锐捷无线总分高可靠组网

技术白皮书

如有疑问
扫一扫在线咨询

Ruijie Networks 锐捷

名词解释

缩略语/术语	说明
AP	Access Point，无线接入点
AC	Access Controller，无线控制器
CAPWAP	Control And Provisioning of Wireless Access Points，无线接入点控制与规定
VAC	Virtual AC，一种将多台AC组合成一台虚拟AC的技术
RIPT	Remote Intelligent Perceptive Technology，边缘智能感知技术，在AP与AC连接断开时，AP能够继续对外提供无线服务

概述

背景

随着无线网络技术的快速普及和各种增值业务的广泛部署，对网络的稳定性要求越来越高。在开展业务过程中，若是出现网络中断，可能影响大量业务，造成人力、物力与财力的损失。在仓储物流、企业办公、普教城域网等常见部署的多城市、多网点的总部分支网络中，部署传统的AC+瘦AP方案时，很多的业务应用都集中到AC端处理，要求AC和AP间的链路带宽越大越好、时延越低越好、稳定性越高越好。但在实际的应用场景中，总部与分支之间未部署专线网络，而是通过广域网互联，网络质量无法保障，很可能引起无线用户接入速率不高或无线用户业务体验不佳等问题。

这就要求在实际网络中，需要有相应的设备冗余设计、链路冗余设计以及用户逃生策略，用以保证网络故障或服务中断时，分支用户能够继续使用无线网络。

业界做法

总分组网模型，业界都是统一做法：总部机构部署总部AC、分支机构部署分支AC，总部AC负责整体无线网络的管理，分支AC负责本地AP、无线用户的接入认证。但是，AP与总部AC、分支AC建立CAPWAP隧道及过程存在差异，一种做法是AP仅与分支AC建立CAPWAP隧道、分支AC由总部AC指定。该技术中存在两个不足之处：

- 分支AP与总部AC无法通信时，则无法获取到分支AC信息，也就无法与分支AC建立CAPWAP隧道，无法提供无线网络服务。
- 分支AC发生故障时，分支AP需要和新的分支AC或总部AC重新建立CAPWAP隧道，此过程会加大无线网络恢复正常服务的时间。

总分组网模型，对于配置的统一管理要求也较高，基础要求是分支AC能够从总部AC获取对应网络配置信息，更高要求是分支AC操作的配置也要能够反向同步回总部AC，在保证统一配置的前提下提供配置便利性，极大地释放总部网管人员的运维压力。业界当前无分支AC配置反向同步总部AC的做法。

解题思路

■ 分支AC依赖总部AC

分支AC由总部AC进行指定，对总部AC具备强依赖。锐捷针对该点，采用解耦总部AC的方式进行，分支AP和分支AC保持原有瘦AP架构的交互方式，保障分支网络维持原有瘦AP架构的稳定性。

■ 单CAPWAP隧道

分支AC发生故障时，分支AP需要重新建立CAPWAP隧道，增加无线网络恢复正常服务的时间。锐捷提出双CAPWAP隧道的通信模型，将灾备通道提前预留，降低从故障状态恢复至正常服务的时间。

在充分考虑链路带宽、网络时延和射频环境的异常情况对网络稳定性的影响后，锐捷网络推出总分高可靠组网技术，通过总部AC虚拟化备份、总部分支AC N+1备份、AP双隧道备份、AP灾备逃生等多重灾备技术，提升总部机构的网络稳定性、减少分支AC对总部的依赖，让网络更可靠，通过总部与分支之间配置上的相互同步功能，让维护更简单。

技术价值

总分高可靠组网模型，提供一种高可靠、高性能、易管理、易扩展无线组网架构。

■ 提升高可靠

分支AC、总部AC、分支AP任一网元出现故障时，均有灾备方案继续提供无线服务，提高网络可靠性。

■ 提升整体性能

由分支AC负责本地分支AP、无线用户的接入认证，分布式控制方式降低总部AC集中控制的压力，提高无线网络整体性能。无线用户在AP之间的切换由分支AC负责，由于分支AC更靠近AP，因此可以更迅速响应漫游事件，提高了漫游性能。（传统的瘦AP架构下，STA的漫游、迁移必须有AC参与。当STA在AP之间切换时，需要AC通知AP切换表项。如果AC和AP间跨越Internet或者时延较大，那么漫游性能势必受到影响）

■ 易于管理

- 统一升级：由总部AC统一为分支AC和分支AP升级软件版本，无需在每个分支AC上逐一升级版本，简化复杂的设备升级工作。
- 统一配置：网络部署阶段，可在总部AC上统一配置分支AC，也可在分支AC上执行的配置业务并自动同步给中心AC的过程，简化网络配置过程，降低分支管理员的重复性工作。
- 统一监控：网络运行阶段，总部AC统一查看所有在网AC、AP和终端的运行情况，便于网络管理员实时掌握整网的网络状况并及时应对可能的运行风险。
- 分权管理：可实现一台AC由多用户共同管理，不同用户管理不同AP、WLAN等信息，从而减少原有总部管理员的日常工作，同时让各分支管理员拥有更多的自主权。

■ 易于扩展

分支AC彼此无耦合，分支机构增加时添补分支AC即可扩展无线网络，无需担心影响其它分支机构、也不用担心受其它分支机构的影响，分支机构增减的扩展更便利。

技术实现

本文用来说明分级AC的功能与技术。分级AC是一种集中管理 + 分布式转发的总部-分支模型。其组网形态，由一台总部AC和多台分支AC组成，分支AC负责管理分支AP和无线用户的接入认证，总部AC负责整体无线网络的管理与灾备。分级AC提供了总分架构的高可靠组网，保证无线网络的体验不变，具备总部统一管理的特性。

基础概念

分支AC

即本地AC，部署在各分支机构的AC，负责管理分支机构的AP和分支机构的无线用户接入认证。

总部AC

即中心AC，部署在总部机构的AC，统一监控与管理整体无线网络的AC。支持查看整网的AP信息和无线用户信息，支持对分支机构的AC和AP进行升级、配置。当总部分支之间链路正常时，分支结构的无线用户在分支网络上完成接入认证及业务数据转发。当分支AC发生故障时，中心AC接管分支AC原有的业务，为AP和无线用户继续提供服务。

分级AC

一种由总部AC和分支AC组成的集中式管理、分布式转发的AC部署模型。总部部署高性能AC，分支部署低端AC。总部AC和分支AC之前同步无线用户数据时采用的同步方式有普通模式和大容量模式两种。

