分支机构REAP部署指南

目录

简介

本文档提供部署远程边缘接入点(REAP)时需要考虑的信息。 有关基本REAP配置信息，请参阅具有轻量AP和无线局域网控制器(WLC)的远程边缘AP(REAP)配置示例。

注意：REAP功能最高支持WLC版本3.2.215。从WLC版本4.0.155.5，此功能称为混合REAP(H-REAP)，在7.0.x.x之前只有少量增强功能。从7.2.103版本开始，此功能称为FlexConnect。

基于传统思科轻量接入点协议(LWAPP)的接入点(AP)（也称为LAP），例如运行Cisco IOS®软件版本12的1010、1020和1100和1200系列AP.3(7)JX或更高版本，允许通过思科的无线局域网控制器(WLC)进行集中管理和控制。 此外，这些LAP允许管理员将控制器用作无线数据聚合的单点。

虽然这些LAP允许控制器执行高级功能(如QoS和访问控制列表(ACL)实施)，但控制器对所有无线客户端流量而言成为入口和出口单点的要求可能阻碍（而非启用）充分满足用户需求的能力。在某些

环境（如远程办公室）中，事实证明，在控制器上终止所有用户数据会占用太多带宽，尤其是当广域网链路上的吞吐量有限时。此外，在LAP和WLC之间的链路容易中断的情况下，使用依赖WLC进行用户数据终止的LAP会导致在WAN中断期间断开无线连接。

相反，您可以利用AP架构，利用传统LWAPP控制平面来执行任务，例如动态配置管理、AP软件升级和无线入侵检测。这样，无线数据就可以保持在本地，而且无线基础设施可以集中管理并恢复广域网中断。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

1030 REAP架构简介

Cisco 1030 REAP将LWAPP控制平面与无线数据平面分离，以提供远程功能。Cisco WLC仍以与常规LAP相同的方式用于集中控制和管理。区别在于所有用户数据都在AP本地桥接。在WAN中断期间，对本地网络资源的访问会得到维护。图1显示了基本的REAP架构。

图 1：基本REAP架构图

注意：有关REAP功能与传统LAP的基本差异的列表，请参阅附录A。

何时应使用REAP AP?

Cisco 1030 REAP AP主要应在以下两种条件下使用：

- 如果LAP和WLC之间的链路容易中断，1030 REAP可用于在链路故障期间允许无线用户不间断地访问数据。
- 如果所有用户数据必须在本地终止(即在AP的有线端口终止（与在控制器终止相反，在控制器终止，因为数据是用于所有其他LAP）)，则1030 REAP可用于允许通过控制器接口和/或无线控制系统(WCS)进行集中控制。 这允许数据保持本地。

如果覆盖或用户密度要求在单个站点部署两个或三个以上1030个REAP AP，请考虑部署2006或2106 WLC。这些控制器最多可支持6个任何类型的LAP。与仅REAP部署相比，这可以证明更具经

济可行性，并提供一系列超级特性和功能。

与所有1000系列AP一样，单个1030 AP覆盖约5000平方英尺。这取决于每个站点的射频(RF)传播特性，以及所需的无线用户数量和其吞吐量需求。在大多数常见部署中，单个1000系列AP可以同时支持12个用户（802.11b的速率为512kbps），12个用户（802.11a的速率为2mbps）。与所有基于802.11的技术一样，介质访问是共享的。因此，当更多用户加入无线AP时，吞吐量会相应地共享。同样，随着用户密度的增加和/或吞吐量要求的提高，请考虑添加本地WLC以节省每用户成本并增加功能。

注意：您可以配置1030 REAP，使其与其他LAP相同地运行。因此，当添加WLC以扩展远程站点的WLAN基础设施时，可以继续利用现有REAP投资。

部署REAP

由于1030 REAP设计为放置在远离WLC基础设施的远程站点，因此通常不使用用于发现和加入控制器（如DHCP选项43）的传统零接触方法LAP。相反，必须首先预装LAP，以允许1030连接回中心站点的WLC。

