开发。如：

- 在本地对设备数据做单位换算。

- 在本地对数据进行过滤。
- 在本地将数据转发至本地存储或应用。
- 在本地访问其他服务接口。

消息路由

物联网边缘计算提供消息路由的能力。您可以设置消息路由路径，控制本地数据在边缘计算节点中的流转，从而实现数据的安全可控。

提供的路由路径如下：

- 设备至IoT Hub
- 设备至函数计算
- 函数计算至函数计算
- 函数计算至IoT Hub
- IoT Hub至函数计算

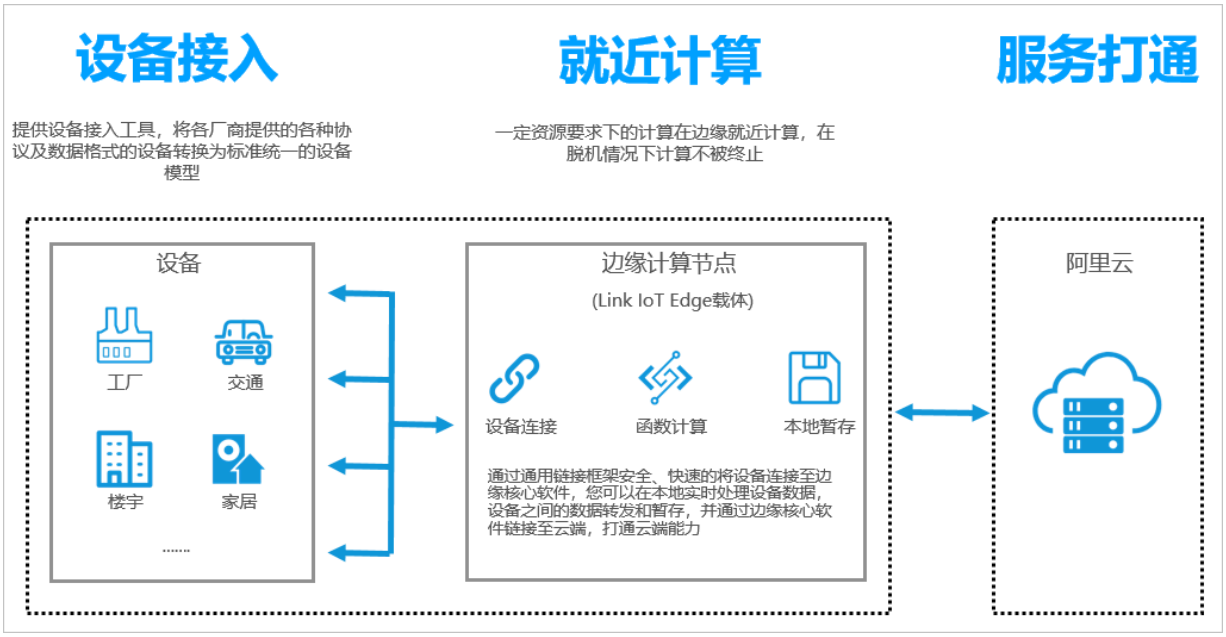
断网续传

边缘计算节点在断网或弱网情况下提供数据恢复能力。您可以在配置消息路由时设置服务质量（QoS），从而在断网情况下将设备数据保存在本地存储区，网络恢复后，再将缓存数据同步至云端。

3.2 产品架构

本章主要介绍物联网边缘计算的产品架构。

产品架构如下图所示。



物联网边缘计算主要涉及设备端、边缘计算端和云端三个部分：

- 设备端

  开发者使用设备接入SDK，将非标设备转换成标准物模型，就近接入网关，从而实现设备的管理和控制。

- 边缘计算端

  设备连接到网关后，网关可以实现设备数据的采集、流转、存储、分析和上报设备数据至云端，同时网关提供规则引擎、函数计算引擎，方便场景编排和业务扩展。

- 云端

  设备数据上传云端后，可以结合阿里云功能，如大数据、AI学习等，通过标准API接口，实现更多功能和应用。

3.3 产品规格

Link IoT Edge提供专业版（LE Pro）、标准版（LE Standard）、轻量版（LE Lite）三个版本的产品，本文为您介绍三个版本产品的能力以及对软硬件的要求。

- LE Pro是基于Docker方式运行的软件包，包含Link IoT Edge所有功能。
- LE Standard是基于二进制自包含包运行的软件包，可以根据运行的软硬件环境选择对应的安装包。
- LE Lite是一款开源软件包，可以使用官方的自包含软件包，也可以使用源码自主编译，该版本提供了远程运维功能。

产品能力

产品能力	专业版	标准版	轻量版
远程SSH服务	支持	支持	支持
远程文件服务	支持	支持	支持
MQTT上云	支持	支持	支持
子设备管理	支持	支持	不支持
设备接入驱动	支持C、Node.js、Python	支持C、Node.js	不支持
函数计算（业务小程序）	支持C、Node.js、Python	支持C、Node.js	不支持
可视化场景联动	支持	支持	不支持
消息路由	支持	支持	不支持