- 普通模式：实时同步无线用户全部的数据信息，实时性更高，支持分支AC数目相对少。
- 大容量模式：非实时同步无线用户关键数据信息（关键数据有备份、用户不掉线），实时性相对弱，支持分支AC数目更多。

集中AC

集中AC是指多个分支共用一台分支AC，可部署在某一分支机构，也可部署在总部AC或其它统一位置，直接管理分支机构的AP，同时负责分支机构无线用户的接入认证。

分支AP

分支机构中接入网络并与总部AC和分支AC建立CAPWAP隧道的AP，简称为分支AP。

技术架构

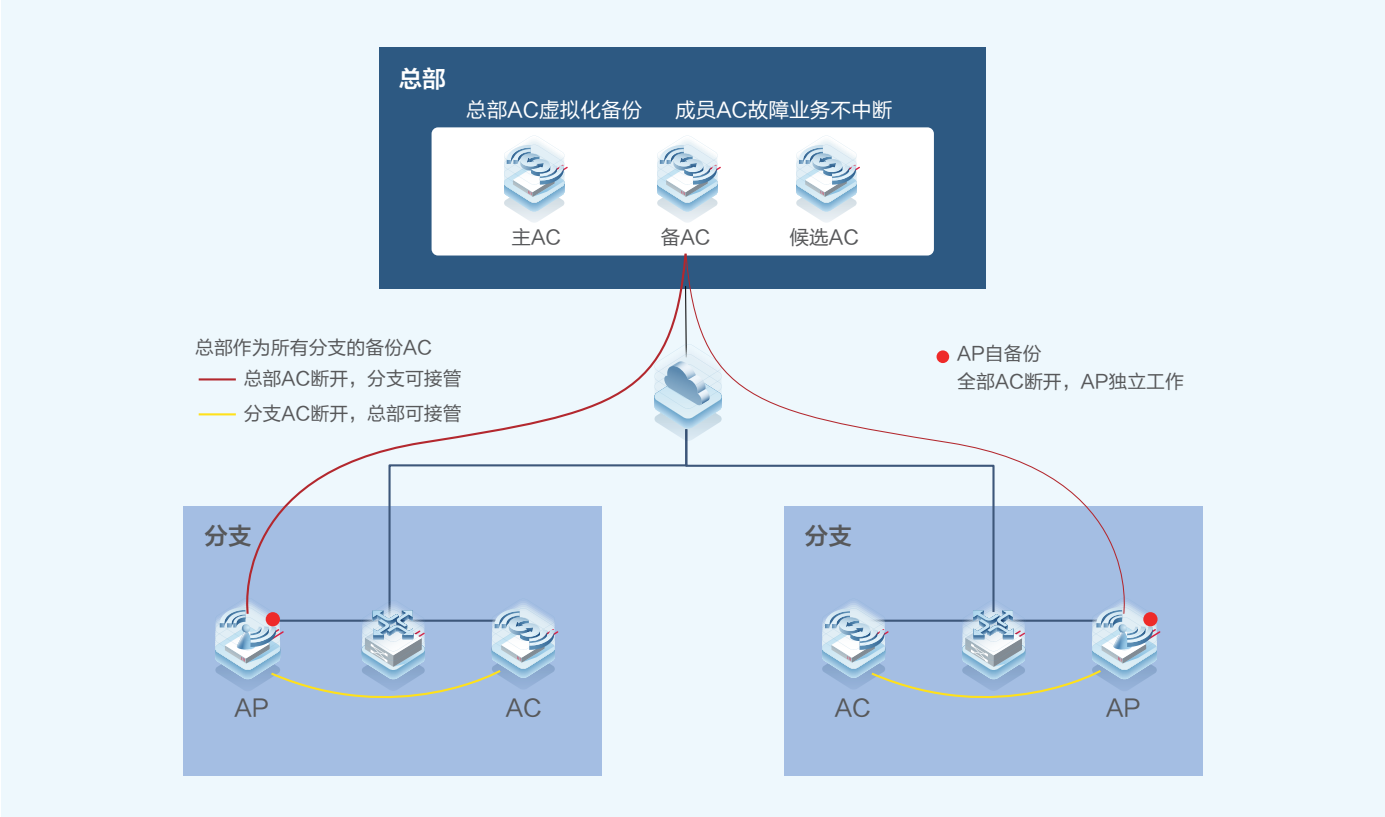


图2-1 可靠性组网架构图

1. 总部AC虚拟化备份

总部AC由两台、三台甚至更多台的成员AC通过AC虚拟化技术虚拟而成，即总部VAC。通过AC虚拟化技术，不仅便于管理员统一配置和管理，同时可以提供更高的可靠性服务。如，4台AC组成的VAC，其中任意一台成员AC故障时，都可将接入在该AC上的AP均衡的迁移到另外三台AC上。

2. 总部分支N+1备份

分支AC和总部AC之间建立管理通道用于相互同步CAPWAP隧道的通信IP和无线网络配置，并确定分支AC为主用AC、总部AC为备用AC。由分支AC管理分支AP和无线用户接入认证，总部AC负责监控与管理整体无线网络的AC，同时分支AC实时向总部AC同步AP和无线用户的状态信息。当分支AC出现故障后，总部AC切换为主用AC。在实际应用场景中，支持使用一台总部AC作为备AC，为N台分支AC（即主AC）提供备份服务，称为N+1的总分组网方案。当主AC故障时，由备AC替代主AC来管理AP。

3. AP双隧道备份

AP双隧道备份是指，在AC+瘦AP组网结构中，由两台AC来管理同一台AP，AP同时和两台AC建立CAPWAP隧道。在分级AC场景中指的是，分支AP同时与分支AC、总部AC建立CAPWAP隧道，其中分支AC为主AC，为分支AP提供无线接入服务，而总部AC为备AC，不提供具体的接入服务。当分支AC与分支AP间CAPWAP隧道出现异常时，总部AC接替主AC来管理分支AP，为AP继续提供服务。

4. AP灾备逃生

当AP和AC间的CAPWAP隧道全部出现故障时，AP上原有的用户会离线，新用户也无法接入网络。尤其在分级AC场景中，总

部和分支通常通过广域网链接，网络质量无法保障，更加大了AP和AC之间链路异常风险。若是出现网络异常，可能导致业务中断。

通过边缘智能感知技术，可在出现以上情况时，尽量让无线网络仍然可用，即：AP直接负责用户接入和数据转发，让原有用户的业务不中断，新用户可以继续接入网络，由此提高网络的可靠性。