启动是为LAP提供WLC列表的过程，WLC可以连接到该列表。加入单个WLC后，LAP将收到移动组中所有控制器的通知，并配备加入组中任何控制器所需的所有信息。有关移动组、负载均衡和控制器冗余的详细信息，请参阅部署Cisco 440X系列无线局域网控制器。

要在中心站点(如网络运营中心(NOC)或数据中心)执行此操作，REAP必须连接到有线网络。这允许他们发现单个WLC。加入控制器后，LAP将下载与WLAN基础设施对应的LAP操作系统版本。然后，移动组中所有WLC的IP地址将传输到AP。这允许AP在其远程站点通电后从其列表中发现并加入利用率最低的控制器，前提是IP连接可用。

注意：DHCP选项43和域名系统(DNS)查找也适用于REAP。有关如何在远程站点配置DHCP或DNS以允许AP查找中央控制器的信息，请参阅部署Cisco 440X系列无线局域网控制器。

此时，如果需要，可以为1030分配静态地址。这可确保IP编址方案与目的远程站点匹配。此外，可以输入WLC名称，以详细说明每个LAP将尝试连接哪三个控制器。如果这三个失败，则LWAPP的自动负载平衡功能允许LAP从集群中的其余控制器列表中选择负载最低的AP。LAP配置的编辑可通过WLC命令行界面(CLI)或GUI完成，或通过WCS更轻松地完成。

注意：1030个REAP需要连接到的WLC才能在第3层LWAPP模式下运行。这意味着需要为控制器指定IP地址。此外，WLC要求DHCP服务器在每个远程站点都可用，或者必须在启动过程中分配静态地址。控制器中嵌入的DHCP功能不能用于为1030s LAP或其用户提供地址。

在关闭1030 LAP以发货到远程站点之前，请确保每个1030都设置为REAP模式。这非常重要，因为所有LAP的默认设置是执行常规的本地功能，需要设置1030以执行REAP功能。这可以通过控制器CLI或GUI在LAP级别完成，也可以通过WCS模板更轻松地完成。

基本REAP启动功能

在1030个REAP连接到移动组内的WLC后，当REAP在远程站点上放置时，可以提供以下信息：

所需的REAP设置

- 移动组中WLC的IP地址列表（在控制器/AP连接时自动提供）
- REAP AP模式（必须将AP配置为在REAP模式下运行，才能执行REAP功能）

可选REAP设置

- 静态分配的IP地址（按AP输入的可选设置）
- 主要、辅助和第三WLC名称（可选设置输入，基于每个AP或通过WCS模板）
- AP名称（可选的信息性设置输入，基于每个AP）
- AP位置信息（可选信息设置，按AP或通过WCS模板输入）

REAP到控制器的链路要求

当您计划部署REAP时，需要记住一些基本要求。这些要求涉及REAP LWAPP控制流量将流经的广域网链路的速度和延迟。1030 LAP用于WAN链路，例如IP安全隧道、帧中继、DSL（非PPPoE）和租用线路。

注意：1030 REAP LWAPP实施假设AP和WLC之间有1500字节的MTU路径。由于MTU小于1500字节而在传输中发生的任何分段都会导致无法预测的结果。因此，1030 LAP不适用于PPPoE等环境，在PPPoE中，路由器会主动将数据包分段到1500个以下字节。

WAN链路延迟尤其重要，因为默认情况下，每1030 LAP每30秒向控制器发送一次心跳消息。心跳消息丢失后，LAP每秒发送5次连续的心跳。如果无成功，则LAP确定控制器连接已中断，1030将恢复为独立REAP模式。虽然1030 LAP能够容忍自身与WLC之间的大延迟，但必须确保LAP与控制器之间的延迟不超过100毫秒。这是由于客户端计时器限制客户端在确定身份验证失败之前等待的时间。

