无线访客接入常见问题

目录

简介

什么是连接非安全网络区域的 Ethernet over IP (EoIP) 隧道？

如何选择正确的控制器以部署为访客锚点控制器？

在访客锚点控制器上可以有多少个 Ethernet over IP (EoIP) 隧道终端？

能否在运行不同软件版本的控制器之间创建 Ethernet over IP (EoIP) 隧道？

Cisco 2100/2500 系列无线局域网控制器能否用作非安全网络区域中的访客锚点控制器？

适用于集成多业务路由器的思科无线局域网控制器模块（WLCM或WLCM2）能否用作非安全网络区域中的访客锚点控制器？

哪些控制器可用来支持非安全网络区域中的访客接入？

如果在防火墙之外使用访客锚点控制器，需要为访客接入打开哪些防火墙端口？

在配置了网络地址转换 (NAT) 的情况下访客流量能否通过防火墙？

在“锚点 - 外部 WLC”方案中，哪个 WLC 将发送 RADIUS 记帐？

内部控制器与锚点控制器之间的访客隧道出现故障。我在WLC中看到以下日志：mm_listen.c:5373 MM-3-INVALID_PKT_RECVD：收到来自10.40.220.18的无效数据包。源成员：0.0.0.0。源成员未知……为什么？

在无线访客接入设置中，客户端不会从DHCP服务器接收IP地址。内部控制器上显示Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP droging REPLY from Export-Foreign STA错误消息。为什么？

如果访客流量通过隧道传输至非安全网络区域，那么访客客户端从哪里获取 IP 地址？

Cisco 无线局域网控制器是否支持用于访客身份验证的 Web 门户？

如何自定义 Web 门户？

如何管理访客凭证？

除无线控制系统(WCS)或NCS外，思科无线局域网控制器中是否还提供接待大使功能？

能否使用外部身份验证、授权和记帐 (AAA) 服务器对访客进行身份验证？

当访客登录时将发生什么情况？

能否跳过访客用户身份验证并只显示网页免责声明选项？

远程控制器和访客锚点控制器是否需要位于相同的移动组中？

如果有多个访客 SSID，能否将每个 WLAN (SSID) 定向到唯一的网页门户？

WLC版本7.0 WebAuth on Mac Filter Failure中的新设置有什么功能？

如果为代理服务器配置了浏览器，客户端是否正常运行？

有没有无线访客接入的部署指南？

有没有有线和无线访客接入的设计指南？

相关信息

简介

本文档提供有关 Cisco 统一无线网络中的无线访客接入功能的最常见问题 (FAQ) 的信息。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

什么是连接非安全网络区域的 Ethernet over IP (EoIP) 隧道？

Cisco 建议为访客流量使用一个专用控制器。此控制器称为访客锚点控制器。

访客锚点控制器通常位于非安全网络区域中，通常也称为隔离区 (DMZ)。流量所来自的其他内部 WLAN 控制器位于企业 LAN 中。EoIP 隧道是在内部 WLAN 控制器与访客锚点控制器之间建立的，旨在确保将访客流量与企业数据流量进行路径隔离。路径隔离是访客接入的一种重要安全管理功能。它确保能够单独设置安全和服务质量 (QoS) 策略，并且能够针对访客流量和公司或内部流量进行区分。

Cisco 统一无线网络架构的一项重要功能就是能够使用 EoIP 隧道将一个或多个所配置的 WLAN（即 SSID）映射到网络中的特定访客锚点控制器。所有流量（包括往返映射WLAN的流量）都经过在远程控制器和访客锚点控制器之间建立的静态EoIP隧道。

使用这种技术，可以透明地将所有关联的访客流量通过企业网络传输至非安全区域中的访客锚点控制器。

如何选择正确的控制器以部署为访客锚点控制器？

访客锚点控制器的选择是由活动的访客客户端会话数和/或控制器上的上行链路接口容量定义的访客流量的函数。

每个访客锚点控制器的总吞吐量和客户端限制如下所示：

- Cisco 2504无线局域网控制器 — 4 * 1 Gbps接口和1000个访客客户端
- 思科5508无线局域网控制器(WLC)- 8 Gbps和7,000个访客客户端
- Cisco Catalyst 6500系列无线服务模块(WiSM-2)- 20 Gbps和15,000客户端
- 思科8500无线局域网控制器(WLC)- 10 Gbps和64,000个客户端