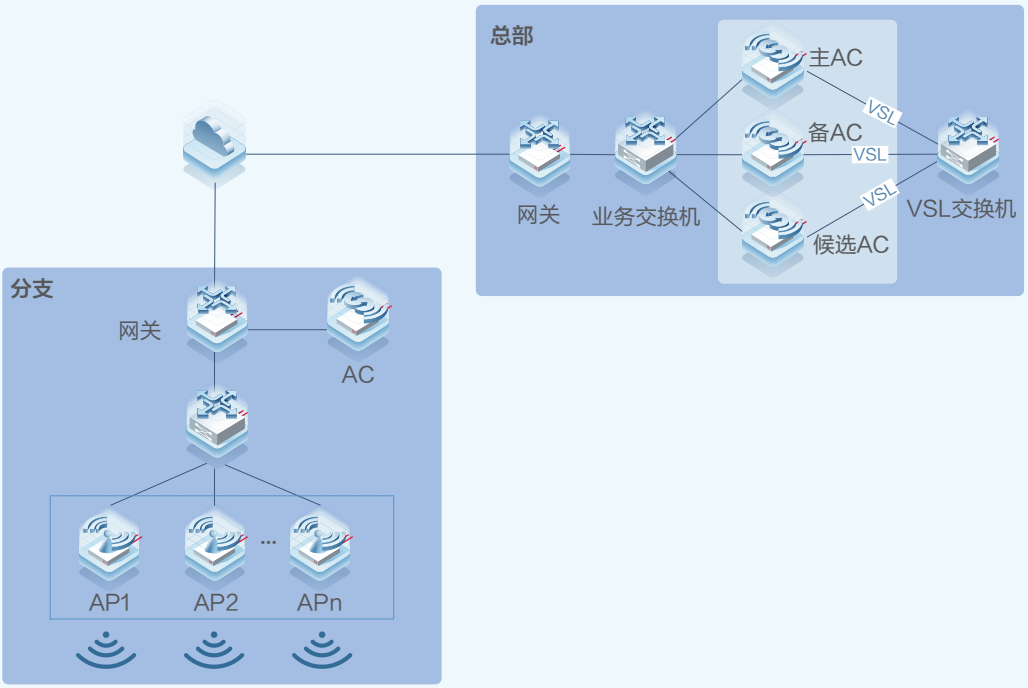
实现原理

说明

本章节中涉及到的拓扑图，是为辅助说明可靠性灾备技术的实现原理而提供的示意图，为便于原理阐述进行了适当的简化处理，不代表用户现场环境的真实拓扑。

总部AC虚拟化备份

总部AC虚拟化备份的组网拓扑，如下图所示：



1. 基本概念

- 域名ID（domain ID）：是VAC的标识，只有域名ID相同才能组成VAC，缺省值为100。
- 设备ID（devicd ID）：成员AC的一个属性，是AC在VAC中的成员编号，缺省值是1。
- AC优先级：是VAC的一个属性，在角色选举中用来确定成员AC的角色，缺省值为100。
- VSL（Virtual Switching Link）：是一条用来在成员AC间交换数据的特殊聚合链路，主要负责转发VAC间的管理报文，但不转发STA的数据报文。

说明

VAC组网的形成过程，需要在做好物理连接的前提下，做好以下配置：

- 在所有AC上配置VSL链路成员口。
- 在业务交换机上配置聚合口的负载均衡策略为基于IP+目的IP。
- 在所有AC上配置VAC参数，包括：域名ID、设备ID、AC优先级。
- 将AC从单机模式切换到VAC模式。

2. 角色选举

总部VAC组网中，当有两台AC时，其中一台选举为主AC，另一台选举为备AC；超过两台AC时，其他AC的角色都是候选AC。在管理面上，只有主AC处于工作状态；在控制面上，每个成员AC都处理无线相关的业务；在数据面，VAC的各个成员AC都参与转发数据报文。主AC的选举过程，遵循以下原则：

- 当前主AC优先。
- AC优先级大的优先为主AC。
- 域名ID小的优先为主AC。

在主AC选举完成后，剩下的AC中选举一台备AC，其选举规则和主AC类似。主备AC确定之后，剩余的成员AC自动变成候选AC。

3. 可靠性设计

总部VAC中的成员AC之间通过心跳链路来传输管理信息（如角色选举信息、配置备份信息）和数据流。当成员AC的角色后，由主AC负责配置同步，所有成员AC均可负责无线用户的业务转发。当主AC出现故障时，备AC自动接替为主AC，而不需要人工参与配置操作（如图2-2）；当备AC出现故障时，候选AC接替为备AC；当候选AC出现故障时，不影响主AC和备AC的业务转发。VAC的成员AC间支持任意AC间备份，当任意一台AC故障时，无线业务都不会中断，转发也不会中断。管理员可以在AC上配置多个端口为VSL接口，提高VSL链路的可靠性。