产品能力	专业版	标准版	轻量版
云服务集成	支持	支持	不支持
业务应用隔离	容器隔离	进程隔离	不支持

环境要求

三个版本对硬件的要求如下所示。

硬件参数	专业版	标准版	轻量版
CPU架构	x86-64	• x86-64 • ARMv8-64 • ARMv7 VFPv3硬浮点型 • ARMv7软浮点型	• x86-64 • ARMv8-64 • ARMv7 VFPv3硬浮点型 • ARMv7软浮点型
CPU主频	≥2 GHZ	≥1 GHZ	不限制
RAM	≥2 GB	≥128 MB	≥1 MB
磁盘	≥2 GB	≥128 MB	≥1 MB

三个版本对软件的要求如下所示。

系统环境	专业版	标准版	轻量版
Linux	依赖docker工具，且docker版本> v17.03	• Linux kernel version ≥ 2.6.32（for x86-64） • Linux kernel version ≥ 2.6.32（for ARMv7软浮点&硬浮点） • Linux kernel version ≥ 3.7.0（for ARMv8-64）	• Linux kernel version ≥ 2.6.32（for x86-64） • Linux kernel version ≥ 2.6.32（for ARMv7软浮点&硬浮点） • Linux kernel version ≥ 3.7.0（for ARMv8-64）
Windows	• 依赖bash执行环境，如安装git bash工具 • 依赖docker工具，且docker版本 > v17.03	不支持	• Windows7 • Windows10
MacOS	依赖docker工具，且docker版本 > v17.03	不支持	> OSX 10.10

3.4 名词解释

本章主要介绍物联网边缘计算中相关的产品名词。

名词	解释
Link IoT Edge	物联网边缘计算产品（Link IoT Edge，简称LE），即阿里云物联网平台（IoT）中的边缘计算产品。提供安全可靠的数据计算能力，可供本地处理设备数据，减少上传云端的成本。
Link IoT Edge软件包	阿里云IoT的边缘计算产品软件包，包含Link IoT Edge标准版、专业版软件包。
LE Pro	Link IoT Edge专业版，Docker镜像的方式发布。
LE Standard	Link IoT Edge标准版，以二进制tar.gz的方式发布。
LE Lite	Link IoT Edge轻量版，以二进制tar.gz的方式发布。
网关	运行Link IoT Edge软件的计算设备统称为边缘网关，简称网关。
子设备	指通过一定的协议或接口接入到Link IoT Edge网关上的设备（即设备接入到网关后称为子设备），网关代理该子设备与云端进行通信。
驱动	Link IoT Edge中的设备接入模块称为驱动（driver）或设备接入驱动。所有连接到Link IoT Edge的设备都需要通过驱动实现接入。
边缘实例	边缘实例通过网关关联您的设备，将设备接入到物联网平台进行管理控制，边缘实例同时也管理您设备使用的其他资源，例如驱动，函数计算，场景联动规则等。
Fun	阿里云Serverless应用工具。支持本地定义、开发、测试、调试Serverless应用，并发布到云端。
断网续传	Link IoT Edge提供的在断网或弱网情况下提供数据恢复能力。通过在配置消息路由时设置服务质量（QoS），实现在断网情况下将设备数据保存在本地存储区，网络恢复后，再将缓存数据同步至云端。
消息路由	通过路由规则动态规划消息的传输路径，使消息按照过滤条件，从消息源路由到目标节点的功能，称为消息路由。
设备模拟器	物联网边缘计算提供的一套设备模拟器（DeviceSimulator）解决方案，由驱动和控制工具两部分组成，用于模拟实际的物理设备。

