

# 在SG350XG和SG550XG上创建基于MAC的ACL

## 目标

访问控制列表(ACL)是一组规则，可根据数据包是否符合特定条件来创建这些规则以控制数据包。这些条件可以是源地址或目标地址、报头字段以及数据包的其他各种组件。如果数据包与ACL的指定条件匹配，则会丢弃或允许继续。基于MAC的ACL使用规则来分析数据包的第2层报头，以满足这些条件，例如MAC地址、VLAN ID和Ethertype值。通过实施基于MAC的ACL，您可以控制第2层级通过交换机传输的数据包。

本文档旨在向您展示如何在SG350XG和SG550XG交换机上创建和配置基于MAC的ACL。

## 适用设备

- SG350XG
- SG550XG

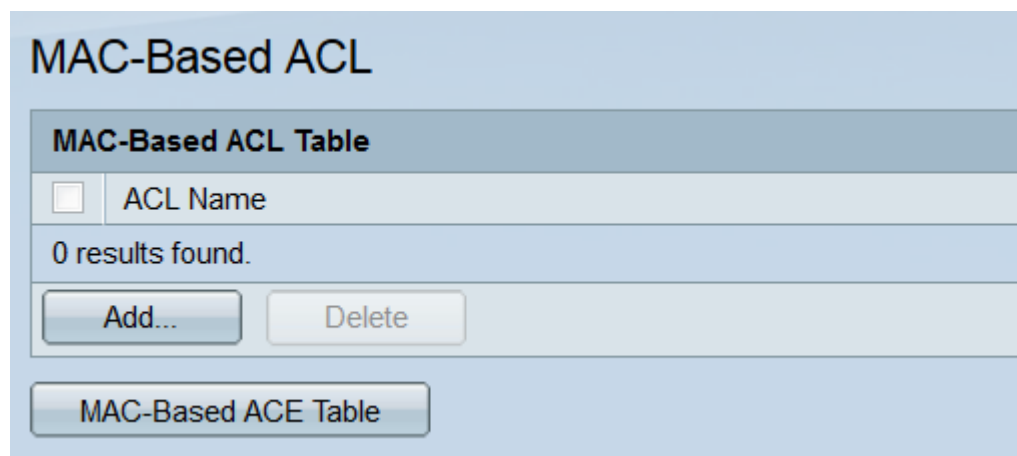
## 软件版本

- v2.0.0.73

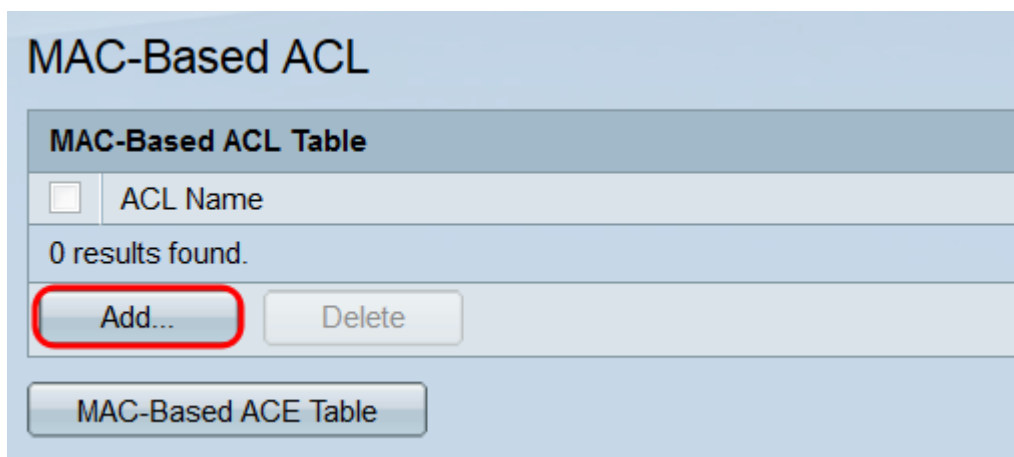
## 配置 基于MAC的ACL

### 创建中 ACL和规则

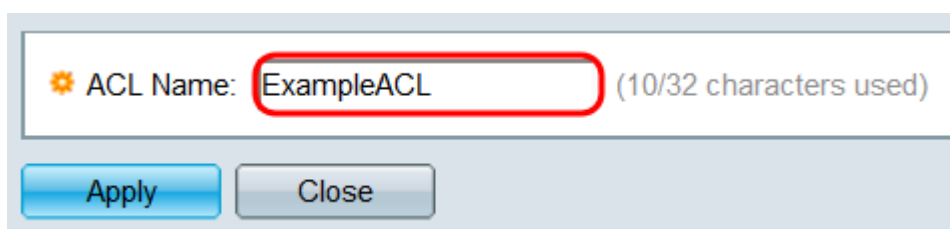
步骤1.登录到Web配置实用程序，然后选择Access Control > MAC-Based ACL。将打开基于MAC的ACL页。



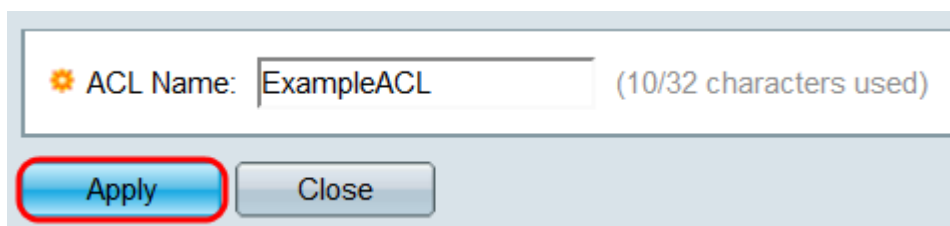
步骤2.基于MAC的ACL表将显示交换机上当前所有基于MAC的ACL。要创建新ACL，请单击Add...按钮。将会打开“添加基于MAC的ACL”窗口。