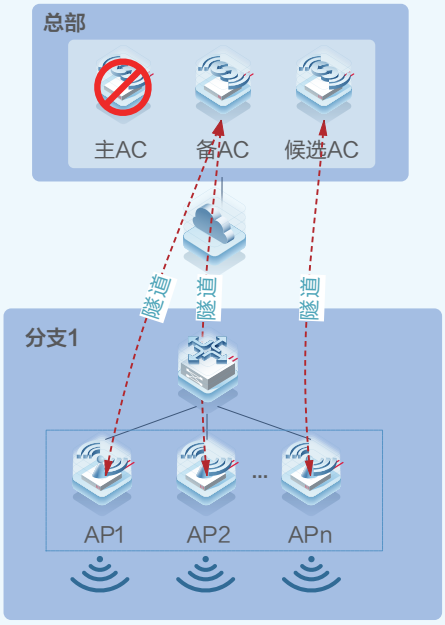


图2-2 主AC故障示意图

总部分支N+1备份

总部/分支N+1备份组网，如下图所示。总部AC支持和N个分支AC组成N个双机备份关系，当分支AC出现故障时，分支AP可以连到总部AC，确保无线可用。

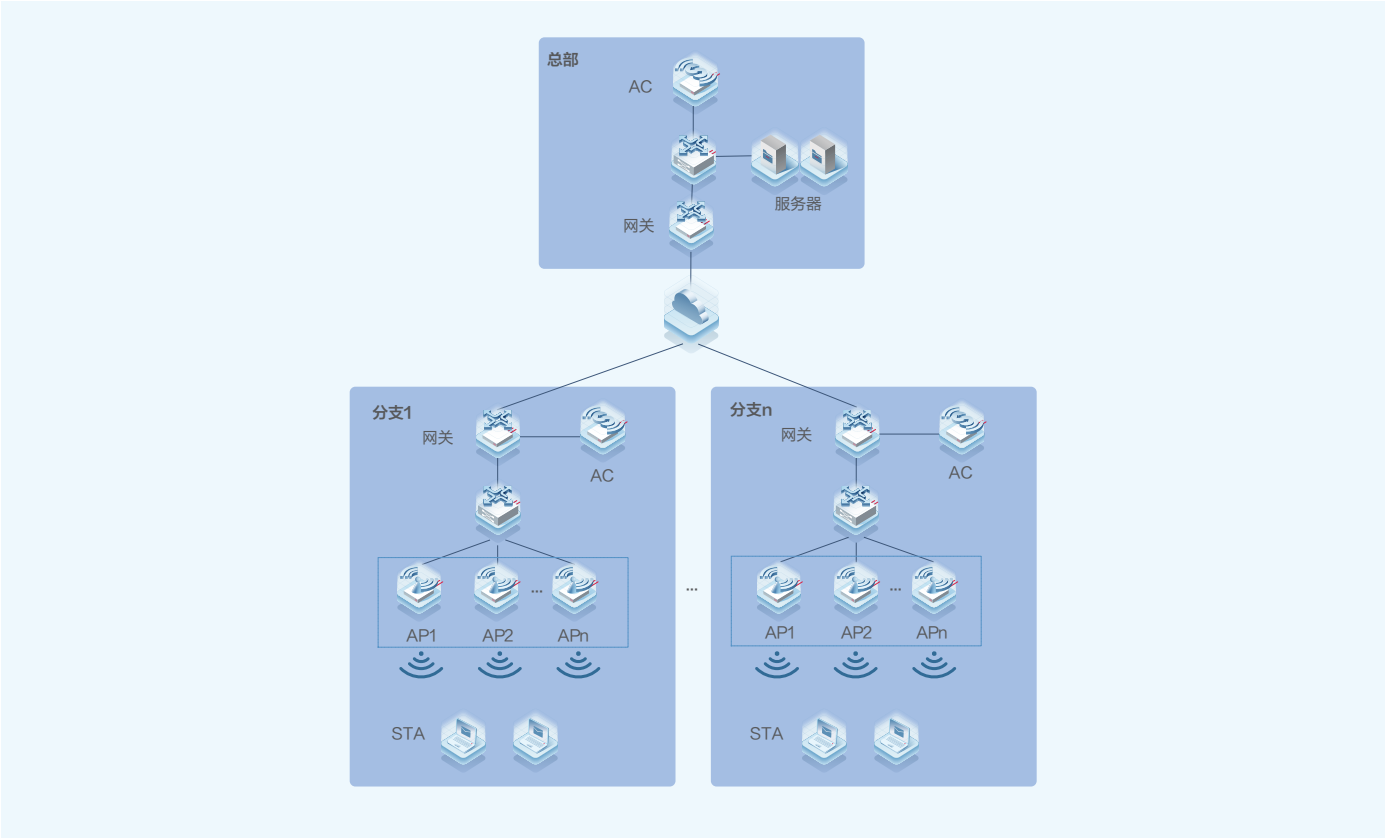


图2-3 总部-分支N+1备份组网

其中：

- 总部AC和分支AC形成了备份关系，用于监控和管理AP。
- 分支机构中的AP1~APn是加入到备份组的分支AP。

1. 主备选择

在总部分支N+1备份组网中，存在多个分支AC和1个总部AC。组建一个总部分支结构的备份网络，需要在总部AC和分支AC上启用分级AC功能，并为AC配置角色。如，将位于分支机构的AC，配置为分支AC；将位于总部机构的AC配置为总部AC。总部AC和分支AC会通过热备协商报文，协商出分支AC为主AC，总部AC为备AC。

当AP接入网络时，将AP加入分支/总部AC所关联的AP组，AP便与两台AC建立双隧道，且自动选择分支AC为主隧道，总部AC为备隧道。此时，总部/分支AC间建立起双机备份关系，主要的备份信息包括CAPWAP状态表项、AP表项、用户表项和DHCP租约等。

2. 主备切换

总部AC和分支AC建立起双机备份关系后，两台AC间定期交互心跳报文，用于检测其中一方AC是否出现故障。AC间交互的保活心跳报文，包括心跳请求报文、心跳应答报文。

- 心跳请求报文：发送给对端的请求报文，需要对端恢复一个应答报文。
- 心跳应答报文：监听并接收到对端的心跳请求报文后，回复的应答报文。

AC监听对端AC发出的心跳报文保活，根据心跳报文标识，回复心跳应答报文。当总部AC（备AC）在连续3个周期内都未收到分支AC（主AC）的心跳应答报文时，认为AC发生故障，主备AC会进行主备切换。

主备切换的动作：
- 总部AC激活内部所有已配置的业务应用，升级为主AC。
- 向在线的AP发送主备AC切换通知，激活AP的备用CAPWAP隧道，完成用户数据通道切换。

3. 主备回切

当分支AC从故障中恢复后，将与总部AC（新主AC）重新进行主备角色协商，重新选举分支AC为主AC。

4. 正向配置同步

> **说明**
> 启用分级AC功能的两台AC，需要保障其配置上的一致性，如加入备份的AP组名称、加入备份的热备实例、WLAN网络名称、DHCP地址池等，但不包括AC管理口的IP地址、AC角色等必须不同的配置。

在N+1的备份网络中，将总部AC上的配置信息在所有的分支AC上配置一遍，是一件繁重且冗余的工作。分级AC支持在总部AC上统一配置分支AC，简化配置过程。分级AC场景提供多种配置同步的方式，用户可根据实际场景需要选择使用。