3.5 产品优势

物联网边缘计算平台在接入、成本、安全等各方面都有极大优势。

速接入

通过边缘提供的快速设备接入方案，您可以通过自己熟悉的语言连接不同协议、不同数据格式的设备。

低延迟

可以在设备所处的本地网络中完成设备数据采集，实现控制策略，在本地对设备数据进行清洗、计算、分析，更实时，更可靠。

低成本

本地数据清洗、计算、过滤可将最优价值的数据上传至云进行存储，减少计算、存储及带宽带来的成本。

高安全

提供云到边缘的安全连接，提供数据加密及安全存储。

弱依赖

可在断网或者弱网环境下运行本地计算、存储、分析。

高智能

提供AI学习、语音识别、视频识别能力，与云能力做结合，提高本地智能化。

3.6 应用场景

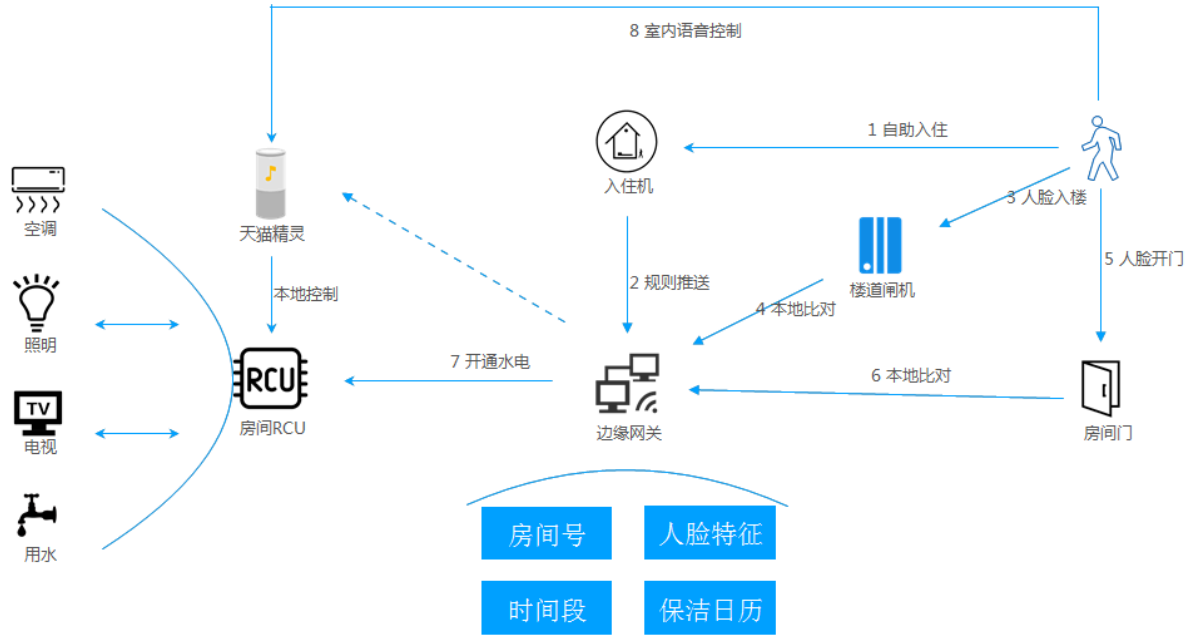
物联网边缘计算平台的典型应用场景有：未来酒店、工业生产、风力发电效率提升等。

未来酒店

通过边缘网关快速集成本地设备后，边缘网关作为本地节点快速响应本地事件，实现本地M2M的智能联动，实现室内室外一体化的语音智能。

特点：

- 设备联动：入楼闸机、房间门、空调、照明、水电等智能联动。
- 边缘计算：人脸信息、房间号、保洁日历、时间段等全部由边缘网关计算处理。
- 语音智能：入住后，天猫精灵成为私人管家，接收住户指令，管理多端设备。



整个场景的运转流程是：

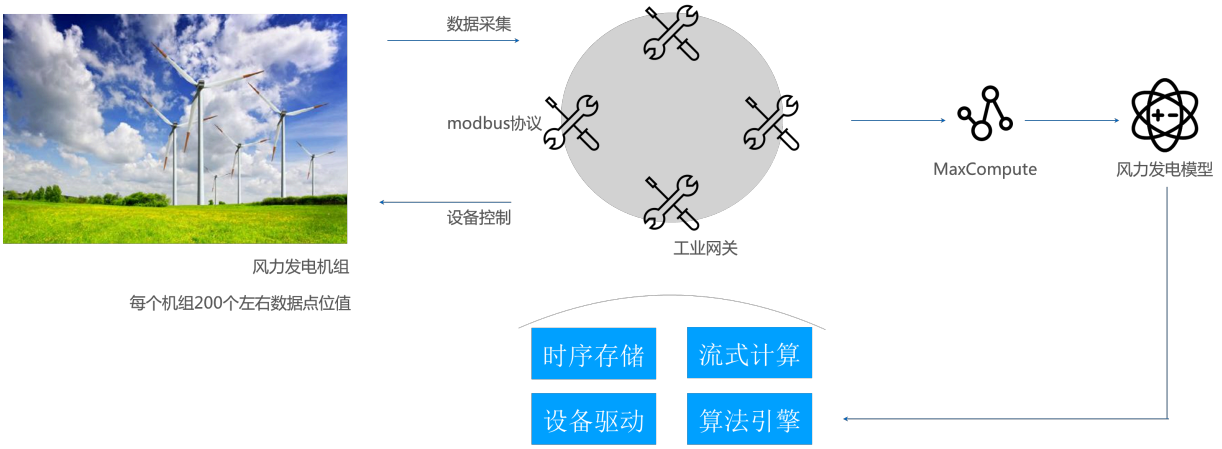
1. 住户自助办理入住，入住机将信息等规则推送给边缘网关。
2. 住户在入楼闸机处刷脸，闸机与边缘网关核对身份信息。
3. 信息核对成功后，闸机打开，住户被允许进入大楼。
4. 住户来到房间门口，刷脸。房间门与边缘网关核对身份信息。
5. 信息核对成功后，房间门打开，住户被允许进入房间。
6. 房间门打开的同时，房间水电、空调、照明、电视等根据环境设置自动开启，天猫精灵开始工作。
7. 住户入住后有其他需求，可以语音将指令需求告知天猫精灵，实现进一步智能联动。

风力发电

在风力发电机组本地网络中，部署边缘计算网关，实时采集机组数据。在本地处理采集的数据后，先将数据上传至阿里云MaxCompute，再使用大数据训练模型后，对发电参数，如风向灵敏度、启动延时参数等做优化。将模型转化为算法或者规则导入本地边缘节点，自动调整风电机组参数，提高机组发电性能。

特点：

- 数据实时采集：多机组多数据点同时采集。
- 大数据处理：数据上传至阿里云后，使用大数据训练模型。
- 即时反馈：算法或规则导入本地边缘节点后，实时自动调整机组参数，实现最优化生产。



3.7 使用限制

物联网边缘计算针对边缘实例功能和规则引擎中的场景联动，设有使用限制。

场景联动相关限制

限制	描述
规则总数<=100	您最多可以在规则引擎服务场景联动中创建100条规则。
规则trigger<=10	每条规则中最多可以添加10个触发条件。
规则condition<=5	每条规则中最多可以添加5个过滤条件。
规则action<=10	每条规则中最多可以添加10个执行动作。