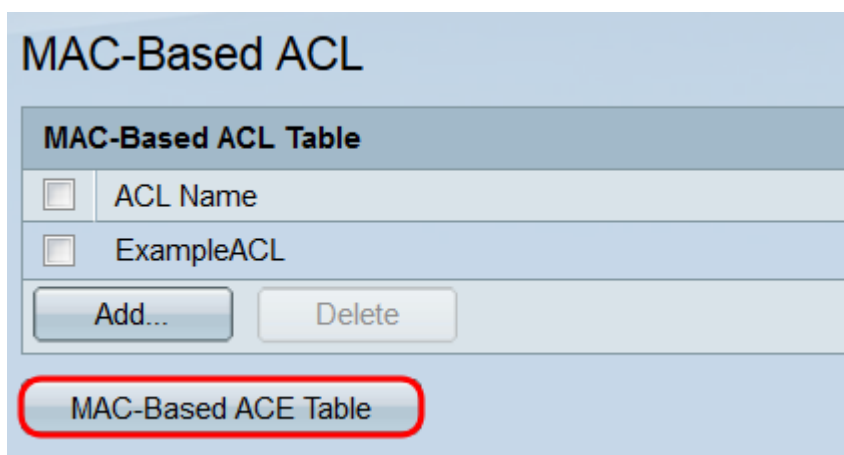
步骤3.在ACL Name字段中，输入新ACL的名称。此名称不会影响ACL的功能，仅用于识别目的。



步骤4.单击“应用”。新ACL将添加到基于MAC的ACL表中。单击Close返回到基于MAC的ACL页面，或通过重复上一步创建另一个ACL。



步骤5.新创建的ACL将为空；即，它不包含任何规则以根据MAC地址阻止或允许数据包。要创建这些规则，必须向ACL添加访问控制条目(ACE)。为此，请单击“基于MAC的ACE表”按钮以转到“基于MAC的ACE”页。



步骤6.在基于MAC的ACE页面上，从基于MAC的ACE表顶部的下拉列表中选择要添加ACE的ACL，然后单击Go。该表显示当前与所选ACL关联的所有ACE。要添加ACE，请单击Add...按钮。将会打开“添加基于MAC的ACE”窗口。

MAC-Based ACE

MAC-Based ACE Table

Filter: ACL Name equals to

Priority	Action	Logging	Destination		Source		VLAN ID	802.1p	802.1p Mask	Ethertype
			MAC Address	Wildcard Mask	MAC Address	Wildcard Mask				
0 results found.										

