

# 捆绑在一台被管理的交换机的入口或出口访问控制表(ACL)

## 客观

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可以适用不仅于入口，而且于输出接口。入口(入站)和出口(outbound) ACL的目的将指定从在网络的设备允许或的网络类型数据流。此功能允许管理员过滤在网路的数据流到互联网，或者到组织防火墙。

此条款提供指令关于怎样配置和捆绑在您的交换机的入口或出口ACL。

## 可适用的设备

- Sx350系列
- SG350X系列
- Sx550X系列

## 软件版本

- 2.2.0.66

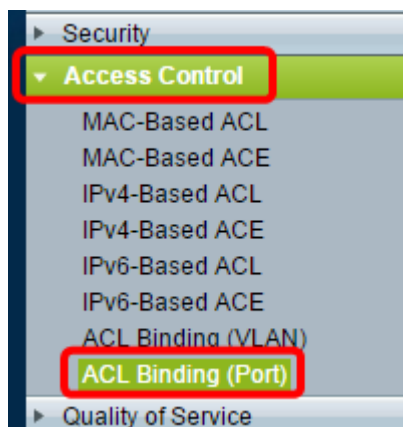
## 配置入口或出口ACL

**重要信息：**保证在您的交换机配置的您有ACL和访问控制项(ACE)。要配置IPv4-based ACL和ACE，为指令[请点击此处](#)。对于IPv6-based，[请点击此处](#)。要配置基于MAC的ACL和ACE，[请点击此处](#)。

### 配置在接口的入口ACL

步骤1.基于Web的工具的洛金然后选择访问控制> ACL捆绑(端口)。

Note:在此方案中，使用SG350-28MP交换机。



Step 2.在接口旁边检查复选框您要适用ACL对，然后点击编辑。

**Note:**在本例中，ACL将适用于GE5接口。

ACL Binding Table					
Filter: <i>Interface Type</i> equals to <input type="text" value="Port"/> <input type="button" value="Go"/>					
<input type="checkbox"/>	Entry No.	Interface	Input ACL		
			MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input checked="" type="checkbox"/>	5	GE5			
<input type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	GE11			
<input type="checkbox"/>	12	GE12			
<input type="checkbox"/>	13	GE13			
<input type="checkbox"/>	14	GE14			
<input type="checkbox"/>	15	GE15			
<input type="checkbox"/>	16	GE16			
<input type="checkbox"/>	17	GE17			
<input type="checkbox"/>	18	GE18			
<input type="checkbox"/>	19	GE19			
<input type="checkbox"/>	20	GE20			
<input type="checkbox"/>	21	GE21			
<input type="checkbox"/>	22	GE22			
<input type="checkbox"/>	23	GE23			
<input type="checkbox"/>	24	GE24			
<input type="checkbox"/>	25	GE25			
<input type="checkbox"/>	26	GE26			
<input type="checkbox"/>	27	GE27			
<input type="checkbox"/>	28	GE28			

第3步。要配置在接口的入口ACL，请检查期望输入ACL复选框。

**Note:**在本例中，基于MAC的ACL被选择。

Interface:  Port GE5  LAG 1

**Input ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL: [v]

IPv6-Based ACL: [v]

Default Action:  Deny Any  Permit Any

**Output ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL: [v]

IPv6-Based ACL: [v]

Default Action:  Deny Any  Permit Any

Apply Close

**Note:**如果要捆绑IPv4或IPv6-Based ACL，请点击相应地选择。

步骤4.从对应的下拉列表选择ACL。

**Note:**在本例中，预先配置的基于MAC的ACL ACL1被选择。

Interface:  Port GE5  LAG 1

**Input ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL: [v]

IPv6-Based ACL: [v]

Default Action:  Deny Any  Permit Any

**Output ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL: [v]

IPv6-Based ACL: [v]

Default Action:  Deny Any  Permit Any

Apply Close

步骤5.点击默认动作单选按钮。

Interface:  Port GE5  LAG 1

**Input ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL: [v]

IPv6-Based ACL: [v]