边缘实例相关限制

限制	描述
边缘实例总数≤ 10万	您最多可以在一个阿里云账号下创建10万个边缘实例。
边缘实例网关=1	每个边缘实例中有且仅有1个网关。
边缘实例驱动≤ 30	每个边缘实例最多可以分配30个驱动。
自定义驱动≤ 50	您最多可以在一个阿里云账号下驱动管理中创建50个自定义驱动。
自定义驱动中上传的代码包≤ 50 MB	每个驱动的驱动包大小不可超过50 MB。
驱动配置中键值对≤ 100	边缘实例驱动配置中最多可添加100个键值对。
驱动配置中JSON格式≤ 1 KB	边缘实例驱动配置中JSON格式的内容不可超过1 KB。

限制	描述
驱动配置中配置文件≤ 1 MB	边缘实例驱动配置中上传的配置文件大小，不可超过1 MB。
设备配置JSON格式≤ 1 KB	边缘实例设备配置中JSON格式的内容不可超过1 KB。
边缘实例子设备≤ 1000	每个边缘实例中最多可以分配1000个子设备。
边缘实例规则计算≤ 30	每个边缘实例中最多可以分配30个规则计算。
边缘实例函数计算≤ 30	每个边缘实例中最多可以分配30个函数计算。
边缘实例消息路由≤ 30	每个边缘实例中最多可以添加30个消息路由。

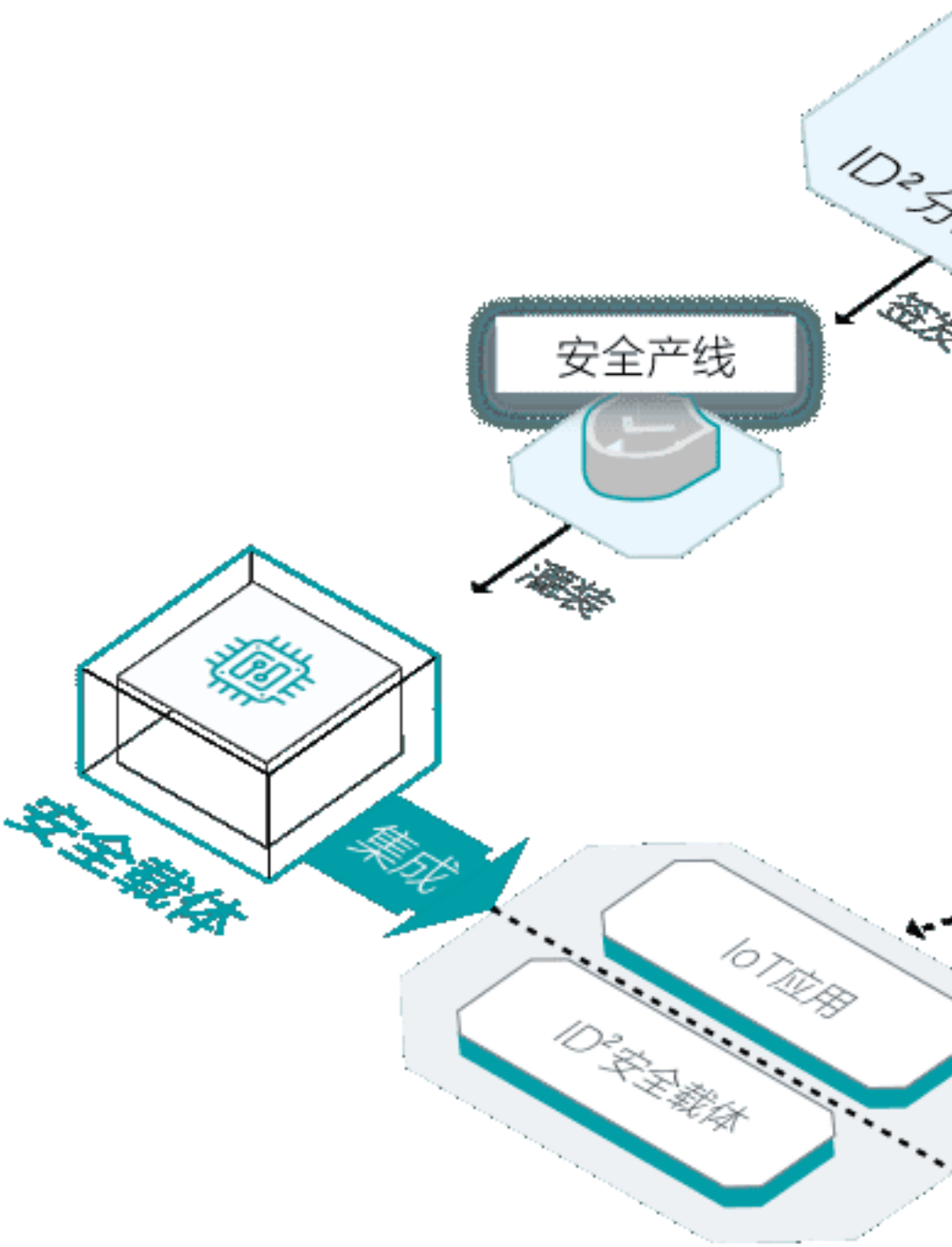
4 物联网设备身份认证

4.1 什么是IoT设备身份认证

IoT设备身份认证ID²（Internet Device ID），是一种物联网设备的可信身份标识，具备不可篡改、不可伪造、全球唯一的安全属性，是实现万物互联、服务流转的关键基础设施。

