

# 目 录

1 MAC地址表 .....	1-1
1.1 MAC地址表简介 .....	1-1
1.1.1 MAC地址表项的生成方式 .....	1-1
1.1.2 MAC地址表项的分类 .....	1-1
1.2 配置MAC地址表 .....	1-2
1.2.1 配置MAC地址表项 .....	1-2
1.2.2 关闭接口的MAC地址学习功能 .....	1-3
1.2.3 配置动态MAC地址表项的老化时间 .....	1-4
1.2.4 配置接口的MAC地址数学习上限 .....	1-4
1.2.5 配置当达到接口的MAC地址数学习上限时的报文转发规则 .....	1-5
1.2.6 配置接口的MAC地址学习优先级 .....	1-5
1.2.7 配置MAC地址迁移上报功能 .....	1-5
1.2.8 开启MAC地址表告警功能 .....	1-6
1.3 MAC地址表显示和维护 .....	1-7
1.4 MAC地址表典型配置举例 .....	1-7

# 1 MAC地址表

## 1.1 MAC地址表简介

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目 的 MAC 地址查询 MAC 地址表，如果 MAC 地址表中包含与报文目的 MAC 地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

### 1.1.1 MAC地址表项的生成方式

MAC 地址表项的生成方式有两种：自动生成、手工配置。

#### 1. 自动生成MAC地址表项

一般情况下，MAC 地址表由设备通过源 MAC 地址学习自动生成。设备学习 MAC 地址的过程如下：

- 从某接口（假设为接口 A）收到一个数据帧，设备分析该数据帧的源 MAC 地址（假设为 MAC-SOURCE），并认为目的 MAC 地址为 MAC-SOURCE 的报文可以由接口 A 转发。
- 如果 MAC 地址表中已经包含 MAC-SOURCE，设备将对该表项进行更新。
- 如果 MAC 地址表中尚未包含 MAC-SOURCE，设备则将这个新 MAC 地址以及该 MAC 地址对应的接口 A 作为一个新的表项加入到 MAC 地址表中。

为适应网络拓扑的变化，MAC 地址表需要不断更新。MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到刷新的表项将被删除，这个生存周期被称作老化时间。如果在到达生存周期前某表项被刷新，则重新计算该表项的老化时间。

#### 2. 手工配置MAC地址表项

设备通过源 MAC 地址学习自动生成 MAC 地址表时，无法区分合法用户和非法用户的报文，带来了安全隐患。如果非法用户将攻击报文的源 MAC 地址伪装成合法用户的 MAC 地址，并从设备的其他接口进入，设备就会学习到错误的 MAC 地址表项，于是将本应转发给合法用户的报文转发给非法用户。

为了提高安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

### 1.1.2 MAC地址表项的分类

MAC 地址表项分为以下几种：

- 静态 MAC 地址表项：由用户手工配置，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项不老化。静态 MAC 地址表项优先级高于自动生成的 MAC 地址表项。
- 动态 MAC 地址表项：可以由用户手工配置，也可以由设备通过源 MAC 地址学习自动生成，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项有老化时间。手工配置的动态 MAC 地址表项优先级等于自动生成的 MAC 地址表项。

- 黑洞 MAC 地址表项：由用户手工配置，用于丢弃源 MAC 地址或目的 MAC 地址为指定 MAC 地址的报文（例如，出于安全考虑，可以禁止某个用户发送和接收报文），表项不老化。

静态 MAC 地址表项和黑洞 MAC 地址表项不会被动态 MAC 地址表项覆盖，而动态 MAC 地址表项可以被静态 MAC 地址表项和黑洞 MAC 地址表项覆盖。



说明

本章节内容只涉及单播的静态、动态和黑洞 MAC 地址表项。

## 1.2 配置MAC地址表

以下配置均为可选配置，且配置过程无先后顺序，用户可以根据实际情况选择配置。

### 1.2.1 配置MAC地址表项

配置 MAC 地址表项时，需要注意：

- 在手工配置动态 MAC 地址表项时，如果 MAC 地址表中已经存在 MAC 地址相匹配的自动生成表项，但该表项的接口与配置不符，那么该手工配置失败。
- 如果不保存配置，设备重启后所有手工配置的 MAC 地址表项都会丢失；如果保存配置，设备重启后手工配置的静态 MAC 地址表项和黑洞 MAC 地址表项不会丢失，手工配置的动态 MAC 地址表项会丢失。