> **说明**
> 在总部AC上统一对分支AC进行配置，称为正向配置。

- 统一配置模板
  用户可以登陆中心AC的命令行页面，通过命令行创建配置模板，并绑定分支AC。当分支AC首次和中心AC建立备份通道时，配置模板中的相关配置会自动下发给该分支AC。配置模板适用于WLAN、认证等全局性、一次性的配置业务。
- AP配置命令
  中心AC可将单AP配置模式或者AP组配置模式下的发生变更的配置自动同步给分支AC。当总部管理员在AP配置模式或者AP组配置模式下进行相关配置时，软件上自动完成该配置同步到分支AC。
- STA黑白名单
  中心AC配置STA接入的黑白名单后同步给分支AC。其中，STA黑白名单模板支持应用并同步到多个分支AC。

5. 反向配置同步

所有分支AC上的配置业务均由总部管理员在中心AC上进行配置，会带来大量的运维工作。另外，分支管理员将配置信息上报给总部管理员，再由总部管理员进行配置操作，该路径过长会带来不及时、配置信息不准确等情况。分级AC场景中，分支管理员是分支机构网络运维的直接负责人，应该具备对分支网络的直接操作权限，但是操作后又带来总部AC、分支AC配置不一致的情况。基于上述情况，锐捷无线产品推出反向配置同步功能，让分支AC将配置反向同步给总部AC，避免总部AC/分支AC配置不一致的情况发生。

> **说明**
> 将在分支AC上执行的配置业务，同步给总部AC的过程，称为反向配置同步。

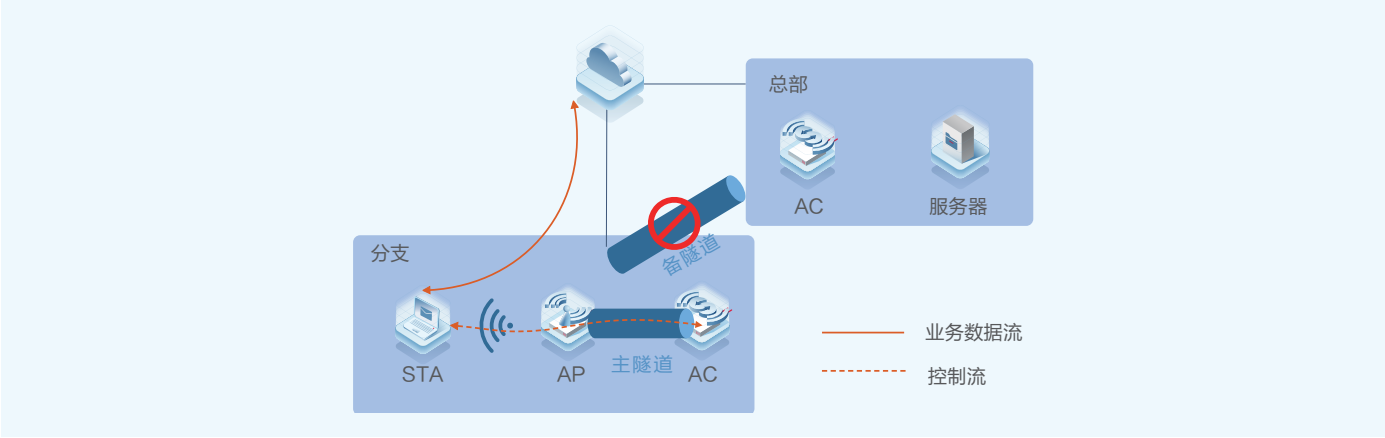
- AP配置命令
  分支AC可将单AP配置模式或者AP组配置模式下的发生变更的配置自动同步给中心AC。当分支管理员在AP配置模式或者AP组配置模式下进行相关配置时，软件上自动完成该配置同步到中心AC备份。
- STA黑白名单
  分支AC配置STA接入的黑白名单后同步给中心AC。其中，STA黑白名单模板同步到中心AC备份，并且中心AC能够继续同步至应用该STA黑白名单模板的其它分支AC，降低分支管理员的重复性工作。

AP双隧道备份

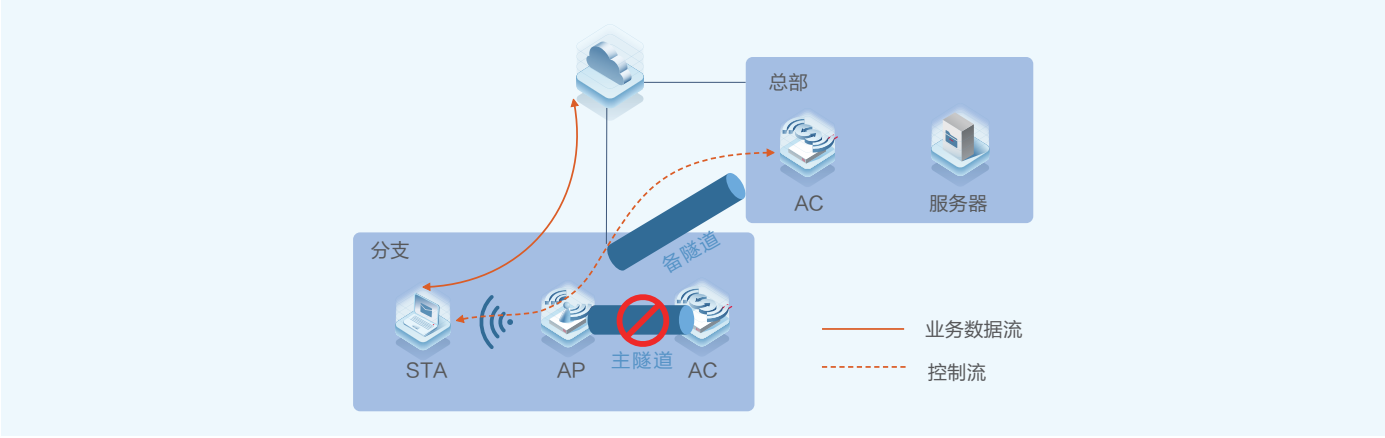
1. 备份原理

AP与总部/分支AC建立双隧道之后，通过CAPWAP隧道定期发送心跳报文进行心跳检测。当AP检测到CAPWAP隧道的心跳检测超时，则认为AP和该隧道对应的AC之间链路中断，会与该AC断开CAPWAP隧道。因此，存在两种断开CAPWAP隧道的场景：