- 产品特点、系统架构等介绍详见下文。
- IoT：物联网 IoT（Internet of things）。
- IoT设备：通过网络协议连接到物联网的设备。

产品架构



核心能力

- 设备身份标识：为每个IoT设备提供唯一的身份标识，基于ID²提供双向身份认证服务，防止设备被篡改或仿冒。
- 安全连接：提供兼容TLS和DTLS的轻量级安全协议：iTLS/iDTLS。更适合物联网设备，在保障安全性的同时大幅减少IoT设备的资源消耗。
- 业务数据保护：基于设备可信根派生的秘钥支持多种加密算法，为设备固件、业务数据、应用授权等敏感数据提供安全防护。
- 密钥管理：为IoT系统中的设备、应用、业务所使用的密钥提供集中管理，包括密钥生成、密钥销毁、端到端的密钥安全分发。

产品特点

- 轻量化：使用ID²代替CA证书，即节省了存储空间又节省了网络资源的消耗。仅连接握手阶段就可以节省70%的网络资源消耗。
- 高安全：为IoT设备提供云端可信根，基于可信根为上层业务提供可信服务，从源头确保IoT设备的合法性和数据的安全性。
- 广覆盖：适用于多种安全等级的IoT应用场景，支持不同安全等级的载体（SE、SIM、TEE、secure MCU、软件沙箱）。

ID²的关联系统

如果您是芯片/模组厂商，需要在您的芯片/模组中烧录ID²，请使用以下系统。

系统	功能	适用人群
ID²芯片厂商入驻	ID²的芯片/模组对接。	芯片/模组商
ID²烧录系统	申请可以烧录的ID²，并将ID²烧录到芯片/模组中。	芯片/模组商

4.2 ID²安全芯片-规格

ID²安全芯片是集成了ID²安全能力的芯片。

安全芯片规格如下：

规格	标准版-恩智浦A71CL	标准版-紫光同芯IOT60	国密版-复旦微FM1280
起订量	6000片	3000片	3000片
CPU	SmartMX（Secure_MX51）	32位ARM内核SC000	32位ARM内核SC000
FLASH容量	20KB E2PROM	256KB~320KB	512KB

规格	标准版-恩智浦A71CL	标准版-紫光同芯IOT60	国密版-复旦微FM1280
RAM容量	6KB	13~20KB	17.5KB
算法	对称算法： AES（128，192 and 256bits）、DES（3DES） 非对称算法： RSA 可达2048bits 摘要算法：SHA-1、SHA-224、SHA-256	对称算法：DES/TDES、SM1、SM4非对称算法：RSA、ECC、SM2 摘要算法：SHA-1、SHA-256、SM3	对称算法： TDES、AES、SM1、SM4、SSF33 非对称算法：RSA、ECC、SM2 摘要算法： SHA-1、SHA-224、SHA-256、SM3
外设	两个时钟 CRC16 真随机数发生器 DES，AES协处理器，RSA协处理器 安全传感器Reset	真随机数发生器CRC引擎：16-bit CRC-CCITTDMA：数据拷贝和数据比较3个通用定时器/计数器，1个ETU定时器	工作时钟：最高频率32MHz 真随机数发生器 1个24-Bits定时器，2个32Bits的计时器TIMERA和TIMERB CRC：支持CRC32和CRC16运算功能 看门狗模块
接口	I2C接口 SPI接口	USB接口ISO/IEC 7816 从/主接口UART接口 SPI主/从接口I2C接口 PWM接口键盘GPIO	ISO/IEC 7816接触接口 ISO/IEC 14443-A接口 SPI接口 I2C接口
封装	SOP8	WaferQFN32	DFN12 SOP8
ICA 安全认证	SE L1载体L2	无	SE L3 载体L3
国际/国内 安全认证	无	无	CC EAL5+
ID² INSIDE商标	有	无	有