注:Cisco 7500 WLC不能配置为访客锚点控制器。有关支持访客锚点功能的WLC列表，请参阅哪些控制器可用于支持非安全网络区域中的访客访问？。

每个控制器的数据库最多可存储2048个访客用户名和密码。因此，如果活动访客凭证的总数超出此数值，将需要多个控制器。或者，访客凭证也可以存储在外部 RADIUS 服务器上。

网络中的接入点数并不影响访客锚点控制器的选择。

在访客锚点控制器上可以有多少个 Ethernet over IP (EoIP) 隧道终端？

一个访客锚点控制器最多可以有 71 个来自内部 WLAN 控制器的 Ethernet over IP (EoIP) 隧道终端

。除WLC-2504外，所有型号的思科无线局域网控制器的容量都相同。2504控制器最多可端接15个EoIP隧道。如果需要附加隧道，可以配置多个访客锚点控制器。

EoIP 隧道按每个 WLAN 控制器计数，与每个 EoIP 中隧道连接的 WLAN 数或安全集标识符 (SSID) 数无关。

在访客锚点控制器与支持带有访客客户端关联的接入点的每个内部控制器之间配置一个 EoIP 隧道。

能否在运行不同软件版本的控制器之间创建 Ethernet over IP (EoIP) 隧道？

并非所有无线局域网控制器软件版本都支持此行为。这种情况下，远程控制器和锚点控制器应运行相同版本的 WLC 软件。但是，最近的软件版本确实支持远程控制器和锚点控制器具有不同的版本。

下表列出了可以创建 Ethernet over IP (EoIP) 隧道的无线局域网控制器软件版本。

EoIP Tunnel Combination Between WLC Versions

Anchor / Remote	4.1.185	4.2.X	5.0.X	5.1.X	5.2.X	6.0.X	7.0.X
4.1.185	✓						
4.2.X		✓		✓	✓	✓	✓
5.0.X			✓	✓	✓	✓	✓
5.1.X		✓	✓	✓	✓	✓	✓
6.0.X		✓	✓	✓	✓	✓	✓
7.0.X		✓	✓	✓	✓	✓	✓

4.2.x = 4.2.61.0, 4.2.99.0, 4.2.112.0, 4.2.130.0, 4.2.173.0, 4.2.176.0, 4.2.205.0, 4.2.207.0, 4.2.209.0
5.0.x = 5.0.148.0, 5.0.148.2
5.1.x = 5.1.151.0, 5.1.163.0
5.2.x = 5.2.157.0, 5.2.178.0, 5.2.193.0
6.0.X = 6.0.182.0, 6.0.188.0, 6.0.196.0, 6.0.199.0, 6.0.199.4
7.0.X = 7.0.98.0, 7.0.116.0 , 7.0.220.0

Cisco 2100/2500 系列无线局域网控制器能否用作非安全网络区域

中的访客锚点控制器？

可以，从Cisco Unified Wireless Network软件版本7.4开始，Cisco 2500系列无线LAN控制器可以终止（最多15个EoIP隧道）防火墙外的访客流量。Cisco 2000 系列无线局域网控制器只能作为访客隧道的源头。

适用于集成多业务路由器的思科无线局域网控制器模块（WLCM或WLCM2）能否用作非安全网络区域中的访客锚点控制器？

否，WLCM或WLCM2无法终止访客隧道。WLCM 只能作为访客隧道的源头。

哪些控制器可用来支持非安全网络区域中的访客接入？

在具有4.0版或更高版本软件映像的思科无线局域网控制器平台中，支持访客隧道锚点功能，包括EoIP隧道终端、Web身份验证和访客客户端访问控制：

- Cisco Catalyst 6500系列无线服务模块(WiSM2)
- 思科WiSM-2系列无线局域网控制器
- Cisco Catalyst 3750G集成无线局域网控制器
- Cisco 5508 Series Wireless LAN Controller
- Cisco 2500系列无线局域网控制器（软件版本7.4中引入的支持）