(1) 若是AP检测到和总部AC间的链路中断，由于总部AC为备份AC，则用户业务不受影响。



(2) 若是AP检测到和分支AC间的链路中断，由于分支AC为主AC，则总部AC将切换为主AC，用户业务同时自动切换到总部AC上。



2. 授权管理

总部AC与分支AC管理同一台AP，涉及到AC上的AP授权问题，默认是要求多个AC都需要为同一个AP购买多次授权。分级AC场景中，总部与分支间的License授权支持共享。在总部AC导入全部授权后，可分享给分支AC使用，当分支AP离线，分支AC自动释放多余的License给总部AC。

分支AC自有License（含出厂自带）会同步给中心AC保存，分支AC在网时该分支AC对应的License在总部为不可用状态；而当分支AC离线后，临时恢复该分支AC对应License在总部为可用状态，确保总部AC转为主AC，分支AP不会因授权问题而无法接入。

License共享过程中，分级AC自动完成License的分配与回收，无需人工参与，减少按各个分支机构计算、导入或分配License授权的繁琐过程。

说明

总部AC共享给分支AC的License默认保留7天的使用权，最大14天。

分支AC离线后，在总部AC上恢复该分支对应License为可用状态，默认保留7天使用权，最大14天。

为保障分支机构的私有财产，分支AC自有License（含出厂自带）不允许共享给其它分支AC使用。

AP灾备逃生

通过在总分结构的备份网络中部署边缘智能感知技术，可以保证AP的主备CAPWAP链路都断开后，用户的业务不受影响，以此来提升无线网络的可靠性。

- 连接模式：开启边缘智能感知功能，且CAPWAP隧道连接正常的AP，称AP处于连接模式。
- 独立模式：开启边缘智能感知功能，但CAPWAP隧道连接断开的AP，称AP处于独立模式。

除了开放式网络外，针对启用了不同安全接入策略的用户，其逃生方式略有差异，包括链接加密用户逃生、802.1X认证用户逃生、外置Portal Web认证用户逃生三种。其中，链接加密用户逃生方式，和开放式网络下用户逃生方式没有区别，以下简要说明几种用户接入类型的逃生策略。

1. 链接加密/开放式网络用户逃生方式

在连接模式下，AC实时地将业务配置下发到AP上，AP会实时地将用户信息同步给AC。

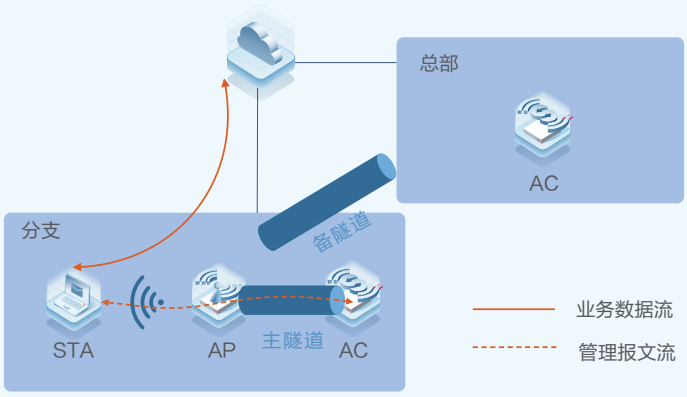


图2-4 AP处于连接模式时，用户关联示意图

在独立模式下，若是集中转发的WLAN网络，已经上线的用户将被迫离线，同时不允许新用户接入网络；若是本地转发的WLAN网络，由AP接管用户接入业务，让已在线用户保持在线，并允许新用户继续上线。

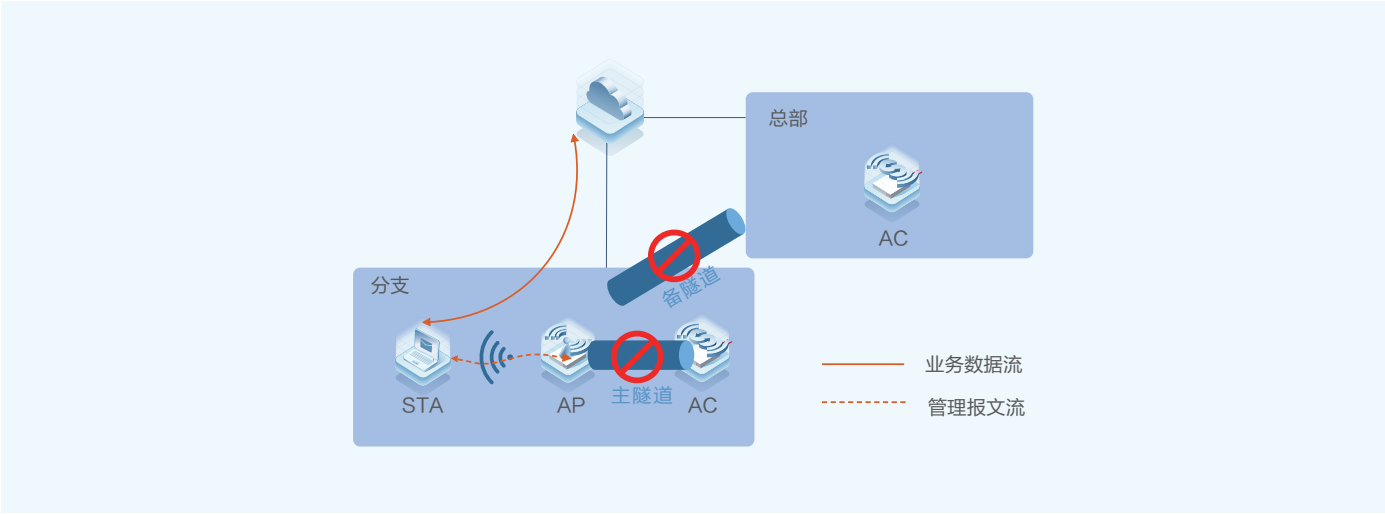


图2-5 AP处于独立模式时，用户关联示意图

2. 802.1X认证用户逃生

在开启了802.1X认证逃生的总部-分支结构的无线网中，通常在AC上部署两个无线信号下发给AP，一个信号开启802.1X认证（下文称为“802.1X信号”），另一个开放的缺省隐藏的无线信号（下文称为“逃生信号”）配置为在CAPWAP断开后再释放信号。

