无线接入点术语表

目标

本文包含用于设置、配置和排除Cisco无线接入点(WAP)故障的术语列表。

适用设备

- 无线接入点

一般术语列表

- 基于802.1Q的VLAN - IEEE 802.1Q规范为使用VLAN成员信息标记以太网帧建立标准方法，并定义VLAN网桥的操作，允许定义、操作和管理桥接LAN基础设施中的VLAN拓扑。802.1Q标准旨在解决以下问题：如何将大型网络划分为更小的部分，以便广播和组播流量使用的带宽不会超过必要的带宽。该标准还有助于在内部网段之间提供更高级别的安全性。

- 802.1X请求方-请求方是802.1X IEEE标准中的三个角色之一。开发802.1X的目的是在OSI模型的第2层提供安全保护。它由以下组件组成：Supplicant客户端、身份验证器和身份验证服务器。Supplicant客户端或软件连接到网络，以便访问网络中的资源。 它需要提供凭证或证书来获取IP地址并成为该特定网络的一部分。请求方在经过身份验证之后才能访问网络资源。

- ACL —访问控制列表(ACL)是网络流量过滤器和相关操作的列表，用于提高安全性。它阻止或允许用户访问特定资源。ACL包含允许或拒绝访问网络设备的主机。ACL可以通过以下两种方式之一进行定义：按IPv4地址或按IPv6地址。

- 频段转向-高级负载平衡（也称为频段转向）是一种检测能够在5 GHz频段传输的设备的功能。2.4 GHz频段经常拥塞，并且遇到来自不同设备（例如蓝牙甚至微波炉）的干扰。此功能允许您的接入点将设备引导到更优化的无线电频率，从而提高网络性能。

- 带宽利用率—带宽利用率使您可以对通过通信路径成功传输的平均数据设置阈值。一些用于改善此状况的技术包括带宽整形、管理、上限和分配。

- Bonjour — Bonjour允许使用组播DNS来发现接入点及其服务。它向网络通告其服务并回答对其支持的服务类型的查询，从而简化小型企业环境中的网络配置。在受支持的WAP设备上启用Bonjour后，任何Bonjour客户端无需事先配置即可发现并访问基于Web的实用程序。Bonjour同时在IPv4和IPv6网络中工作。

- 强制网络门户-强制网络门户方法强制网络上的LAN用户或主机在正常访问公共网络之前查看特定网页。强制网络门户将Web浏览器转变为身份验证设备。在允许访问使用网络之前，网页需要用户交互或身份验证。

- 信道隔离-启用了信道管理的设备会自动将无线无线电信道分配给集群中的其他WAP设备。自动信道分配可降低对其集群之外的其他接入点的干扰，并最大限度地提高Wi-Fi带宽，有助于保持无线网络通信的效率。

- 客户端QoS -客户端服务质量(QoS)关联是一个部分，提供用于自定义无线客户端QoS的其他

选项。这些选项包括允许发送、接收或保证的带宽。客户端QoS关联还可以使用访问控制列表(ACL)进行处理。

- 事件日志记录—系统事件是系统中的活动，可能需要引起注意并采取必要的行动，才能使系统平稳运行并防止出现故障。这些事件将记录为日志。系统日志使管理员能够跟踪设备上发生的特定事件。事件日志对于网络故障排除、调试数据包流和监控事件非常有用。

- 快速漫游-无线接入点之间的快速漫游允许快速、安全、不间断的无线连接，以实现实时应用（如FaceTime、Skype和Cisco Jabber）的无缝移动体验。

- HTTPS —安全超文本传输协议(HTTPS)是一种比HTTP更安全的传输协议。当配置了HTTP/HTTPS服务器时，可以通过HTTP和HTTPS连接管理接入点。某些Web浏览器使用HTTP，而其它浏览器使用HTTPS。接入点必须具有有效的安全套接字层(SSL)证书才能使用HTTPS服务。

- IPv4 - IPv4是用于识别网络中设备的32位寻址系统。它是大多数计算机网络（包括Internet）中使用的编址系统。

- IPv6 - IPv6是用于识别网络中设备的128位寻址系统。它是IPv4的后继者，也是计算机网络中使用的最新版本寻址系统。IPv6目前正在全球推广。IPv6地址以八个十六进制数字字段表示，每个字段包含16位。IPv6地址分为两部分，每部分由64位组成。第一部分是网络地址，第二部分是主机地址。

- LLDP —链路层发现协议(LLDP)是在IEEE 802.1AB标准中定义的发现协议。LLDP允许网络设备将自身信息通告给网络中的其他设备。LLDP使用逻辑链路控制(LLC)服务来与其他LLDP代理相互传输和接收信息。LLC为访问LLDP提供链路服务接入点(LSAP)。每个LLDP帧都作为单个MAC服务请求进行传输。LLC实体在MAC服务接入点(MSAP)处接收每个传入LLDP帧作为MAC服务指示。