MAC-Based ACL Table

步骤7. *ACL Name* 字段将显示要添加ACE的ACL的名称。在 *Priority* 字段中，输入ACE的优先级编号。ACE的优先级越高，处理越快。范围为 1 - 2147483647，其中1是最高优先级。

ACL Name:

Priority:  (Range: 1 - 2147483647)

Action:  Permit  
 Deny  
 Shutdown

Logging:  Enable

Time Range:  Enable

Time Range Name:

Destination MAC Address:  Any  
 User Defined

\* Destination MAC Address Value:

\* Destination MAC Wildcard Mask:  (0s for matching, 1s for no matching)

Source MAC Address:  Any  
 User Defined

\* Source MAC Address Value:

\* Source MAC Wildcard Mask:  (0s for matching, 1s for no matching)

VLAN ID:  (Range: 1 - 4094)

802.1p:  Include

\* 802.1p Value:  (Range: 0 - 7)

\* 802.1p Mask:  (Range: 0 - 7)

Ethertype:  (Range: 5DD - FFFF)

步骤8. 在“操作”字段中，选择一个单选按钮以确定在满足ACE的条件时会发生什么情况。

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input type="checkbox"/> Enable	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	<input type="button" value="▼"/> <a href="#">Edit</a>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
VLAN ID:	<input type="text"/> (Range: 1 - 4094)	
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/> (Range: 0 - 7)	
802.1p Mask:	<input type="text"/> (Range: 0 - 7)	
Ethertype:	<input type="text"/> (Range: 5DD - FFFF)	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

选项有：

- 允许 — 转发符合条件的数据包。
- 拒绝 — 丢弃符合条件的数据包。
- 关闭 — 丢弃符合条件的数据包，然后禁用端口。

步骤9.在Logging字段中，选中**Enable**复选框以启用与ACE规则匹配的日志记录ACL流。如果使用基本显示模式，请跳至[步骤12](#)。可通过Web实用程序右上角的下拉列表更改显示模式。

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="Edit"/>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
VLAN ID:	<input type="text"/> (Range: 1 - 4094)	
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/> (Range: 0 - 7)	
802.1p Mask:	<input type="text"/> (Range: 0 - 7)	
Ethertype:	<input type="text"/> (Range: 5DD - FFFF)	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

步骤10.在Time Range字段中，选中**Enable**复选框，使ACE仅在指定时间范围内处于活动状态。如果交换机上未配置现有时间范围，则此字段将不可用。

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="ExampleRange"/> <input type="button" value="Edit"/>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
VLAN ID:	<input type="text"/> (Range: 1 - 4094)	
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/> (Range: 0 - 7)	
802.1p Mask:	<input type="text"/> (Range: 0 - 7)	
Ethertype:	<input type="text"/> (Range: 5DD - FFFF)	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

步骤11.如果您为此ACE启用了时间范围，则“时间范围名称”字段将可用。使用下拉列表选择交换机上已配置的时间范围，以应用到ACE。如果交换机上不存在时间范围，则此字段将不可用；单击“编辑”链接转到“时间范围”页以创建或修改时间范围。有关详细信息，请参阅[“在SG350XG和SG550XG上设置时间范围”一文](#)。

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="ExampleRange"/> <a href="#">Edit</a>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text"/>	(Range: 1 - 4094)
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text"/>	(Range: 0 - 7)
Ethertype:	<input type="text"/>	(Range: 5DD - FFFF)

步骤12. 在Destination MAC Address字段中，选择一个单选按钮，确定将构成匹配的目标MAC地址。选择Any使任何目标地址都匹配，或选择User Defined指定地址或地址范围。

Destination MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text" value="00:12:34:56:78:90"/>	
Destination MAC Wildcard Mask:	<input type="text" value="00:00:00:00:00:00"/>	(0s for matching, 1s for no matching)