配置 MAC 地址表项后，当设备收到的报文的源 MAC 地址与配置表项中的 MAC 地址相同时，不同类型的 MAC 地址表项处理方式不同：

表1-1 不同类型 MAC 地址表项对源 MAC 地址匹配报文的处理方式

MAC 地址表项类型	报文源 MAC 地址与配置表项中的 MAC 地址相同
静态MAC地址表项	<ul style="list-style-type: none"> <li>• 如果报文入接口与表项中的接口不同，则丢弃该报文</li> <li>• 如果报文入接口与表项中的接口相同，则转发该报文</li> </ul>
动态MAC地址表项	<ul style="list-style-type: none"> <li>• 如果报文入接口与该表项中的接口不同，则进行 MAC 地址学习，并覆盖该表项</li> <li>• 如果报文入接口与该表项中的接口相同，则转发该报文，并更新该表项老化时间</li> </ul>

## 2. 配置静态/动态MAC地址表项

### (1) 全局配置静态/动态 MAC 地址表项

表1-2 全局配置静态/动态 MAC 地址表项

操作	命令	说明
进入系统视图	<b>system-view</b>	-

操作	命令	说明
添加或者修改静态/动态MAC地址表项	<b>mac-address { dynamic   static }</b> <i>mac-address interface interface-type interface-number vlan vlan-id</i>	缺省情况下，系统没有配置任何MAC地址表项 <b>interface</b> 参数指定的接口必须属于 <i>vlan-id</i> 参数指定的VLAN，而且该VLAN必须事先创建，否则将配置失败

## (2) 接口配置静态/动态 MAC 地址表项

表1-3 接口配置静态/动态 MAC 地址表项

操作	命令	说明
进入系统视图	<b>system-view</b>	-
二层以太网接口视图	<b>interface interface-type interface-number</b>	-
在当前接口下添加或者修改静态/动态MAC地址表项	<b>mac-address { dynamic   static }</b> <i>mac-address vlan vlan-id</i>	缺省情况下，接口下没有配置任何MAC地址表项 当前接口必须属于 <i>vlan-id</i> 参数指定的VLAN，而且该VLAN必须事先创建，否则将配置失败

## 3. 配置黑洞MAC地址表项

表1-4 配置黑洞 MAC 地址表项

操作	命令	说明
进入系统视图	<b>system-view</b>	-
添加或者修改黑洞MAC地址表项	<b>mac-address blackhole mac-address vlan vlan-id</b>	缺省情况下，系统没有配置任何MAC地址表项 <i>vlan-id</i> 参数指定的VLAN必须事先创建，否则将配置失败

### 1.2.2 关闭接口的MAC地址学习功能

缺省情况下，MAC地址学习功能处于开启状态。有时为了保证设备的安全，需要关闭MAC地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源MAC地址不同的报文攻击设备，导致设备MAC地址表资源耗尽，造成设备无法根据网络的变化更新MAC地址表。关闭MAC地址学习功能可以有效防止这种攻击。

在开启全局的MAC地址学习功能的前提下，用户可以关闭设备上单个接口的MAC地址学习功能。

表1-5 关闭接口的MAC地址学习功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-

操作		命令	说明
进入接口视图	二层以太网接口视图	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	-
关闭接口的MAC地址学习功能		<b>undo mac-address</b> <b>mac-learning enable</b>	缺省情况下，接口的MAC地址学习功能处于开启状态

### 1.2.3 配置动态MAC地址表项的老化时间

当网络拓扑改变后，如果动态 MAC 地址表项不及时更新，会导致用户流量不能正常转发。配置动态 MAC 地址表项的老化时间后，超过老化时间的动态 MAC 地址表项会被自动删除，设备将重新进行 MAC 地址学习，构建新的动态 MAC 地址表项。

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，导致设备广播大量的数据报文，增加网络的负担。

用户需要根据实际情况，配置合适的老化时间。如果网络比较稳定，可以将老化时间配置得长一些或者配置为不老化；否则，可以将老化时间配置得短一些。比如在一个比较稳定的网络，如果长时间没有流量，动态 MAC 地址表项会被全部删除，可能导致设备突然广播大量的数据报文，造成安全隐患，此时可将动态 MAC 地址表项的老化时间设得长一些或不老化，以减少广播，增加网络稳定性和安全性。