REAP限制

虽然1030 AP旨在集中管理并在广域网链路中断期间提供WLAN服务，但REAP通过WLC连接提供的服务与断开连接时提供的服务之间存在一些差异。

WLAN

虽然1030 REAP最多可支持16个WLAN（每个WLAN都包含服务集标识符[SSID]，以及所有安全、QoS和其他策略），每个WLAN都具有自己的多个基本服务集ID(MBSSID)，但1030 REAP只能支持第一个WLAN当与控制器的连接中断时。在WAN链路中断期间，除第一个WLAN外的所有WLAN都将停用。因此，WLAN 1应作为主WLAN，并相应地规划安全策略。第一个WLAN上的安全性尤其重要，因为如果WAN链路发生故障，后端RADIUS身份验证也会发生故障。这是因为此类流量通过LWAPP控制器平面。因此，没有用户被授予无线访问权限。

建议在第一个WLAN上使用本地身份验证/加密方法，例如Wi-Fi保护访问(WPA-PSK)的预共享密钥部分。有线等效保密(WEP)已足够，但由于已知的安全漏洞，不推荐使用。当使用WPA-PSK（或WEP）时，即使WAN链路关闭，正确配置的用户仍然可以访问本地网络资源。

注意：所有基于RADIUS的安全方法都要求通过LWAPP控制平面将身份验证消息传回中心站点。因此，在WAN中断期间，所有基于RADIUS的服务都不可用。这包括但不限于基于RADIUS的MAC身份验证、802.1X、WPA、WPA2和802.11i。

1030 REAP只能驻留在单个子网上，因为它无法执行802.1q VLAN标记。因此，每个SSID上的流量在有线网络的同一子网上终止。这意味着，虽然无线流量可能在SSID之间通过空中分段，但用户流量在有线端不会分离。

安全

1030 REAP可提供思科基于控制器的广域网架构支持的所有第2层安全策略。这包括所有第2层身份验证和加密类型，如WEP、802.1X、WPA、WPA2和802.11i。如前所述，这些安全策略中的大多数都需要WLC连接来进行后端身份验证。WEP和WPA-PSK在AP级别完全实施，不需要后端RADIUS身份验证。因此，即使WAN链路断开，用户仍可以连接。1030 LAP支持Cisco WLC中提供的客户端排除列表功能。如果可以连接回控制器，则MAC过滤功能在1030上运行。

注意：当AP处于独立模式时，REAP不支持WPA2-PSK。

1030 LAP不提供所有第3层安全策略。这些安全策略包括Web身份验证、基于控制器的VPN终端、ACL和点对点阻塞，因为它们是在控制器上实施的。VPN直通对连接到外部VPN集中器的客户端运行。但是，仅允许发往指定VPN集中器（仅VPN直通）的流量的控制器功能不允许。

网络地址转换 (NAT)

REAP连接的WLC不能驻留在NAT边界后。但是，如果用于LWAPP的端口(UDP端口12222和12223)被转发到1030，则远程站点的REAP可以位于NAT框后面。这意味着每个REAP必须具有静态地址才能使端口转发可靠工作，并且每个NAT实例后面只能有一个AP。原因是每个NAT IP地址只能存在一个端口转发实例，这意味着在远程站点的每个NAT服务后面只能有一个LAP。一对一NAT可以与多个REAP配合使用，因为LWAPP端口可以针对每个外部IP地址转发到每个内部IP地址（静态REAP IP地址）。

服务质量 (QoS)

基于802.1p优先位的数据包优先级不可用，因为REAP无法执行802.1q标记。这意味着不支持Wi-Fi多媒体(WMM)和802.11e。支持基于SSID和身份库网络的数据包优先级。但是，通过基于身份的网络分配VLAN与REAP无法配合使用，因为它无法执行802.1q标记。

漫游和客户端负载均衡

在存在多个REAP且需要AP间移动的环境中，每个LAP必须位于同一子网中。1030 LAP不支持第3层移动性。通常，这并不是限制，因为远程办公室通常没有配备足够的LAP来强制实施这种灵活性。