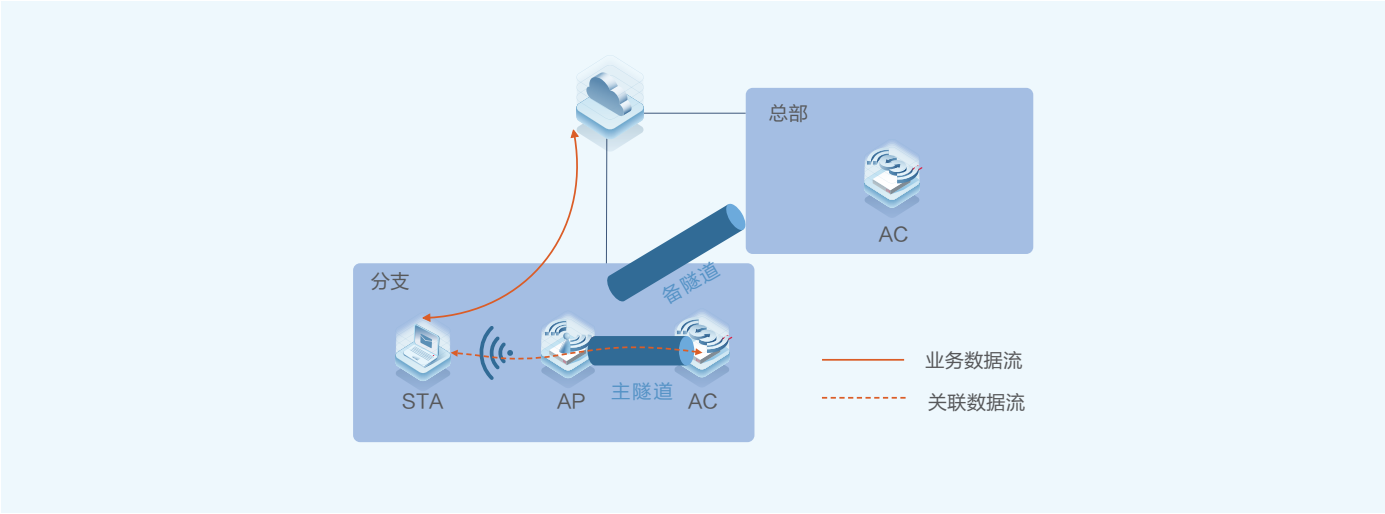


图2-6 AP处于连接模式时，用户认证示意图

在AP与AC连接正常的情况下，逃生信号隐藏，无线用户接入802.1X信号通过总部的认证服务器和总部AC完成认证过程，如图2-6所示。在认证客户端认证通过后，认证客户端的业务数据流直接通过分支机构的本地网络通往外网。

当CAPWAP断开链路时，逃生信号释放无线信号，AP能够继续提供数据业务，已认证成功802.1X老客户端业务不中断，新客户端会通过逃生信号接入免认证的无线网络访问外网，如图2-7所示。由于绝大多数的认证客户端都具备自动重认证功能，因此，在CAPWAP从断开恢复为链接状态后，已认证成功的802.1X老客户端可自动重新接入，对用户而言是无感知的，很好的保障了无线网的射频可靠性。

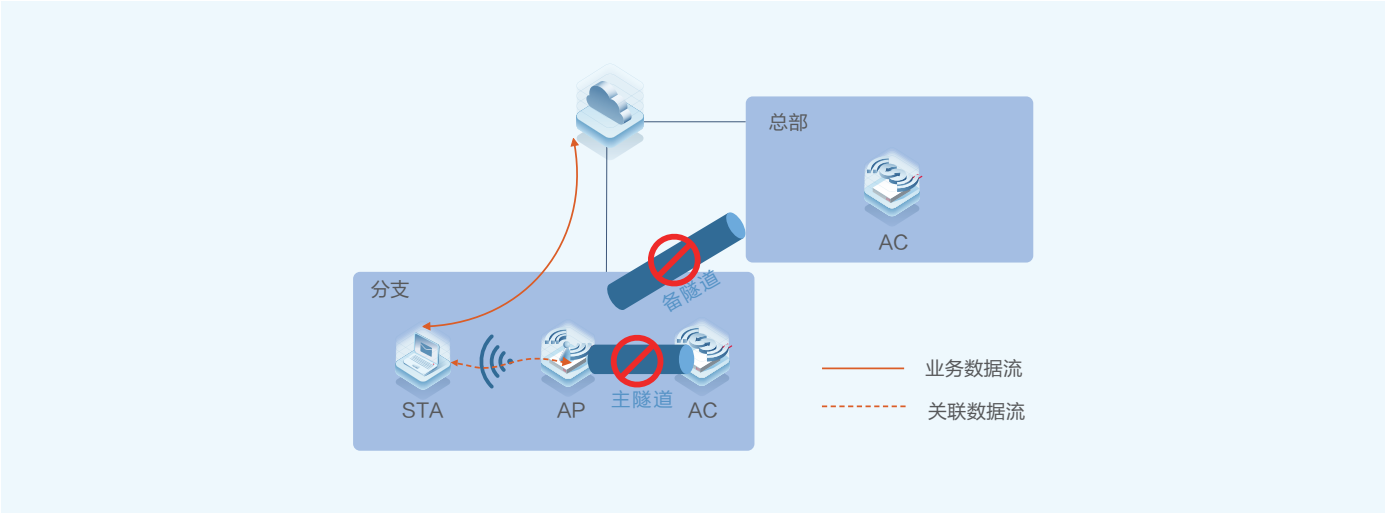


图2-7 AP处于独立模式时，用户接入示意图

3. 外置Portal Web认证逃生

Web认证逃生功能是指在AP的两条CAPWAP隧道都断开情况下，Web认证用户依然可接入无线网络。启用边缘智能感知功能和Web认证逃生功能后，在分支和总部AC上配置的Web认证信号会自动下发给AP，其认证系统图与图2-6 AP处于连接模式时，用户认证示意图类似。