如果在防火墙之外使用访客锚点控制器，需要为访客接入打开哪些防火墙端口？

在访客锚点控制器与远程控制器之间的任何防火墙上，需要打开以下端口：

- 传统移动性：用于用户数据流量的IP协议97,UDP端口16666
- 新移动性：UDP端口16666和16667

对于可选管理，需要打开以下防火墙端口：

- SSH/Telnet - TCP端口22/23
- TFTP - UDP端口69
- NTP - UDP端口123
- SNMP - UDP端口161（获取和设置）和162（陷阱）
- HTTPS/HTTP - TCP端口443/80

- 系统日志 — TCP端口514
- RADIUS身份验证/帐户UDP端口1812和1813

在配置了网络地址转换 (NAT) 的情况下访客流量能否通过防火墙？

必须为通过防火墙的 EoIP 隧道使用一对一 NAT。

在“锚点 - 外部 WLC”方案中，哪个 WLC 将发送 RADIUS 记帐？

在此方案中，始终由锚点 WLC 进行身份验证。因此，RADIUS 记帐将由锚点 WLC 发送。

注意：在集中式Web身份验证(CWA)和/或授权更改(CoA)部署中，应在锚点上禁用RADIUS记帐，并且仅在外部WLC上使用。

内部控制器与锚点控制器之间的访客隧道出现故障。我在WLC中看到以下日志： `mm_listen.c:5373 MM-3-INVALID_PKT_RECVD`：收到来自10.40.220.18的无效数据包。源成员：0.0.0.0。源成员未知。.为什么？

请在 WLAN 页面上的 WLC GUI 中检查隧道状态。单击 WLAN 旁边的下拉框并选择 Mobility Anchors，其中包含控制和数据路径的状态。该错误消息是由以下原因之一造成的：

1. 锚点和内部控制器的代码版本不同。请确保它们运行相同的代码版本。
2. 移动锚点配置中的配置错误。请检查以确保 DMZ 本身配置为移动锚点并且内部 WLC 的 DMZ WLC 配置与该移动锚点相同。有关如何配置移动锚点的详细信息，请参阅Cisco无线LAN控制器配置指南7.0版的配置自动锚点移动部分。这会导致访客用户无法传递流量。

在无线访客接入设置中，客户端不会从DHCP服务器接收IP地址。Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP droging REPLY from Export-Foreign STA错误消息出现在内部控制器上。为什么？

在无线访客接入设置中，访客锚点控制器和内部控制器中的DHCP代理设置必须匹配。否则，来自客户端的DHCP请求将被丢弃，您将在内部控制器上看到以下错误消息：

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

使用以下命令更改WLC上的dhcp代理设置：

```
<#root>

(Cisco Controller) >

config dhcp proxy ?


enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

在两台控制器上使用show dhcp proxy命令，以验证两台控制器是否具有相同的DHCP代理设置。

```
<#root>

(Cisco Controller) >

show dhcp proxy


DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

如果访客流量通过隧道传输至非安全网络区域，那么访客客户端从哪里获取 IP 地址？

访客流量是在第 3 层通过 EoIP 在企业内传输的。因此，动态主机配置协议 (DHCP) 服务的第一点可以在访客锚点控制器上本地实现，或者，访客锚点控制器可以将 DHCP 请求中继至外部服务器。这也是处理域名系统 (DNS) 地址解析的方法。

Cisco 无线局域网控制器是否支持用于访客身份验证的 Web 门户？

Cisco 无线局域网控制器软件版本 3.2 或更高版本提供了一个内置 Web 门户，可捕获用于身份验证的访客凭证并提供简单的标记功能，还能够显示免责声明和可接受的使用策略信息。

如何自定义 Web 门户？

有关如何自定义 Web 门户的信息，请参阅选择 Web 身份验证登录页。

如何管理访客凭证？

可以使用思科无线控制系统(WCS)版本7.0和/或网络控制系统(NCS)版本1.0集中创建和管理访客凭

证。网络管理员可以在 WCS 中建立有限权限的管理帐户，允许进行“接待大使”访问以创建访客凭证。在WCS或NCS中，拥有接待大使帐户的人员能够为充当访客锚点控制器的控制器创建、分配、监控和删除访客凭证。

接待大使可以输入访客用户名（或 ID）和口令，也可以自动生成凭证。还有一个全局配置参数，允许为所有访客使用一个用户名和口令，或者为每个访客使用唯一的用户名和口令。

