

# 接入点ACL过滤器配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[使用标准访问列表的过滤器](#)

[使用扩展访问列表的过滤器](#)

[使用基于 MAC 的 ACL 的过滤器](#)

[使用基于时间的 ACL 的过滤器](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文说明如何使用命令行界面 (CLI) 在 Cisco Aironet 接入点 (AP) 上配置基于访问控制表 (ACL) 的过滤器。

## 先决条件

### 要求

Cisco 建议您具有以下主题的基础知识：

- 使用 Aironet AP 和 Aironet 802.11 a/b/g 客户端适配器配置无线连接
- ACL

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS® 软件版本 12.3(7)JA1 的 Aironet 1200 系列 AP
- Aironet 802.11a/b/g 客户端适配器
- Aironet Desktop Utility (ADU) 软件版本 2.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

您能使用 AP 上的过滤器执行以下任务：

- 限制对无线 LAN (WLAN) 网络的访问
- 提供附加的无线安全层

您能使用不同种类的过滤器基于以下条件过滤数据流：

- 特定协议
- 客户端设备的 MAC 地址
- 客户端设备的 IP 地址

您还能使过滤器限制来自有线 LAN 上的用户的数据流。IP 地址和 MAC 地址过滤器可允许或禁止转发特定 IP 或 MAC 地址接收或发送的单播和组播数据包。

基于协议的过滤器提供一种更精细的方式来限制通过 AP 的以太网和无线电接口对特定协议的访问。您能使用以下方法之一在 AP 上配置过滤器：

- Web GUI
- CLI

本文档说明如何通过 CLI 使用 ACL 配置过滤器。有关如何通过 GUI 配置过滤器的信息，请参阅 [配置过滤器](#)。

您能使用 CLI 在 AP 上配置以下类型的基于 ACL 的过滤器：

- 使用标准 ACL 的过滤器
- 使用扩展 ACL 的过滤器
- 使用 MAC 地址 ACL 的过滤器

**注意：**ACL 上允许的条目数量受 AP 的 CPU 限制。如果有大量条目要添加到 ACL，例如，当过滤客户端的 MAC 地址列表时，请使用网络中能够执行此任务的交换机。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

有关本文档所用命令的详细信息，请使用 [命令查找工具 \(仅限注册用户\)](#)。

本文档中的所有配置均假设无线连接已经建立。本文档仅着重介绍如何使用 CLI 配置过滤器。如果您没有基本无线连接，请参阅 [基本无线 LAN 连接配置示例](#)。

### 使用标准访问列表的过滤器

您能使用标准 ACL 根据客户端的 IP 地址允许或禁止客户端设备进入 WLAN 网络。标准 ACL 通过将 IP 数据包源地址与 ACL 中配置的地址进行比较来控制数据流。此种 ACL 可以称为基于源 IP 地址的 ACL。

标准 ACL 的命令语法格式为 **access-list access-list-number {permit | deny} {host ip-address | source-ip source-wildcard |任意}**。

在Cisco IOS®软件版本12.3(7)JA中，ACL编号可以是1到99之间的任意数字。标准ACL也可以使用1300到1999的扩展范围。这些附加的编号是扩充的IP ACL。

当标准ACL配置成拒绝对客户端的访问时，客户端仍然与AP关联。然而，在AP和客户端之间没有数据通信。

此示例说明配置成从无线接口（radio0接口）过滤客户端IP地址10.0.0.2的标准ACL。AP的IP地址为10.0.0.1。

完成后，IP地址为10.0.0.2的客户端不能通过WLAN网络发送或接收数据，即使客户端已与AP关联也是如此。

要通过CLI创建标准ACL，请完成以下步骤：

1. 通过CLI登录到AP。要通过以太网接口或无线接口访问ACL，请使用控制台端口或使用Telnet。

2. 在AP上进入全局配置模式：

```
AP#configure terminal
```

3. 发出以下命令，创建标准ACL：

```
AP<config>#access-list 25 deny host 10.0.0.2
```

```
!--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2.
```

```
AP<config>#access-list 25 permit any
```

```
!--- Allow all other hosts to access the network.
```

4. 发出以下命令，将此ACL应用到无线电接口：

```
AP<config>#interface Dot11Radio 0
```

```
AP<config-if>#ip access-group 25 in
```

```
!--- Apply the standard ACL to the radio interface 0.
```

您也可以创建标准命名ACL (NACL)。NACL使用名称而不是编号来定义ACL。

```
AP#configure terminal
```

```
AP<config>#ip access-list standard name
```

```
AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

发出以下命令，使用标准NACL拒绝主机10.0.0.2对WLAN网络的访问：