当上游控制器连接可用时，在具有多个单个AP的站点中的所有REAP之间提供主动客户端负载均衡（仅在主机控制器上启用负载均衡）。

Radio Resource Management (RRM)

当存在与控制器的连接时，1030个LAP会从WLC中的RRM机制接收动态信道和电源输出。当WAN链路关闭时，RRM无法正常工作，信道和电源设置不会更改。

欺诈检测和IDS功能

REAP架构支持与常规LAP匹配的所有欺诈检测和入侵检测签名(IDS)。但是，当与中央控制器的连接断开时，收集到的所有信息都不会共享。因此，对远程站点的RF域的可视性会丢失。

REAP限制摘要

附录B中的表汇总了REAP在正常运行期间以及在WAN链路上无法连接到WLC时的功能。

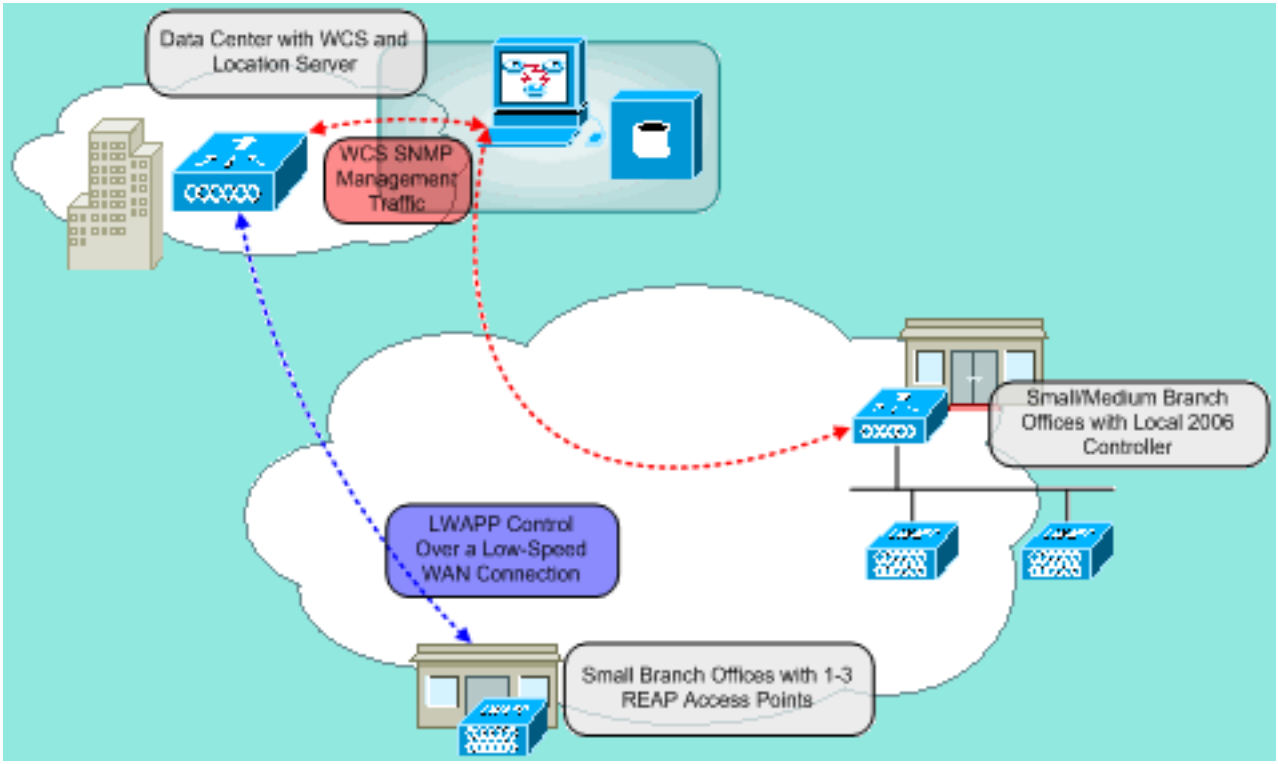
管理REAP和中心WLAN架构

1030 REAP管理与常规LAP和WLC的REAP管理无异。管理和配置全部在控制器级别完成，可通过每个控制器的CLI或Web GUI完成。通过WCS提供系统级配置和网络可视性，所有控制器和AP（REAP或其他）均可作为单个系统进行管理。当REAP控制器连接中断时，管理功能也会中断。