a 当AP与AC的CAPWAP链路正常时，STA接入Web无线信号通过AC完成接入认证。

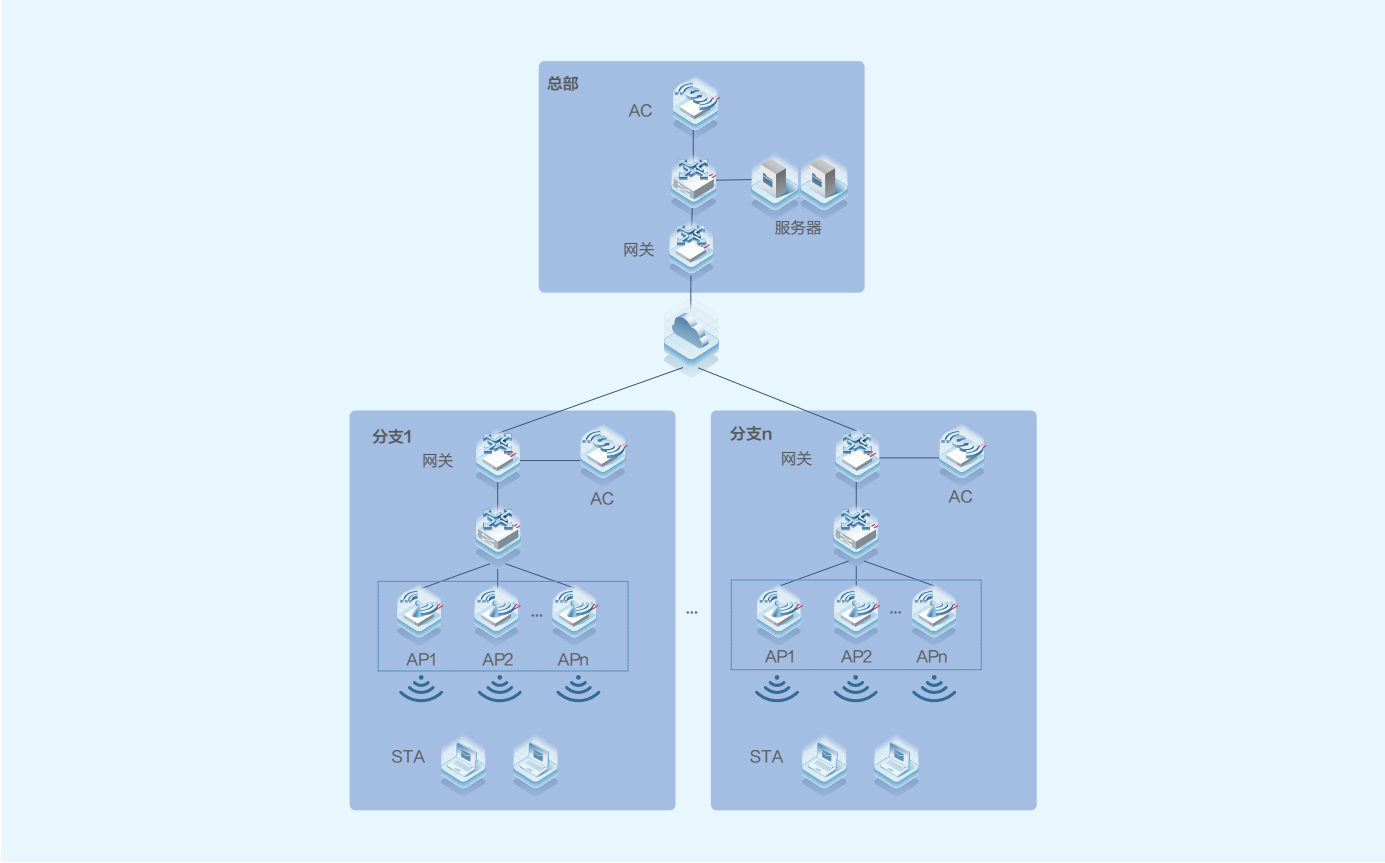
b 当CAPWAP断开后，下发给AP的Web认证信号自动转为免认证信号，AP可继续提供接入服务，已认证成功Web老用户业务不中断，新用户可以通过免认证信号接入网络，而不会影响用户体验。

c 当AP与AC之间的CAPWAP恢复连接后，用户只需重新Web认证便可继续使用网络。

典型应用

总分组网模型

总部-分支组网模型是分级AC的典型模型，可以应用于仓储物流行业、中大型办公及生产企业、普教城域网、多校区的高教等大规模多无线网点的网络建设场景。分级AC是一种集中管理 + 分布式转发的总部-分支模型，提供高可靠的无线网络，同时减少网络管理人员的工作量，降低网络维护的成本。



限制信息

- 在总分高可靠组网中，仅支持部署本地转发的无线网络。集中转发模式的无线网络对广域网链路的丢包、时延更为敏感，易引起网络可用性问题。
- 锐捷大部分AP产品和AC均支持分级AC。不支持分级AC的产品包括但不限于下表所示的产品型号。

产品类别	产品系列及型号
AP	智分无线接入点：RG-AM5532、RG-AM5528、RG-AM5514、RG-AM5528(ES)、RG-AM5528(EP)
	胖AP：所有型号均不支持
AC	RG-WS7005-A多业务无线控制器等

- 总部AC必须选择中高端型号：RG-WS7880、RG-WS6816、RG-WS6812、RG-WS6512、RG-M8600E-WS-ED、RG-M18000-WS-ED。
- 不同产品型号的中心AC可纳管的分支AC、分支AP数目不同。具体产品是否支持分级AC技术、具体产品的容量规格，请联系销售工程师评估。

常见问题

（1）区域的分级AC跨广域网通信时，如果广域网链路不稳定出现异常，对于总分架构组网的技术上是怎么解决保障的?

a 分支AC工作时，广域网链路影响的只是总部AC对分支AC的管理权，对无线网络服务无影响。

b 分支AC未工作，总部AC与分支AP广域网断开，RIPT边缘感知技术可以保障PSK/OPEN终端不受影响，认证终端可逃生。极端情况广域网时断时续、时延大，可开启AP本地接入保障PSK/OPEN终端不受影响，认证终端目前无解。

（2）总部AC出现故障时，分支AC怎么实现业务保障不断网?

常规状态下，总部AC只有管理面工作，即对分支AC、分支AP进行配置管理、状态监控等；而控制面工作在分支AC、分支管理员依旧可以通过分支AC对AP设备及无线网络进行控制，不受影响；转发面工作在分支AP，即无线终端的数据通信由分支AP负责数据转发，总部AC、分支AC均不参与，也不受影响。

（3）中心AC最大可接入多少分支AC、多少AP、多少用户数?

不同产品型号的总部AC可纳管的分支AC、分支AP数目存在差异，请参考不同型号AC的规格说明书。

但最大可支持分支AC数为500个，AP数为10240台。

（4）分支AC出现故障时，该AC下的所有用户终端切换到中心AC时，机制上是分批切换、还是统一一起切换，有没有容量数限制?

按AP分批切换，无容量限制。

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818

*本资料产品图片及技术数据仅供参考，如有更新恕不另行通知，具体内容解释权归锐捷网络所有。