```
AP#configure terminal
```

```
AP<config>#ip access-list standard TEST
```

```
!--- Create a standard NACL TEST.
```

```
AP<config-std-nacl>#deny host 10.0.0.2
```

```
!--- Disallow the client with IP address 10.0.0.2 !--- access to the network. AP<config-std-
```

```
nacl>#permit any
```

```
!--- Allow all other hosts to access the network. AP<config-std-nacl>#exit
```

```
!--- Exit to global configuration mode. AP<config>#interface Dot11Radio 0
```

```
!--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in
```

```
!--- Apply the standard NACL to the radio interface.
```

## 使用扩展访问列表的过滤器

扩展ACL通过将IP数据包的源地址和目标地址与ACL中配置的地址进行比较来控制数据流。扩展

ACL 还提供了一种根据特定协议过滤数据流的方法。这在 WLAN 网络上实施过滤器提供了更精细的控制。

扩展 ACL 允许某客户端访问网络上的某些资源，但不能访问其他资源。例如，您能使用一种过滤器，允许到客户端的 DHCP 和 Telnet 数据流，同时限制所有其他数据流。

以下是扩展 ACL 的命令语法：

**注意：**由于空间考虑，此命令被换行为四行。

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name]
```

在 Cisco IOS 软件版本 12.3(7)JA 中，扩展 ACL 可以使用 100 到 199 范围内的数字。扩展 ACL 也可以使用 2000 到 2699 范围内的数字。这是扩展 ACL 的扩展范围。

**注意：**单个 ACL 条目末尾的 log 关键字显示：

- ACL 编号和名称
- 已允许还是拒绝该数据包
- 端口特定的信息

扩展 ACL 也能使用名称而不是编号。以下是创建扩展 NACL 的语法：

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-
name]
```

此配置示例使用扩展 NACL。要求是，扩展 NACL 必须允许对客户端的 Telnet 访问。您必须限制 WLAN 网络上的所有其他协议。并且，客户端使用 DHCP 以获得 IP 地址。您必须创建以下这种扩展 ACL：

- 允许 DHCP 和 Telnet 流量
- 拒绝所有其他数据流类型

一旦将此扩展 ACL 应用于无线电接口，客户端将与 AP 关联并且从 DHCP 服务器获得 IP 地址。客户端也能使用 Telnet。所有其他数据流类型被拒绝。

要在 AP 上创建扩展 ACL，请完成以下步骤：

1. 通过 CLI 登录到 AP。使用控制台端口或 Telnet 以通过以太网接口或无线接口访问 ACL。
2. 在 AP 上进入全局配置模式：

```
AP#configure terminal
```

3. 发出以下命令，创建扩展 ACL：

```
AP<config>#ip access-list extended Allow_DHCP_Telnet
!--- Create an extended ACL Allow_DHCP_Telnet.
```

```
AP<config-extd-nacl>#permit tcp any any eq telnet
!--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc
!--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps
```

```
!--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any
!--- Deny all other traffic types. AP<config-extd-nacl>#exit
!--- Return to global configuration mode.
```

#### 4. 发出以下命令，将该 ACL 应用到无线电接口：

```
AP<config>#interface Dot11Radio 0
AP<config-if>#ip access-group Allow_DHCP_Telnet in
!--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.
```

## 使用基于 MAC 的 ACL 的过滤器

您可以使用基于 MAC 地址的过滤器以便根据硬编码 MAC 地址过滤客户端设备。当通过基于 MAC 的过滤器拒绝客户端访问时，该客户端不能与 AP 产生关联。MAC 地址过滤器可允许或禁止转发特定 MAC 地址接收或发送的单播和组播数据包。

这是在 AP 上创建基于 MAC 地址的 ACL 的命令语法：

**注意：**由于空间考虑，此命令已换行为两行。

```
access-list access-list-number {permit | deny} 48-bit-hardware-address 48-bit-hardware-address-mask
```

在 Cisco IOS 软件版本 12.3(7)JA 中，MAC 地址 ACL 能使用 700 到 799 范围内的数字作为 ACL 编号。它们也可以使用 1100 到 1199 扩展范围内的编号。

此示例说明如何通过 CLI 配置一个基于 MAC 的过滤器，以过滤 MAC 地址为 **0040.96a5.b5d4** 的客户端：

1. 通过 CLI 登录到 AP。使用控制台端口或 Telnet 以通过以太网接口或无线接口访问 ACL。
2. 在 AP CLI 上进入全局配置模式：