采用REAP的集中式WLAN架构

图2显示了集中式LWAPP架构的每个部分如何协同工作以满足各种无线网络需求。通过WCS和2700位置设备集中提供管理和位置服务。

图 2：采用REAP的集中式WLAN架构



附录 A

REAP架构和常规LAP之间的主要区别是什么？

- 如果DHCP选项43或DNS解析在远程站点不可用，则必须先在中心办公室预装1030。然后，将其发送到目标站点。
- 在WAN链路发生故障时，只有第一个WLAN保持活动状态。需要RADIUS的安全策略将失败。WLAN 1建议使用WPA-PSK的身份验证/加密。WEP有效，但不建议使用。
- 无第3层加密（仅第2层加密）
- REAP连接的WLC不能驻留在NAT边界后。但是，如果每个内部静态REAP IP地址都将两个LWAPP端口(12222和12223)转发给它们，则REAP可以。**注意**：不支持端口地址转换(PAT)/过载NAT，因为源自LAP的LWAPP流量的源端口可能随时间而改变。这会中断LWAPP关联。在REAP的NAT实施中，端口地址可能会发生更改（如PIX/ASA），具体取决于配置时，可能会出现同样的问题。
- 只有LWAPP控制消息通过WAN链路。
- 数据流量在1030的以太网端口桥接。

- 1030 LAP不执行802.1Q标记(VLAN)。 因此，来自所有SSID的无线流量会终止于同一有线子网。

附录 B

正常和独立REAP模式在功能上有何区别？

		REAP（正常模式）	REAP（独立模式）
协议	IPv4	Yes	Yes
	IPv6	Yes	Yes
	所有其他协议	是（仅当客户端也启用IP时）	是（仅当客户端也启用IP时）
	IP 代理 ARP	无	无
WLAN	SSID数量	16	1（第一个）
	动态信道分配	Yes	无
	动态功率控制	Yes	无
	动态负载均衡	Yes	无
VLAN	多个接口	无	无
	802.1Q支持	无	无
WLAN安全	欺诈AP检测	Yes	无
	排除列表	Yes	是（仅现有成员）
	点对点阻塞	无	无
	入侵检测系统	Yes	无
第2层安全	MAC 验证	Yes	无
	802.1X	Yes	无
	WEP(64/128/152位)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	Yes	无
	WPA-EAP	Yes	无
	WPA2-EAP	Yes	无
第3层安全	Web 身份验证	无	无
	IPsec	无	无
	L2TP	无	无
	VPN直通	无	无
	访问控制列表	无	无
QoS	QoS配置文件	Yes	Yes
	下行链路QoS（加权轮询队列）	Yes	Yes
	802.1p支持	无	无

	每用户带宽合同	无	无
	WMM	无	无
	802.11e（未来）	无	无
	AAA QoS配置文件覆盖	Yes	无
移动性	子网内	Yes	Yes
	子网间	无	无
DHCP	内部 DHCP 服务器	无	无
	外部 DHCP 服务器	Yes	Yes
拓扑	直接连接（2006年）	无	无

相关信息

- 具有轻量AP和无线局域网控制器(WLC)的Remote-Edge AP (REAP)与配置示例
- 统一无线网络中的 AP 负载均衡和 AP 后退
- 部署 Cisco 440X 系列无线局域网控制器
- 无线 LAN 控制器和轻量接入点基本配置示例
- 技术支持和文档 - Cisco Systems