无线访问访问接入点术语词汇表

客观

此条款包含用于安装，配置和排除Cisco无线接入点术语目录(WAP)故障。

可适用的设备

- 无线访问访问接入点

术语目录

- 基于802.1Q的VLAN — IEEE 802.1Q规格设立标记的以太网帧一个标准方法用VLAN成员信息，并且定义了的VLAN网桥操作允许VLAN结构定义、操作和管理在桥接LAN基础设施内的。802.1Q标准打算涉及问题的如何隔开大型网络成更小的零件，因此请播放，并且组播数据流比必要不使用更多带宽。标准帮助也提供高水平在内部网络的分段的之间安全。
- 802.1X请求方—请求方是在802.1X IEEE标准的三作用之一。802.1X被开发提供在OSI模型的第2层的安全。它由以下组件组成：请求方、证明人和认证服务器。请求方是连接到网络的客户端或软件，以便能访问在该网络的资源。 它需要提供证件或证书获得IP地址和是该特定网络的一部分。请求方不能访问网络资源，直到验证。
- ACL —访问控制表(ACL)是网络列表用于的数据流过滤器和关联的动作改进安全。它阻拦或允许用户访问特定资源。ACL包含允许或对网络设备的拒绝访问的主机。ACL可以在两种方式之一中被定义：由IPv4地址或由IPv6地址。
- 波段操舵—先进的负载均衡，以波段指点更著名，是发现设备能够传输在5 GHz频段的功能。2.4 GHz频段经常拥塞并且体验从不同的设备的甚而干扰例如蓝牙和微波炉。此功能允许您的接入点操纵和处理设备到更加最佳的无线电频率，因而，改进网络性能。
- 带宽利用率—带宽利用率在平均的成功的数据传输允许您放置阈值通过通信路径。用于的某些技术改进此是整形的带宽，管理，加盖和分配。
- Bonjour — Bonjour允许接入点和其服务将被发现通过使用组播DNS。它在小型企业环境里通告其服务对网络和答案查询为支持的服务类型，简单化网络配置。当Bonjour在一个支持的WAP设备时被启用，所有Bonjour客户端能发现和访问基于Web的工具，不用前期配置。Bonjour在IPv4和IPv6网络工作。
- 俘虏门户—俘虏门户方法强制LAN用户或主机在看到一个特殊网页的网络，在他们能通常前访问公共网络。俘虏门户把一Web浏览器变成认证设备。在访问允许使用网络前，网页要求用户交互作用或认证。
- 信道隔离—有信道管理功能的一个设备自动地分配无线信号发射信道到在簇的其他WAP设备。自动信道分配减少干扰用其他接入点在其簇外面并且最大化Wi-Fi带宽帮助维护通信效率在无线网络的。
- 客户端QoS —客户端服务质量(QoS)关联是该的部分无线客户端的QoS的定制的提供其它选项。这些选项包括允许发送，接受或者保证的带宽。客户端QoS关联可能进一步操作与使用访问控制列表(ACL)。
- 事件日志—系统事件是在可能要求将被采取的注意和必要的动作为了顺利运行系统和防止故障的系统的活动。这些事件被记录作为日志。系统日志enable (event)记录在设备发生的特定的事件的管理员。事件日志为排除故障的网络是有用的，调试信息包流和监控事件。
- 快速地漫游—快速地漫游在无线访问访问接入点之间允许一个快速，安全和不间断的无线连接达到实时应用的无缝的便携经验例如FaceTime、Skype和Cisco Jabber。
- HTTPS —安全的超文本传输协议(HTTPS)是比HTTP安全的传输协议。当配置时，接入点可以通过HTTP和HTTPS连接被管理HTTP/HTTPS服务器。当其他使用HTTPS时，一些Web浏览器