4.3 ID²的功能特性

ID²为IoT设备的身份标识、认证、数据加密提供了以下核心服务：

设备身份认证 为每个IoT设备提供唯一的身份标识，基于ID²提供双向身份认证服务，防止设备被篡改或仿冒。

安全连接 提供兼容TLS和DTLS的轻量级安全协议：iTLS/iDTLS。更适合物联网设备，在保障安全性的同时大幅减少IoT设备的资源消耗。

业务数据保护 基于设备可信根派生的秘钥支持多种加密算法，为设备固件、业务数据、应用授权等敏感数据提供安全防护。

密钥管理 为IoT系统中的设备、应用、业务所使用的密钥提供集中管理，包括密钥生成、密钥销毁、端到端的密钥安全分发。

4.4 ID²的优势

ID²具有轻量化、高安全、广覆盖的特点，适合在低功耗的物联网设备中使用。

轻量化

使用ID²代替CA证书，即节省了存储空间又节省了网络资源的消耗。仅连接握手阶段就可以节省70%的网络资源消耗。

高安全

为IoT设备提供云端可信根，基于可信根为上层业务提供可信服务，从源头确保IoT设备的合法性和数据的安全性。

广覆盖

适用于多种安全等级的IoT应用场景，支持不同安全等级的载体（SE、SIM、TEE、secure MCU、软件沙箱）。

4.5 ID²的使用限制

使用ID²之前，请您务必了解以下信息：

序号	说明
1	ID²是一款能够独立运行的面向IoT系统的安全产品，也可以与物联网平台搭配一起使用。
2	（推荐）搭配物联网平台使用ID²，可以获得轻量级安全连接（iTLS/iDTLS）。如果您需要对接物联网平台，请在物联网平台上创建产品，并将”认证方式“选择为 ID²。。
3	ID²是基于产品型号进行授权的，您可以在ID²管理控制台创建多个产品，但是产品之间的ID²授权额度不能共享、不能交叉使用。
4	同一个产品型号下所有的ID²，有效期必须一致。请在购买时按实际的生命周期选择相应年限的有效期。例如，产品A已经购买了1年期的ID²，那么产品A续费时只能续费1年期的ID²
5	支持的Region：目前仅支持中国-华东2区（上海），其他Region会陆续支持。
6	基础版ID²的限制：每个ID²每天认证次数限制为10次。尽管现在超出认证次数后不会做限制，但是强烈建议您控制认证调用量。过高的、频繁的、超标的调用量在未来会受到严格的控制。

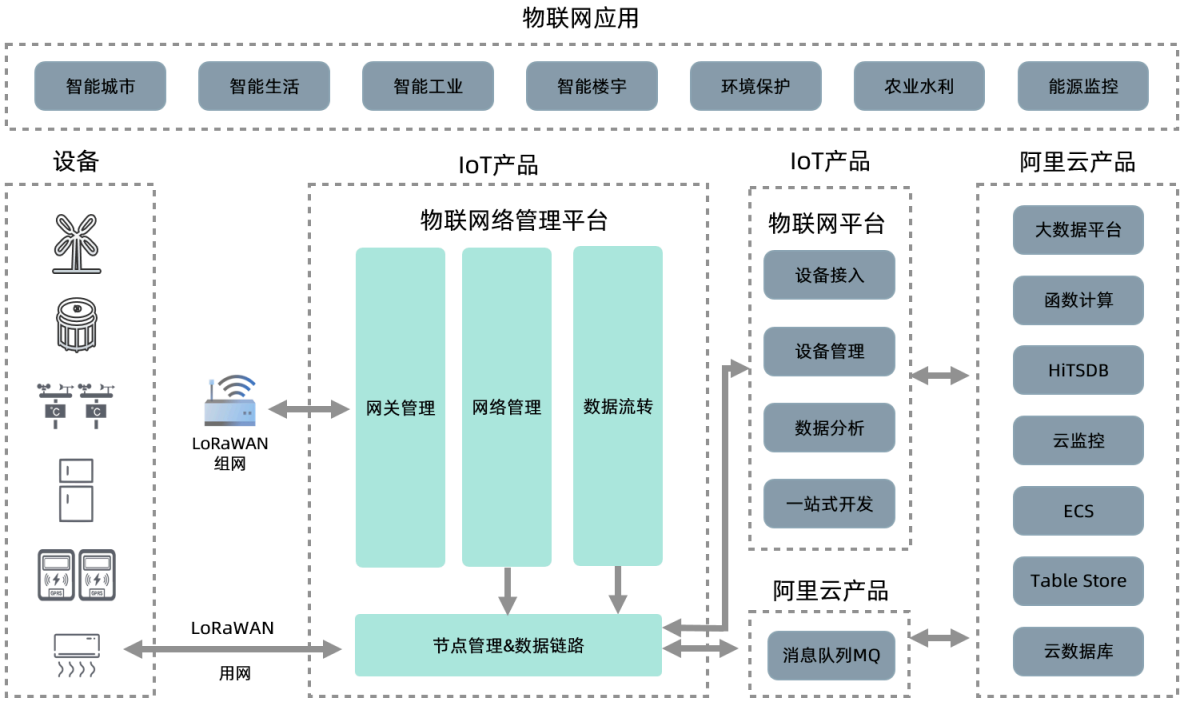
5 物联网络管理平台

5.1 什么是物联网络管理平台

物联网络管理平台（Alibaba Cloud Link WAN，简称Link WAN），是阿里云面向物联网企业所推出的网管平台，旨在帮助开发者搭建企业物联网络，实现企业级、大容量、高并发的网络专网服务。