如果选择了“用户定义”，请填写以下字段：

- 目标MAC地址值 — 输入目标MAC地址。如果数据包包含此目的地址，ACE会将其视为匹配。
- 目标MAC通配符掩码 — 输入掩码以定义地址范围。将位设置为1将导致忽略MAC地址中的对应位，而0将是匹配位。

**注意：**假设掩码为0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111（这表示匹配位的位置）为0，在有1的位上不匹配）。您需要将1转换为十六进制值，并且每四个零写0。在本示例中，自111 1111 = FF以来，掩码将写成：00:00:00:00:00:FF。

步骤13.在Source MAC Address 字段中，选择一个单选按钮以确定哪些源MAC地址将构成匹配。选择Any以使任何源地址为匹配，或选择User Defined以指定地址或地址范围。

Source MAC Address:  Any  
 User Defined

Source MAC Address Value:

Source MAC Wildcard Mask:  (0s for matching, 1s for no matching)

如果选择了“用户定义”，请填写以下字段：

- 源MAC地址值 — 输入源MAC地址。如果数据包包含此源地址，ACE会将其视为匹配。
- 源MAC通配符掩码 — 输入掩码以定义地址范围。将位设置为1将导致忽略MAC地址中的对应位，而0将是匹配位(例如00:00:00:00:00:11)。

**注意：**假设掩码为0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 (这表示匹配位的位置)为0，在有1的位上不匹配)。您需要将1转换为十六进制值，并且每四个零写0。在本示例中，自111 1111 = FF以来，掩码将写成：00:00:00:00:00:FF。

步骤14.在VLAN ID 字段中，输入1 - 4094之间的VLAN ID。如果数据包包含此VLAN ID，ACE会将其视为匹配。此字段不是必需的；将其留空将导致ACE在检查数据包时不考虑VLAN ID。

VLAN ID:  (Range: 1 - 4094)

步骤15.在802.1p 字段中，选中Include 复选框以使ACE包括802.1p条件。如果包括802.1p条件，请在“802.1p值”和“802.1p掩码” 字段中输入802.1p值和掩码。两个字段的范围是0 - 7。如果数据包包含相应的802.1p值并符合掩码，ACE会将其视为匹配。

802.1p:  Include

802.1p Value:  (Range: 0 - 7)

802.1p Mask:  (Range: 0 - 7)

步骤16.在Ethertype 字段中，输入将与传入数据包进行比较的Ethertype值。Ethertype是帧中的一个二进制八位数字段，表示数据包中封装的协议。范围为5DD-FFFF。如果数据包包含指定的Ethertype值，ACE会将其视为匹配。Ethertype值列表可在此[IEEE标准页上找到](#)。

Ethertype:  (Range: 5DD - FFFF)

步骤17.单击“应用”。ACE将添加到指定的ACL。单击Close返回到基于MAC的ACE页。



ACL Name: ExampleACL

Priority:  (Range: 1 - 2147483647)

Action:  Permit  
 Deny  
 Shutdown

Logging:  Enable

Destination MAC Address:  Any  
 User Defined

Destination MAC Address Value:

Destination MAC Wildcard Mask:  (0s for matching, 1s for no matching)

Source MAC Address:  Any  
 User Defined

Source MAC Address Value:

Source MAC Wildcard Mask:  (0s for matching, 1s for no matching)

VLAN ID:  (Range: 1 - 4094)

802.1p:  Include

802.1p Value:  (Range: 0 - 7)

802.1p Mask:  (Range: 0 - 7)

Ethertype:  (Range: 5DD - FFFF)

**Apply** Close

## 映射基于MAC的ACL 到端口

步骤1. ACL可以映射到端口或VLAN。要将基于MAC的ACL映射到端口，请导航至Access Control > ACL Binding(Port)。将打开“ACL绑定(端口)”页。

ACL Binding (Port)