使用HTTP。接入点必须有使用一个有效安全套接字层SSL的认证HTTPS服务。

- IPv4 — IPv4是用于的32位寻址系统识别在网络的一个设备。是用于多数计算机网络的寻址系统，包括互联网。
- IPv6 — IPv6是用于的128-bit寻址系统识别在网络的一个设备。是后继对IPv4和用于计算机网络的寻址系统的多数最新版本。IPv6当前被转出环球。IPv6地址在八表示十六进制数字领域，包含16位的每个字段。IPv6地址分开成两部分，每个部分组成由64位。是的第一部分网络地址和第二部分主机地址。
- LLDP —链路层发现协议(LLDP)是在IEEE 802.1AB标准被定义的发现协议。LLDP允许网络设备发布关于他们自己的信息到在网络的其它设备。LLDP使用逻辑链路控制(LLC)服务到/从其他LLDP代理程序传播和获得信息。LLC提供一个链路服务访问点(LSAP)进入对LLDP的入口。每个LLDP帧被传输作为单个MAC服务请求。每个流入LLDP帧接收在MAC服务访问点(MSAP)由LLC实体作为MAC服务征兆。
- 负载均衡—负载均衡是用于分配在多台计算机、网络链路和各种各样的资源间的工作量取得适当的资源利用率的网络术语，最大化吞吐量，响应时间和主要避免超载。
- MAC ACL —根据访问控制表(ACL)的媒体访问控制(MAC)是源MAC地址列表。如果信息包自无线访问访问接入点来到局域网端口或反之亦然，此设备检查信息包的源MAC地址是否匹配在此列表的任何条目并且根据帧的内容检查ACL规则。它然后使用被匹配的结果允许或丢弃此信息包。然而，信息包从LAN到局域网端口不会被检查。
- 多个SSID —您能配置几个服务集标识(Ssid)或虚拟访问访问接入点(VAPs)在您的接入点和分配不同的配置设置到每SSID。所有Ssid可能同时是活跃的。使用任何Ssid，客户端设备能联合到接入点。
- 操作模式— WAP设备能作为单点到点集式接入点，点对多点网桥和作为中继器。在点到点模式下，单个WAP设备接受从客户端和其它设备的连接在网络。在点对多点网桥模式下，单个WAP设备正常运行作为许多接入点之间的一条普通的链路。WAP设备能也作为中继器，能建立接入点之间的连接是离得很远从彼此。无线客户端能连接到此中继器。一个无线分布式系统(WDS)角色系统可以比较的类似于中继器的角色。
- 信息包获取—信息包获取是enable (event)获取和存储信息包的您由设备传输并且收到网络设备的功能。获取信息包可以被网络协议分析器分析排除或优化性能故障。获取信息包文件可以通过HTTP/HTTPS或TFTP server下载。可以共享进一步然后分析它了解在网络的信息包流。信息包获取页可以用于配置远程或本地信息包捕获，下载信息包捕获文件或者查看当前捕获状态。
- QoS —服务质量(QoS)允许您指定优先级不同的应用程序、用户或者数据流的数据流。它可能也用于保证性能到一个指定的级别，因而，影响客户端的服务质量。QoS通常是受以下要素的影响的：抖动、潜伏期和信息包丢失。
- RADIUS服务器—远程验证拨入用户服务(RADIUS)是使用的设备的一个认证机制能连接和网络服务。它使用集中认证、授权和记帐目的。RADIUS服务器通过验证用户的身份调控对网络的访问通过被输入的登录证件。例如，公共Wi-Fi网络在大学校园上安装。有密码只有的那些学员能访问这些网络。RADIUS服务器检查用户输入的密码并且准许或者拒绝访问如适当。
- 远程管理—远程管理操作一个网络设备的设置从一个远端位置的。这在设备典型地执行类似有一个IP地址的计算机、交换机，路由器和许多其他。因为他们不必须物理的，现场它允许网络管理员迅速回答请求或挑战。接入设备在远程管理方面是几乎类似执行它本地，除了设备的本地IP地址用于访问设备本地，而使用设备的广域网IP，当执行它在一个远端设备时。
- 非法AP检测—恶意接入点(AP)是在网络上安装了，不用明确授权从系统管理员的接入点。恶意接入点造成一个安全威胁，因为任何人与对区域的访问能熟悉或不知道安装能允许未授权的当事人访问网络的无线访问访问接入点。在您的接入点的非法AP检测功能允许它发现在范围内的这些恶意接入点和显示他们的在基于Web的工具的信息。您能添加对委托的AP列表的所有被核准的接入点。
- RSTP —快速生成树协议(RSTP)是STP的增进。RSTP在拓扑更改以后提供一更加快速的生成