Link WAN可与阿里云物联网平台搭配使用，确保物联网平台每个环节的开发者都能轻松实现各自功能，并且拥有可自主管理的物联网无线覆盖区。

物联网络管理平台与整个物联网产品的关系图如下所示。



Link WAN目前支持LoRaWAN协议的网关与设备接入，主要功能如下。

- 网络管理

  用户可将网关关联于自主账号内，实现网络覆盖的服务，Link WAN提供网关管理功能。

- 网络分享

  透过入网凭证的分发，用户可分享自己搭建的网络给其他的阿里云用户，使其设备接入网络上云。

- 数据出口

  可实现对凭证数据的出口统一配置，支持阿里云物联网平台（IoT Platform）配置。

沙箱调试完成后，请确保数据上下行正确，然后再前往实验室官网申请互联互通认证。

5.2 产品优势

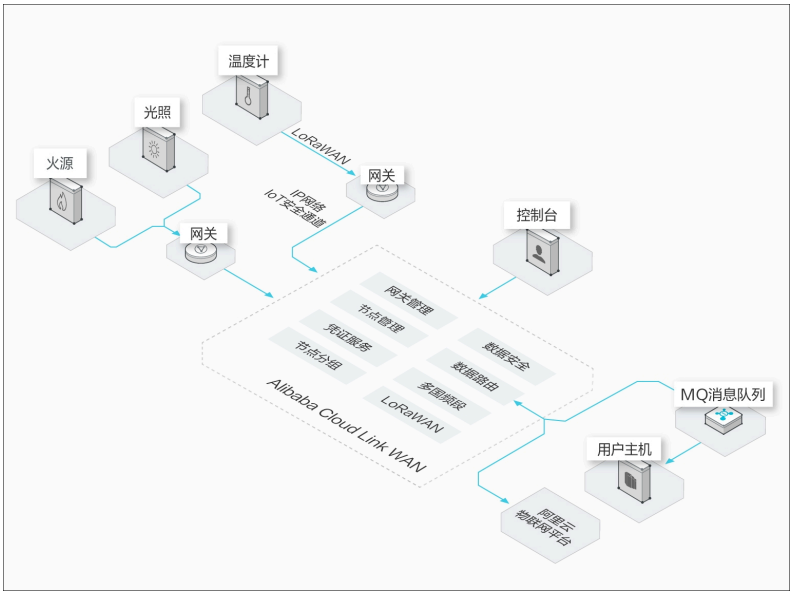
本章节主要介绍Alibaba Cloud Link WAN 物联网络管理平台核心与自建核心能力间的差异。

能力	其他LoRa平台	Link WAN (LoRaWAN)
LoRaWAN 国际标准	标准纷乱，彼此互不相通，系统维护成本高。	遵循LoRaWAN国际标准协议。
技术领先性	普偏采用开源Demo版本NS自行迭代，对于新协议能力开发，被动演进。	阿里云自主迭代，跟随联盟定义标准，目前支持LoRaWAN 1.0/1.0.2/1.1，Class A/B/C。
性能	自行实现扩展性架构，极难做到从设备粒度调度服务器、负载均衡等基础设施。	具有亿级设备的长连接能力、百万级并发的能力，架构支撑水平性扩展。
安全	需要额外开发、部署各种安全措施，保障设备数据安全是个极大挑战。	基于LoRaWAN AES与阿里云物联网安全通道，双重链路保障。
稳定	需自行发现宕机并完成迁移，迁移时服务会中断。稳定性无法保障。	服务可用性高达99.9%。单点故障，自动迁移。
简单易用	需要购买服务器搭建负载均衡分布式架构，需要花费大量人力物力开发“接入 + 计算 + 存储”，自己组建复杂网络管理系统。	一站式网络管理、实时管理覆盖区、无缝连接阿里云产品与物联网平台，用户搭建灵活简便。

5.3 产品架构

当前Alibaba Cloud Link WAN接入网软件由网关SDK、节点SDK组成，帮助设备连接阿里云，是设备与云端安全通信的数据通道。节点SDK统一了节点的协议栈，网关SDK统一了各种网关接入平台的方式。

产品架构图如下图所示。



- 节点SDK具有下列特性
  - LoRaWAN协议栈：支持最新LoRaWAN 1.0.2 版本。
  - AT指令扩展： 通讯模块操作界面，符合ICA标准指令集。
- 网关SDK有以下特性
  - 网关监测：支持实时监控网关健康状况，支持CPU、内存、传输等状态实时监测。
  - 网关OTA： 支持OTA签名校验、断电恢复等功能。
  - 安全存储：支持保护网关中已下载的密钥安全，防止密钥被异常窃取。

网关与节点管理

物联网络平台为您提供功能丰富的网元管理服务。

凭证服务

用户可自行采购网关组建网络，形成物联网覆盖服务区域，凭证则是用户是否能使用此张网络的通行证。 物联网络平台可使您将创建的凭证授权给自己或者您的客户，分享网络覆盖给其他阿里云用户使用。 当设备采集数据传至云端时，您可以将平台搜集的数据进行按凭证分群归属，然后配置转发规则，将数据转发到目的应用所对应的服务上，例如可转发到阿里云物联网平台。

安全产线

安全是IoT的重要话题。阿里云物联网络管理平台提供多重防护保障设备云端安全。

- 平台为每个节点设备颁发唯一证书，节点通过双向加密连接到云端。
- 支持工厂端的安全产线烧录功能，保证对于设备或者模组大规模烧录时的通道安全。

5.4 名词解释

本章主要介绍物联网络管理平台中相关的名词解释。

名词	描述
物联网络管理平台	又称Alibaba Cloud Link WAN，简称Link WAN。
网络商户	接入网关，自组网络的用户。
应用商户	使用网络商户颁发的凭证，接入设备开发应用的用户。
设备商户	制造与销售符合Link WAN接入标准的设备合作伙伴。
服务合作伙伴	取得Link WAN互联互通认证证书的和合作伙伴。
网关	LoRaWAN接入网络的网元，负责和终端节点的上下行无线通信。
节点	具有LoRa通信功能的终端或者模组等。
凭证	入网凭证，在LoRaWAN协议里，关联写入于节点设备的JoinEUI，每个节点分组透过入网凭证，指向接入网络。
专用凭证	接入权限仅限于用户自组接入网的凭证。
泛在凭证	接入权限可用于加入泛在网接入网的凭证，又称共享网络。
频段计划	LoRa网关和节点工作的无线频段，如中国CN470，亚太AS923。
Class A	LoRa节点最佳节能的工作模式，服务端无法主动下发，上行数据按需发送。
Class B	服务端数据可主动下发，节点可节能并时延可控的工作模式。
Class C	服务端数据可实时上下行双向通信，功耗较高，需有固定电源。
D2D	Device to Device, LoRa节点点对点通信，支持下行主动唤醒。
GwEUI	LoRaWAN网关的全局唯一身分标识。
DevEUI	LoRa节点的全局唯一身分标识。
数据出口	节点分组数据流向目的地，对接用户的应用服务。
CN470	中国境内470M-510MHz的无线频谱资源，可在法规允许的范围内使用。
AS923	亚太地区920M-923MHz的无线频谱资源，可在法规允许的范围内使用。
同频	LoRa网络上下行通信使用相同频率。
异频	LoRa网络上下行通信使用不同频率。
Hybrid 网关	同时支持上下行数据可在本地（边缘）与接入公共云两种混合能力的网关。
产线配置	支持工厂产线，可从云端线上下载密钥，安全烧录于生产设备。