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

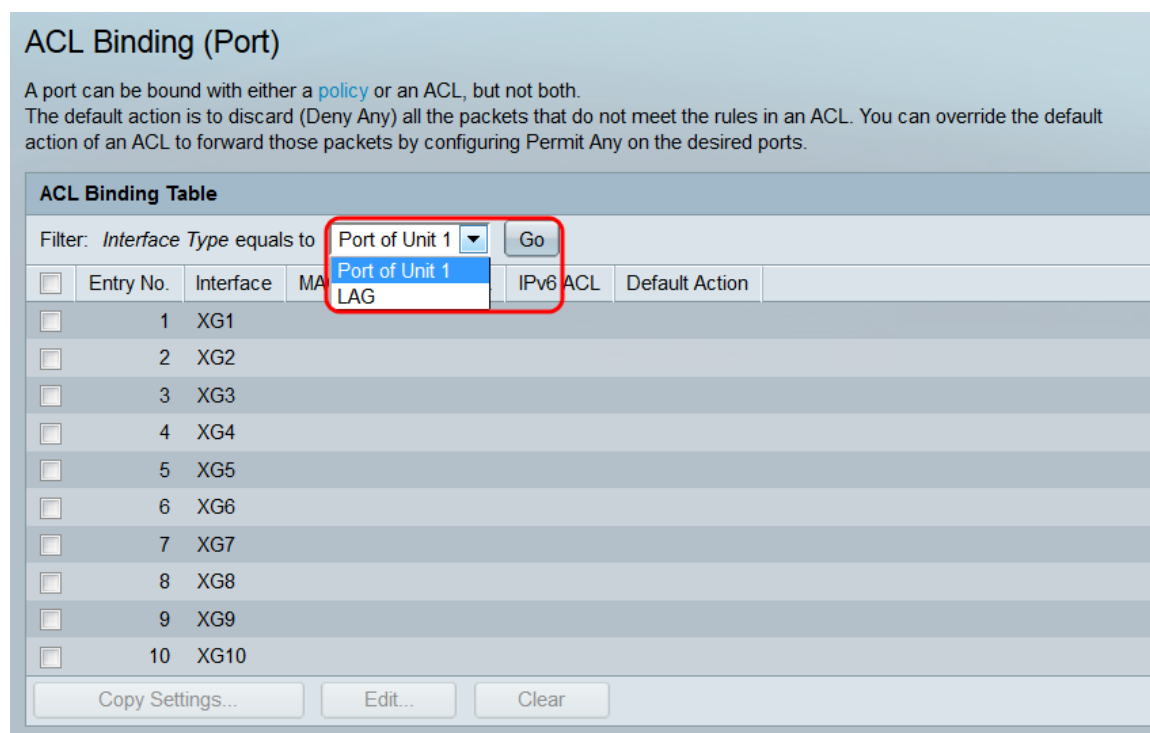
ACL Binding Table Showing 1-10 of 48  per page

Filter: Interface Type equals to

<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input type="checkbox"/>	1	XG1				
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

[\[1-10\]](#) [\[11-20\]](#) [\[21-30\]](#) [\[31-40\]](#) [\[41-48\]](#)

步骤2.在ACL绑定表顶部的下拉列表中，选择端口或LAG（链路聚合组）作为接口类型。如果交换机是堆栈的一部分，则可以从其他设备选择端口。单击Go以显示指定接口类型的列表。



ACL Binding (Port)