树收敛。当RSTP在三倍内回应被配置的Hello时间时， STP能用回应的30到50秒拓扑更改。RSTP向后是与STP兼容。

- 调度程序—无线调度程序帮助安排时间间隔于虚拟访问访问接入点(VAP)或无线电是可操作的，帮助节省功率和强化安全。您能关联16个配置文件到另外VAPs或无线接口，但是每个接口只提供一个配置文件。每个配置文件能有一定数量的时间规定该控制相关的VAP或WLAN的正常运行。
- 单点设置—单点设置是允许您配置和管理一个组接入点支持功能的简单，多设备的管理技术。它提供配置一个组便利从单点的接入点而不是单个配置他们。它也允许您本地或远程管理接入点。
- SNMP —简单网络管理协议(SNMP)是存储和共享信息网络标准关于网络设备。SNMP实现网络管理，排除故障和维护。
- 生成树—生成树协议(STP)是在LAN使用的网络协议。STP的目的将保证LAN的一个无回环拓扑。STP通过保证的算法去除循环只有两个网络设备之间的一活动路径。STP保证数据流上最短路径可能在网络内。如果活动路径出故障， STP能自动地也重新授权给冗余路径作为备用路径。
- SSID —服务集标识(SSID)是无线客户端能连接到或共享在无线网络的所有设备的唯一标识符。它区分大小写，并且不能超出32个字母或数字字符。这也称为无线网络名字。
- SSID广播—当无线设备搜索区域能连接到的无线网络，通过他们的网络名或Ssid将发现在其范围内的无线网络。SSID的默认情况下广播被启用。然而，您可以也选择禁用它。
- TSPEC —数据流规格(TSPEC)是从一个支持QOS的无线客户端被发送到WAP设备要求一定数量的网络访问为数据流的数据流规格(TS)它表示。
- VLAN —虚拟局域网是由功能、区域或者应用程序逻辑上分段的交换网络，不考虑用户的物理位置。VLAN是可以任何地方位于网络的一个组主机或端口，但是沟通，好象他们在同一个物理分段。VLAN帮助简化网络管理通过让您移动设备向新的VLAN没有更改任何物理连接。
- WDS —无线分布式系统(WDS)是功能enable (event)接入点的无线互连在网络的。它enable (event)扩展网络的用户用多接入点无线地。WDS也保留客户端帧MAC地址在链路间的接入点之间。因为为漫游的客户端提供一个无缝的经验并且允许多个无线网络的管理，此功能是重要。
- WMM —Wi-Fi多媒体(WMM)是指定不同的流程优先级到不同类型的流量的功能。WMM也是通过设置根据四个类别的无线数据包优先权提高无线网络性能的QoS功能：语音、视频、尽力和背景。默认情况下， WMM是启用的。如果应用程序不要求WMM，比视频和语音产生低优先级。
- 无线隔离—防止通信和文件传输在被连接到不同的Ssid的计算机之间。在一SSID的数据流不会转发到任何其他Ssid。
- WPA/WPA2 —Wi-Fi受保护的访问(WPA和WPA2)是用于无线网络的安全协议保护保密性通过加密在无线网络的传送的数据。WPA和WPA2是向前与IEEE 802.11e兼容和802.11i。WPA和WPA2改进认证和加密功能与有线等效保密(WEP)安全协议比较。