5.5 功能特性

Alibaba Cloud Link WAN提供符合国际标准的LoRaWAN接入服务。

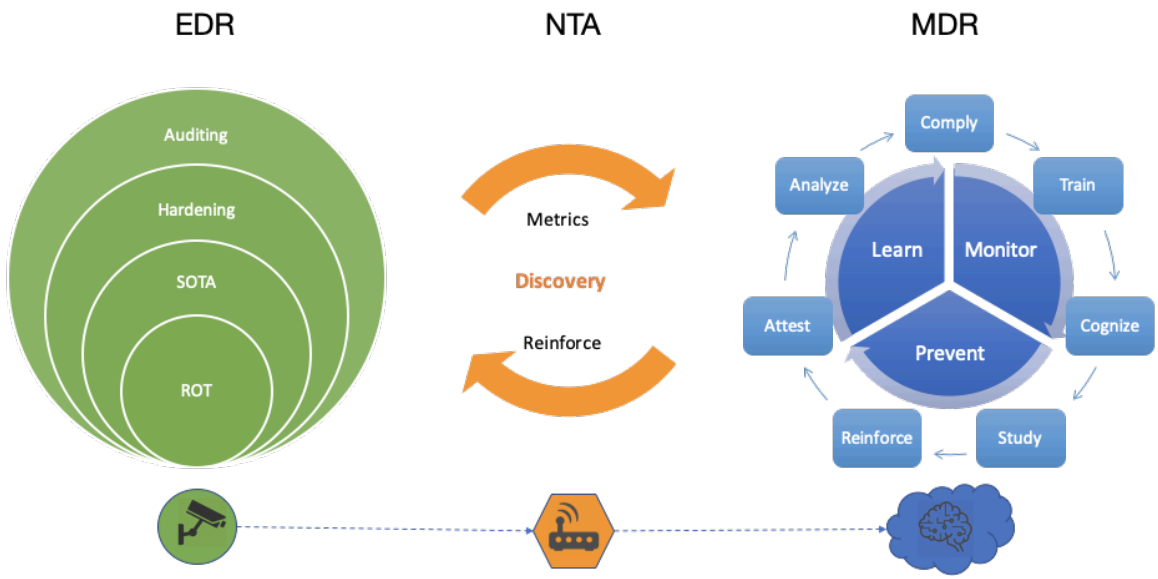
能力	详细	备注
LoRaWAN	1.0.3	1.1内测中
支持频段	AS923同频/CN470同频/CN470异频	无
支持模式	半双工/全双工	无
通道数	8/16/32/64CH	无
Class	A/B/C	无
入网模式	ABP/OTAA	Hybrid网关提供ABP入网。
ADR	支持	无
中继网元	支持	内测中。
安全	LoRaWAN AES-128/网关安全通道	无
GWMP协议	支持	无
组播协议	支持	专业版支持。
LoRa D2D	支持	内测中。
数据接口	MQTT/阿里物联网平台	无
边缘部署	支持	Hybrid网关。
本地部署	支持	内测中。

6 物联网安全运营中心

6.1 产品介绍

本文介绍了IoT安全运营中心诞生的背景以及简介。

大数据平台日趋成熟，智能分析方兴未艾，IoT安全运营中心（Link SOC）就是在这样一个背景下，立足于终端安全，借鉴成熟的传统安全方案，借助大数据和云计算而产生的，旨在适应物联网环境的，一站式管控，可持续运营的安全管理平台。 在设备上可以理解为基于大数据的一种HIPS（Hosted Intrusion Prevention System）实现。在服务上可以理解为一种综合借鉴EDR（Endpoint Detectionand Response），NTA（Network Traffic Analytics），MDR（Managed Detection and Response）等安全服务特点，针对物联网场景优化的面向持续运营的安全服务。



在平台侧，不仅使用智能化手段检测和预警设备风险，更规范设备接入，发布和运营三个阶段流程，控制设备准入，保证持续运营。

在设备侧，基于基线的策略设计，不仅有高度事件聚合能力以适应各种带宽和稳定性的要求，还可以提供及时的威胁阻断能力。而独立的安全域设计，可以利用和兼容设备既有安全机制，提供增强的安

全服务。 在部署上，支持设备，网关，边缘，区域多纵深部署，提供基于主机的全网防护。并构建三方生态提高垂直安全能力，达到全场景防护。 Link SOC随着阿里云在IoT的不断发展，已成功在阿里巴巴集团内部，菜鸟等事业部，以及电力，工业，园区等合作伙伴范围内广泛使用。