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

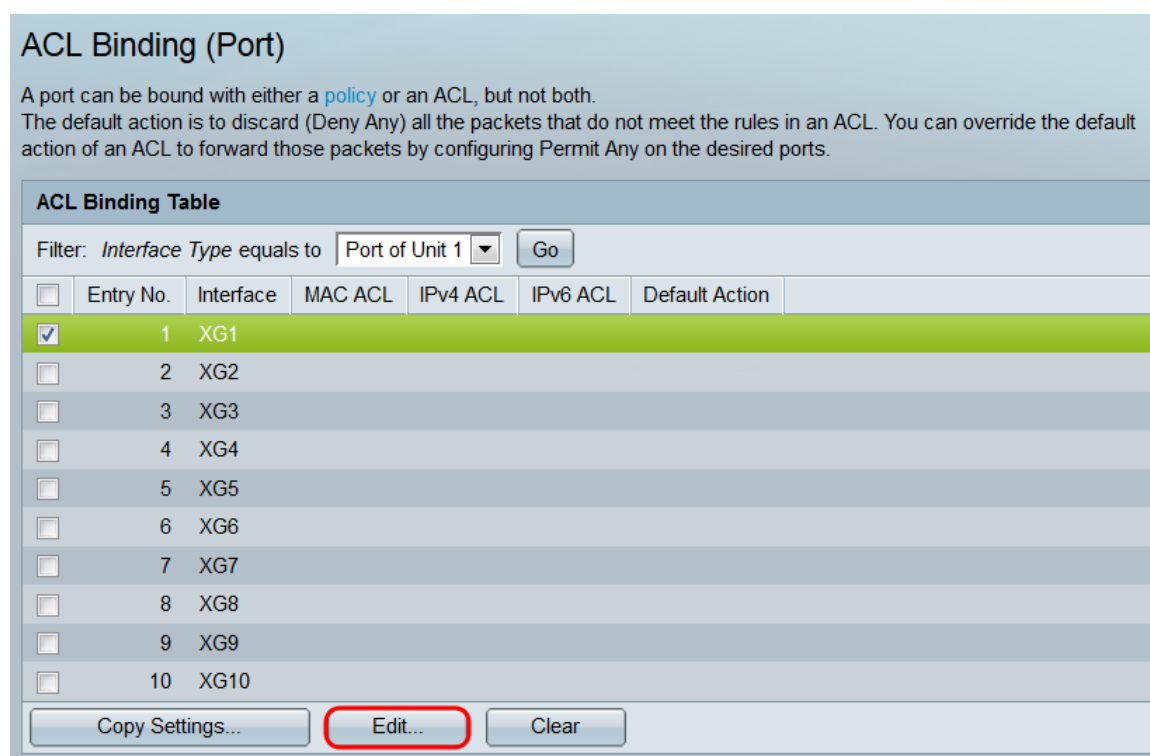
ACL Binding Table

Filter: Interface Type equals to Port of Unit 1 Go

<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input type="checkbox"/>	1	XG1				
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

Copy Settings... Edit... Clear

步骤3.选中接口的复选框，然后单击“编辑.....”按钮。“编辑ACL绑定”窗口打开。



ACL Binding (Port)

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

ACL Binding Table

Filter: Interface Type equals to Port of Unit 1 Go

<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	XG1				
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

Copy Settings... Edit... Clear

步骤4. Interface字段显示当前正在配置的端口或LAG。它将自动显示ACL绑定表中选定的接口。此字段可用于在不返回ACL绑定（端口）页的情况下在不同接口之间快速切换。

Interface:  Unit 1 Port XG1  LAG 1

Select MAC-Based ACL: ExampleACL

Select IPv4-Based ACL: [dropdown]

Select IPv6-Based ACL: [dropdown]

Default Action:  Deny Any  Permit Any

Apply Close

步骤5.选中**Select MAC-Based ACL** 复选框，然后使用下拉列表选择要映射到指定接口的ACL。

Interface:  Unit 1 Port XG1  LAG 1

Select MAC-Based ACL: ExampleACL

Select IPv4-Based ACL: [dropdown]

Select IPv6-Based ACL: [dropdown]

Default Action:  Deny Any  Permit Any

Apply Close

步骤6.在“默认操作”字段中，选择单选按钮以确定如何处理与ACL标准不匹配的数据包。默认值为**Deny Any**，它会丢弃任何与ACL标准不匹配的数据包；**Permit Any**将转发不匹配的数据包。

Interface:  Unit 1 Port XG1  LAG 1

Select MAC-Based ACL: ExampleACL

Select IPv4-Based ACL: [dropdown]

Select IPv6-Based ACL: [dropdown]