```
AP#configure terminal
```

3. 创建 MAC 地址 ACL 700。此 ACL 不允许客户端 0040.96a5.b5d4 与 AP 关联。

```
access-list 700 deny 0040.96a5.b5d4 0000.0000.0000
!--- This ACL denies all traffic to and from !--- the client with MAC address
0040.96a5.b5d4.
```

4. 发出此命令，将此基于 MAC 的 ACL 应用于无线电接口：

```
dot11 association mac-list 700
```

```
!--- Apply the MAC-based ACL.
```

在 AP 上配置此过滤器之后，具有此 MAC 地址的客户端（它以前与该 AP 关联）将取消关联。AP 控制台传送以下消息：

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

## 使用基于时间的 ACL 的过滤器

基于时间的 ACL 是可以在特定时期启用或禁用的 ACL。通过此功能，便能可靠和灵活地定义允许

或拒绝某些种类数据流的访问控制策略。

以下示例说明如何通过 CLI 配置基于时间的 ACL，其中，在工作日的工作时间允许从网络内部到外部的 Telnet 连接：

**注意：**基于时间的ACL可以根据您的要求在快速以太网端口或Aironet AP的无线电端口上定义。但从不应将其用于网桥组虚拟接口 (BVI)。

1. 通过 CLI 登录到 AP。使用控制台端口或 Telnet 以通过以太网接口或无线接口访问 ACL。
2. 在 AP CLI 上进入全局配置模式：

```
AP#configure terminal
```

3. 创建时间范围。为此，请在全局配置模式下发出以下命令：

```
AP<config>#time-range Test
```

```
!--- Create a time-range with name Test. AP(config-time-range)# periodic weekdays 7:00 to 19:00
```

```
!--- Allows access to users during weekdays from 7:00 to 19:00 hrs.
```

4. 创建 ACL 101：

```
AP<config># ip access-list extended 101
```

```
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test
```

```
!--- This ACL permits Telnet traffic to and from !--- the network for the specified time-range Test.
```

此 ACL 在工作日允许到 AP 的 Telnet 会话。

5. 发出以下命令，将此基于时间的 ACL 应用于以太网接口：

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
```

```
!--- Apply the time-based ACL.
```

## 验证

当前没有可用于此配置的验证过程。

## 故障排除

使用本部分可排除配置故障。

完成以下步骤，从接口删除 ACL：

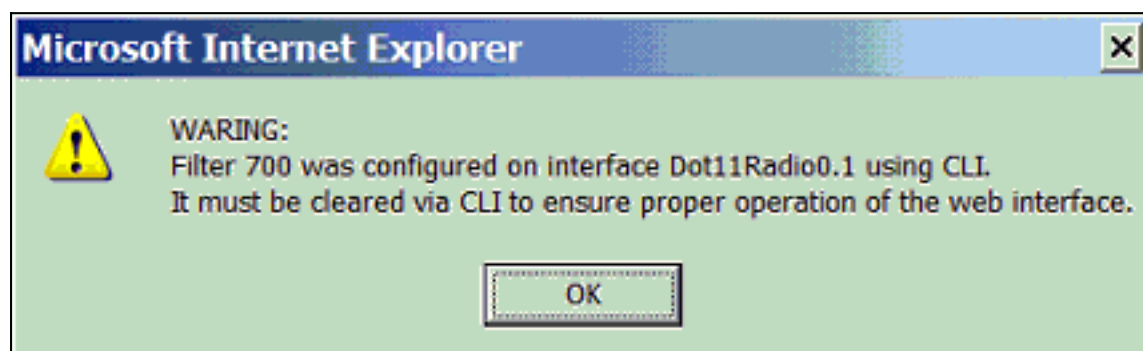
1. 进入接口配置模式。
2. 在 `ip access-group` 命令前面输入 `no`，如以下示例所示：

```
interface interface
no ip access-group {access-list-name | access-list-number} {in | out}
```

您也可以使用 `show access-list name | number` 命令，以排除配置故障。`show ip access-list` 命令可提供数据包计数，它显示匹配的 ACL 条目。

避免同时使用 CLI 和 Web 浏览器接口来配置无线设备。如果使用 CLI 配置无线设备，Web 浏览器界面可能会显示配置的不准确的解释。然而，不准确并不意味着无线设备的配置是不正确的。例

如，如果使用 CLI 配置 ACL，Web 浏览器界面可能显示以下消息：



如果看到此消息，请使用 CLI 删除 ACL 并使用 Web 浏览器界面重新配置它们。

## [相关信息](#)

- [配置过滤器](#)
- [无线支持页](#)
- [技术支持和文档 - Cisco Systems](#)