Default Action:  Deny Any  Permit Any

**Output ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL: [v]

IPv6-Based ACL: [v]

Default Action:  Deny Any  Permit Any

选项是：

- 拒绝其中任一——交换机丢弃不满足ACL的必需的标准的信息包。
- 允许其中任一——交换机转发满足ACL的必需的标准的信息包。

步骤6. 点击**适用**保存对运行配置文件的更改然后点击**Close**。

第7.步。ACL绑定表应该显示在选择的接口的被配置的ACL。点击“**Save**”更新启动配置文件。

cisco Language

P 28-Port Gigabit PoE Managed Switch

**ACL Binding Table**

Filter: Interface Type equals to Port [v] Go

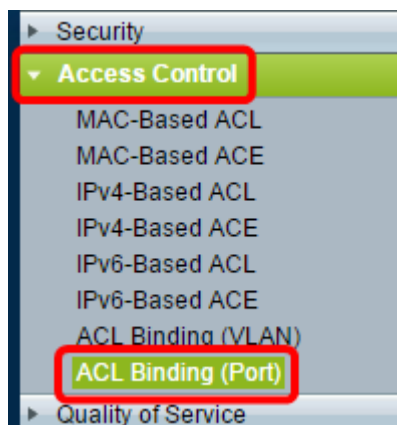
	Entry No.	Interface	Input ACL				Output ACL
			MAC ACL	IPv4 ACL	IPv6 ACL	Default Action	MAC ACL
<input type="checkbox"/>	1	GE1					
<input type="checkbox"/>	2	GE2					
<input type="checkbox"/>	3	GE3					
<input type="checkbox"/>	4	GE4					
<input checked="" type="checkbox"/>	5	GE5	ACL1			Deny Any	
<input type="checkbox"/>	6	GE6					
<input type="checkbox"/>	7	GE7					
<input type="checkbox"/>	8	GE8					

## 配置在接口的出口ACL

**重要信息：**在继续进行步骤前，请保证您已经创建了基于MAC的ACL和访问控制项(ACE)在您的交换机。对于详细指令，请点击[此处](#)。

**Step 1.**在基于Web的工具中，请选择访问控制> ACL捆绑(端口)。

**Note:**在此方案中，使用SG350-28MP交换机。



**Step 2.**在接口旁边检查复选框您要适用ACL对，然后点击编辑。

**Note:**在本例中，GE6被选择。

**ACL Binding Table**

Filter: *Interface Type* equals to

<input type="checkbox"/>	Entry No.	Interface	Input ACL		
			MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input type="checkbox"/>	5	GE5			
<input checked="" type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	GE11			
<input type="checkbox"/>	12	GE12			
<input type="checkbox"/>	13	GE13			
<input type="checkbox"/>	14	GE14			
<input type="checkbox"/>	15	GE15			
<input type="checkbox"/>	16	GE16			
<input type="checkbox"/>	17	GE17			
<input type="checkbox"/>	18	GE18			
<input type="checkbox"/>	19	GE19			
<input type="checkbox"/>	20	GE20			
<input type="checkbox"/>	21	GE21			
<input type="checkbox"/>	22	GE22			
<input type="checkbox"/>	23	GE23			
<input type="checkbox"/>	24	GE24			
<input type="checkbox"/>	25	GE25			
<input type="checkbox"/>	26	GE26			
<input type="checkbox"/>	27	GE27			
<input type="checkbox"/>	28	GE28			

第3步。要配置在接口的入口ACL，请检查期望输出ACL复选框。

**Note:**在本例中，基于MAC的ACL被选择。

Interface:  Port GE5  LAG 1

**Input ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL:

IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

**Output ACL**

MAC-Based ACL: ACL2

IPv4-Based ACL:

IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

Apply Close

**Note:**如果要捆绑IPv4或IPv6-Based ACL，请点击相应地选择。

步骤4.从基于MAC的ACL下拉列表选择ACL。

**Note:**在本例中，预先配置的基于MAC的ACL ACL2被选择。

Interface:  Port GE6  LAG 1

**Input ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL:

Default Action:  Deny Any  Permit Any

**Output ACL**

MAC-Based ACL: ACL2

IPv4-Based ACL:

Default Action:  Deny Any  Permit Any

Apply Close

步骤5.点击默认动作单选按钮。

Interface:  Port GE6  LAG 1

**Input ACL**

MAC-Based ACL: ACL1

IPv4-Based ACL:

Default Action:  Deny Any  
 Permit Any

**Output ACL**

MAC-Based ACL: ACL2

IPv4-Based ACL:

Default Action:  Deny Any  
 Permit Any

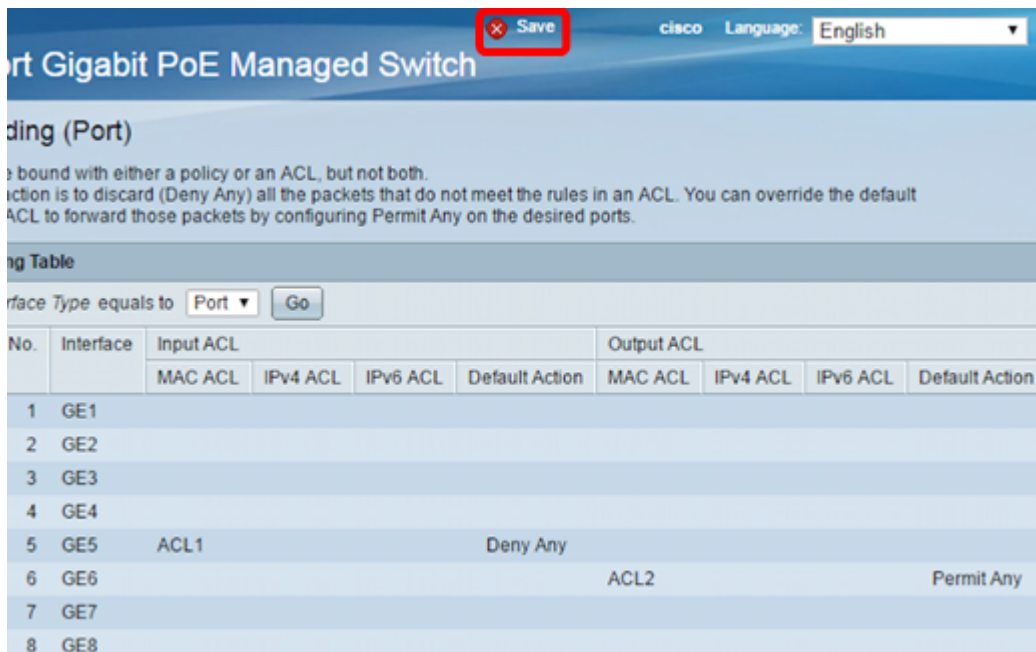
Apply Close

选项是：

- 拒绝其中任一——交换机丢弃不满足ACL的必需的标准的信息包。
- 允许其中任一——交换机转发满足ACL的必需的标准的信息包。

步骤6. 点击**适用**保存对运行配置文件的更改然后点击**Close**。

第7.步。ACL绑定表应该显示在选择的接口的被配置的ACL。点击“**Save**”更新启动配置文件。



Port Gigabit PoE Managed Switch

Save

Binding (Port)

bound with either a policy or an ACL, but not both.  
Action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. You can override the default ACL to forward those packets by configuring Permit Any on the desired ports.

Binding Table

Interface Type equals to Port Go

No.	Interface	Input ACL				Output ACL			
		MAC ACL	IPv4 ACL	IPv6 ACL	Default Action	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
1	GE1								
2	GE2								
3	GE3								
4	GE4								
5	GE5	ACL1			Deny Any				
6	GE6					ACL2			Permit Any
7	GE7								
8	GE8								

**Note:** 如果希望同时配置出口和入口ACL，您可以通过配置输入ACL和输出ACL如此执行区域。

您应该当前配置了在您的交换机接口的出口和入口ACL。