Default Action:  Deny Any  Permit Any

Apply Close

步骤7.单击“应用”。ACL映射到指定接口。可以使用接口字段选择要配置的不同接口，或单击关闭返回ACL绑定（端口）页。

Interface:  Unit  Port  LAG

Select MAC-Based ACL: ExampleACL

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

**Apply** Close

步骤8.要快速将接口的设置复制到其他接口，请选中要复制的接口的复选框，然后单击“复制设置……”按钮。“复制设置”窗口打开。

### ACL Binding (Port)

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

ACL Binding Table						
Filter:	Interface	Type	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
Interface Type equals to	Port of Unit 1					
<input checked="" type="checkbox"/>	1	XG1	ExampleACL			Deny Any
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

**Copy Settings...** Edit... Clear

步骤9.在文本字段中，输入要将设置复制到的接口。接口可以用逗号分隔，也可以指定范围。

Copy configuration from entry 1 (XG1)

to:  (Example: 1,3,5-10 or: XG1,XG3-XG5)

**Apply** Close

步骤10.单击“应用”。将复制设置。

Copy configuration from entry 1 (XG1)

to:  (Example: 1,3,5-10 or: XG1,XG3-XG5)

步骤11.如果要清除接口的设置，请选中其复选框并单击“清除”。请注意，可以同时选择和清除多个接口。

### ACL Binding (Port)

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

ACL Binding Table						
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1"/> <input type="button" value="Go"/>						
<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	XG1	ExampleACL			Deny Any
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

## 将基于MAC的ACL映射到VLAN

步骤1. ACL可以映射到端口或VLAN。要将基于MAC的ACL映射到VLAN，请导航到**Access Control > ACL Binding(VLAN)**。将打开“ACL绑定(VLAN)”页。

### ACL Binding (VLAN)

ACL Binding Table					
<input type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
0 results found.					

步骤2. ACL绑定表显示当前映射到VLAN的所有ACL。如果尚未映射ACL，则表为空。要将ACL映射到VLAN，请单击**Add...**按钮。“添加ACL绑定”窗口打开。

## ACL Binding (VLAN)

ACL Binding Table					
<input type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
0 results found.					
Copy Settings...		Add...		Edit...	Delete

步骤3.选择VLAN，使用VLAN ID字段中的下拉列表将ACL映射。此字段还可用于在不返回ACL绑定(VLAN)页的情况下在不同VLAN之间快速切换。

VLAN ID:

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

步骤4.选中Select MAC-Based ACL 复选框，然后使用下拉列表选择要映射到指定VLAN的ACL。

VLAN ID:

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

**注意：**不能将使用VLAN ID作为其条件一部分的基于MAC的ACL绑定到VLAN。此外，时间范围内的ACL无法绑定到VLAN。

步骤5.在Default Action字段中，选择一个单选按钮以确定如何处理与ACL标准不匹配的数据包。默认值为Deny Any，它会丢弃任何与ACL标准不匹配的数据包；Permit Any将转发不匹配的数据包。

VLAN ID:

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

步骤6.单击“应用”。ACL映射到指定的VLAN。您可以使用 *VLAN ID* 字段选择要配置的不同 VLAN，或单击关闭返回ACL绑定(VLAN)页面。

VLAN ID:

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action:  Deny Any  Permit Any

步骤7.要快速将VLAN的设置复制到其他VLAN，请选中要复制的VLAN配置的复选框，然后单击“复制设置……”按钮。“复制设置”窗口打开。

### ACL Binding (VLAN)

ACL Binding Table					
<input checked="" type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	ExampleACL			Deny Any

步骤8.在文本字段中，输入要将设置复制到的VLAN ID或VLAN ID。ID可以用逗号分隔，也可以指定范围。

Copy configuration from VLAN1  
to VLAN(s):  (Example: 1,3,5-10)

步骤9.单击“应用”。将复制设置。

Copy configuration from VLAN1  
to VLAN(s):  (Example: 1,3,5-10)

步骤10.如果要清除VLAN的设置，请选中其复选框，然后单击删除。请注意，可以同时选择和清除多个VLAN。

### ACL Binding (VLAN)

ACL Binding Table					
<input checked="" type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	ExampleACL			Deny Any