- 负载均衡—负载均衡是一种网络术语，用于跨多台计算机、网络链路和各种其他资源分配工作负载，以实现适当的资源利用率、最大化吞吐量和响应时间，并主要避免过载。

- MAC ACL —基于访问控制列表(ACL)的介质访问控制(MAC)是源MAC地址列表。如果数据包从无线接入点传输到LAN端口（反之亦然），此设备将检查数据包的源MAC地址是否与此列表中的任何条目匹配，并检查ACL规则与帧内容是否匹配。然后，它使用匹配的结果来允许或拒绝此数据包。但是，不会检查从LAN到LAN端口的数据包。

- 多个SSID -您可以在接入点上配置多个服务集标识符(SSID)或虚拟接入点(VAP)，并为每个SSID分配不同的配置设置。所有SSID可能同时处于活动状态。客户端设备可以使用任意SSID与接入点关联。

- 工作模式- WAP设备可以充当单点对点模式接入点、点对多点网桥和中继器。在点对点模式下，单个WAP设备接受来自客户端和网络中其他设备的连接。在点对多点桥接模式下，单个WAP设备作为多个接入点之间的通用链路运行。WAP设备还可以用作中继器，它可以在彼此远离的接入点之间建立连接。无线客户端可以连接到此中继器。无线分布系统(WDS)角色系统可以与中继器的角色系统相提并论。

- 数据包捕获-数据包捕获是网络设备的一项功能，使用此功能可以捕获和存储设备传输和接收的数据包。网络协议分析器可以分析捕获的数据包，以排除故障或优化性能。捕获的数据包文

件可以通过HTTP/HTTPS或TFTP服务器下载。可以共享该数据包，然后对其进行进一步分析，以了解网络中的数据包流。Packet Capture（数据包捕获）页面可用于配置远程或本地数据包捕获、下载数据包捕获文件或查看当前捕获状态。

- QoS -服务质量(QoS)允许您为不同的应用、用户或数据流确定流量的优先级。它还可以用于保证性能达到指定级别，从而影响客户端的服务质量。QoS通常受以下因素的影响：抖动、延迟和丢包。

- RADIUS服务器-远程身份验证拨入用户服务(RADIUS)是设备连接和使用网络服务的身份验证机制。它用于集中身份验证、授权和记帐。RADIUS服务器通过输入的登录凭证验证用户的身份来监管对网络的访问。例如，在大学校园中安装了公共Wi-Fi网络。只有那些拥有密码的学生才能访问这些网络。RADIUS服务器会检查用户输入的密码，并根据需要授予或拒绝访问权限。

- 远程管理-远程管理从远程位置操作网络设备的设置。这通常在计算机、交换机、路由器等具有IP地址的设备上完成。它使网络管理员能够快速响应请求或挑战，因为他们不必亲自到场。在远程管理中访问设备与本地操作几乎相同，不同之处在于设备的本地IP地址用于本地访问设备，而在远程设备上访问设备时则使用设备的WAN IP。

- 欺诈AP检测—欺诈接入点(AP)是在未获得系统管理员明确授权的情况下安装在网络上的接入点。非法接入点会带来安全威胁，因为任何能够访问该区域的人都可以故意或不知情地安装一个无线接入点，使未经授权的用户能够访问网络。接入点上的“非法AP检测”功能允许其查看范围内的这些非法接入点，并在基于Web的实用程序中显示其信息。您可以将任何授权接入点添加到受信任AP列表。

- RSTP —快速生成树协议(RSTP)是STP的增强功能。RSTP在拓扑更改后提供更快的生成树收敛。STP可能需要30到50秒来响应拓扑更改，而RSTP则会在配置的hello时间的三倍之内做出响应。RSTP与STP向后兼容。

- 调度程序-无线调度程序可帮助调度虚拟接入点(VAP)或无线电正常运行的时间间隔，这有助于节省电力并提高安全性。您最多可以将16个配置文件关联到不同的VAP或无线电接口，但每个接口仅允许一个配置文件。每个配置文件可具有特定数量的时间规则，用于控制关联VAP或WLAN的运行时间。

- 单点设置—单点设置是一种简单的多设备管理技术，允许您部署和管理一组支持此功能的接入点。它提供了从单个点配置一组接入点而不是单独配置接入点的便利性。它还允许您在本地或远程管理接入点。