要在WCS上配置接待大使帐户，请参阅Cisco无线控制系统配置指南7.0版的创建访客用户帐户部分。

除无线控制系统(WCS)或NCS外，思科无线局域网控制器中是否还提供接待大使功能？

Yes.如果未部署WCS或NCS，网络管理员可以在访客锚点控制器上建立接待大使帐户。使用接待大使帐户登录访客锚点控制器的用户只能访问访客用户管理功能。

如果有多个访客锚点控制器，则必须使用WCS或NCS在多个访客锚点控制器上同时配置用户名。

有关如何使用无线LAN控制器创建接待大使帐户的信息，请参阅Cisco无线LAN控制器配置指南7.0版的创建接待大使帐户部分。

能否使用外部身份验证、授权和记帐 (AAA) 服务器对访客进行身份验证？

Yes.可以将访客身份验证请求中继至外部 RADIUS 服务器。

当访客登录时将发生什么情况？

当无线访客通过 Web 门户登录时，访客锚点控制器将通过执行以下步骤处理身份验证：

1. 访客锚点控制器将检查其本地数据库中的用户名和口令，如果存在，则允许访问。
2. 如果访客锚点控制器上不存在本地用户凭证，访客锚点控制器将检查 WLAN 配置设置以查看是否为访客 WLAN 配置了外部 RADIUS 服务器。如果进行了配置，控制器将创建一个包含用户名和口令的 RADIUS 接入请求包并将其转发给所选的 RADIUS 服务器进行身份验证。
3. 如果没有为 WLAN 配置特定 RADIUS 服务器，控制器将检查其全局 RADIUS 服务器配置设置。任何配置了验证“网络用户”选项的外部RADIUS服务器都将使用访客用户的凭证进行查询。否则，如果未选择服务器“网络用户”，且用户尚未通过步骤1或2进行身份验证，则身份验证将失败。

能否跳过访客用户身份验证并只显示网页免责声明选项？

Yes.无线访客接入的另一个配置选项是绕过用户身份验证并允许开放式接入。但是，在允许接入之前可能需要为访客提供可接受的使用策略和免责声明页。为此，可以为 Web 策略通过配置访客

WLAN。在此方案中，访客用户将重定向至包含免责声明信息的 Web 门户页面。为了标识访客用户的身份，通过模式还有一个选项，可使用户在连接之前输入电子邮件地址。

远程控制器和访客锚点控制器是否需要位于相同的移动组中？

否。访客锚点控制器和远程控制器可以位于不同的移动组中。

如果有多个访客 SSID，能否将每个 WLAN (SSID) 定向到唯一的网页门户？

Yes.所有访客流量（位于一个或多个 WLAN 中）都将重定向到一个网页。在 WLC 版本 4.2 或更高版本中，可以将每个 WLAN 定向到唯一的 Web 门户页面。请参阅Cisco无线LAN控制器配置指南7.0版的分配每个WLAN的登录、登录失败和注销页部分。

WLC版本7.0 WebAuth on Mac Filter Failure中的新设置有什么功能？

如果WLAN同时配置了第2层(mac-filter)和第3层安全(webauth-on-macfilter-failure)，则当其中任一客户端通过时，客户端将转到RUN状态。如果第2层安全(mac-filter)失败，客户端将移至第3层安全(webauth-on-macfilter-failure)。

如果为代理服务器配置了浏览器，客户端是否正常运行？

在版本7.0之前，在浏览器中配置代理服务器时，客户端无法建立TCP连接。版本7.0之后，添加此WebAuth代理服务器支持，并且可以在控制器上配置代理服务器IP地址和端口。

有没有无线访客接入的部署指南？

下面是指向该部署指南的链接：

部署指南：使用思科无线局域网控制器的思科访客接入

有没有有线和无线访客接入的设计指南？

以下是设计指南的链接：

- Cisco 统一无线访客接入服务
- 使用 Cisco WLAN 控制器的有线访客接入配置示例

相关信息

- 使用 Cisco WLAN 控制器的有线访客接入配置示例
- 部署指南：使用思科无线局域网控制器的思科访客接入，版本4.1

- 技术支持和文档 - Cisco Systems

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）。