- SNMP -简单网络管理协议(SNMP)是用于存储和共享网络设备信息的网络标准。SNMP有助于网络管理、故障排除和维护。

- 生成树-生成树协议(STP)是LAN上使用的网络协议。STP的目的是确保LAN的无环拓扑。STP通过一种算法来消除环路，该算法可确保两台网络设备之间只有一条活动路径。STP可确保流量在网络中采用尽可能短的路径。如果主用路径发生故障，STP还可以自动重新启用冗余路径作为备用路径。

- SSID -服务集标识符(SSID)是无线客户端可以连接到无线网络中的所有设备或在其中共享的唯一标识符。它区分大小写，并且不能超过32个字母数字字符。这也称为无线网络名称。

- SSID广播-当无线设备搜索可连接的无线网络的区域时，它会通过其网络名称或SSID检测其范围内的无线网络。默认情况下启用SSID广播。但是，您也可以选择禁用。

- TSPEC —流量规范(TSPEC)是从支持QoS的无线客户端发送到请求一定数量的网络访问的WAP设备的流量规范，它代表流量流(TS)。

- VLAN -虚拟局域网(VLAN)是一种交换网络，它按功能、区域或应用进行逻辑分段，而不考虑用户的物理位置。VLAN是一组主机或端口，它们可以位于网络中的任何位置，但进行通信的方式与它们位于同一个物理网段上一样。VLAN允许您将设备移动到新的VLAN而不更改任何物理连接，从而有助于简化网络管理。

- WDS -无线分布系统(WDS)是一种功能，可在网络中实现接入点的无线互连。它使用户能够通过多个接入点以无线方式扩展网络。WDS还会保留通过接入点之间的链路传输的客户端帧的MAC地址。此功能至关重要，因为它为漫游客户端提供无缝体验并允许管理多个无线网络。

- WMM - Wi-Fi多媒体(WMM)功能为不同类型的流量分配不同的进程优先级。WMM也是一种QoS功能，它通过设置无线数据包的优先级来增强无线网络的性能，该优先级基于四个类别：语音、视频、尽力而为和背景。默认情况下，WMM已启用。如果应用不需要WMM，则其优先级低于视频和语音。

- 无线隔离-阻止连接到不同SSID的计算机之间的通信和文件传输。一个SSID上的流量不会转发到任何其他SSID。

- WPA/WPA2 — Wi-Fi保护访问（WPA和WPA2）是用于无线网络的安全协议，用于通过加密无线网络上传输的数据来保护隐私。WPA和WPA2均与IEEE 802.11e和802.11i向前兼容。与有线等效保密(WEP)安全协议相比，WPA和WPA2改进了身份验证和加密功能。

网状网络中的术语列表

- 接入点(AP)：网络中用于允许用户以无线方式连接到网络的设备。根据其功能，可添加特定标签：主要、远程、根、从属等。
- 无线网状网络：一种拓扑，其中无线接入点彼此连接以中继信息。这些网络以动态方式工作，从而调整需求并维护所有用户的连接。
- 主AP：主AP提供对无线网络和拓扑的管理和控制。它是使用Internet服务提供商(ISP)连接到外部网络其余部分的网桥（通常是Internet）。主AP直接链接到本地路由器，而本地路由器又将流量路由到WAN ISP接口。主AP是网状网络中提供无线服务的所有节点的协调器。它管理来自网络上节点的信息、每个客户端的连接质量和邻居信息，以便做出最佳路由决策，将优化的无线服务输出到移动客户端。
- 主要主要：当前负责管理无线局域网的AP。
- Preferred Primary：将支持主功能的特定接入点列为首选的设置。如果主AP发生故障，首选主AP将接管。一旦首选AP恢复，它不会自动切换回。您没有指定Preferred Primary。
- 主要支持AP：具有返回网络的物理有线连接的AP。此AP需要连接到以太网，如果主AP发生故障，此AP可以成为主AP。
- 网状网扩展器：网络中未连接到有线网络的远程从属AP。
- 从属AP：一般术语，可应用于未配置为主网状AP的任何网状AP。
- 父AP：父AP是为返回主AP提供最佳路由的AP。

- 子AP：子AP是网状扩展器，选择父AP作为返回主AP的最佳路由。
- 上行AP：上行AP是一般术语，指数据从客户端传输到服务器时通过AP的方向。
- 下行AP：下行AP将数据从Internet向下传送到客户端。
- 共置AP：回传信道广播范围内的网状网扩展器。
- 节点：在本文中，AP称为节点。一般来说，节点描述的是在网络中建立连接或交互，或者能够发送、接收和存储信息、与互联网通信并具有IP地址的任何设备。在网状网络中，所有节点上的优化无线参数可确保最大无线覆盖范围，同时减少节点之间的无线干扰，以提供卓越的数据速度和吞吐量。
- 回程：在无线网状网络中，局域网(LAN)中的信息需要到达有线接入点才能到达互联网。回传是将信息返回到有线接入点的过程。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。