动态 MAC 地址表项的老化时间作用于全部接口上。

表1-6 配置动态 MAC 地址表项的老化时间

操作		命令	说明
进入系统视图		<b>system-view</b>	-
配置动态MAC地址表项的老化时间		<b>mac-address timer</b> { <b>aging</b> <i>seconds</i>   <b>no-aging</b> }	缺省动态MAC地址表项的老化时间为300秒

### 1.2.4 配置接口的MAC地址数学习上限

通过配置接口的 MAC 地址数学习上限，用户可以控制设备维护的 MAC 地址表的表项数量。如果 MAC 地址表过于庞大，可能导致设备的转发性能下降。当接口学习到的 MAC 地址数达到上限时，该接口将不再对 MAC 地址进行学习。

表1-7 配置接口的 MAC 地址数学习上限

操作		命令	说明
进入系统视图		<b>system-view</b>	-
进入接口视图	二层以太网接口视图	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	-

操作	命令	说明
配置接口的MAC地址数学习上限	<b>mac-address max-mac-count</b> <i>count</i>	-

### 1.2.5 配置当达到接口的MAC地址数学习上限时的报文转发规则

当学习到的 MAC 地址数达到上限时，用户可以选择是否允许系统转发源 MAC 不在 MAC 地址表里的报文。

表1-8 配置允许转发源 MAC 地址不在 MAC 地址表里的报文

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入接口视图	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	-
配置当达到接口的MAC地址数学习上限时，允许转发源MAC地址不在MAC地址表里的报文	<b>mac-address max-mac-count</b> <b>enable-forwarding</b>	缺省情况下，当达到接口的MAC地址数学习上限时，允许转发源MAC地址不在MAC地址表里的报文

### 1.2.6 配置接口的MAC地址学习优先级

基于 MAC 地址转发报文的网络有时会因为下行接口的攻击行为或者环路，下行接口学习到网关等上层设备的 MAC 地址。为了避免这种情况，将接口的 MAC 地址学习功能分为两个优先级：高优先级和低优先级。对于高优先级的接口，可以学习任何 MAC 地址；对于低优先级的接口，在学习 MAC 地址时需要查看高优先级接口是否已经学到该 MAC 地址，如果已经学到，则不允许学习该 MAC 地址。比如，可以将上行接口的 MAC 地址学习优先级配置为高优先级，下行接口的 MAC 地址学习优先级配置为低优先级，那么，下行接口就不会学到网关等上层设备的 MAC 地址，避免了攻击。

表1-9 配置接口的 MAC 地址学习优先级

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入接口视图	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	-
配置接口的MAC地址学习优先级	<b>mac-address mac-learning priority</b> { <b>high</b>   <b>low</b> }	缺省情况下，MAC地址学习优先级为低优先级

### 1.2.7 配置MAC地址迁移上报功能

MAC 地址迁移是指：设备从某接口（假设接口 A）学习到某 MAC 地址，之后从另一接口（假设接口 B）接收到了以该 MAC 地址为源 MAC 地址的报文，且接口 B 与接口 A 所属的 VLAN 相同，则该 MAC 地址表项的出接口改为接口 B，此时认为该 MAC 地址从接口 A 迁移到接口 B。

如果 MAC 地址迁移频繁出现，且同一 MAC 地址总是在特定的两个接口之间迁移，那么网络中可能存在二层环路。可以通过查看 MAC 地址迁移记录，发现和定位环路。

当监测到某端口频繁迁移时，用户可以通过配置 MAC 地址迁移抑制功能，使频繁迁移的端口 down，一定时间后该端口将自行恢复 up，或者用户通过手动方式将该端口 up。

如果需要查看设备启动后的 MAC 地址迁移记录，请使用 **display mac-address mac-move** 命令。

表1-10 配置 MAC 地址迁移上报功能

操作		命令	说明
进入系统视图		<b>system-view</b>	-
开启MAC地址迁移上报功能		<b>mac-address notification mac-move [ interval interval-value ]</b>	缺省情况下，MAC地址迁移上报功能处于关闭状态 需要注意的是，执行本命令后，必须同时通过 <b>snmp-agent trap enable mac-address</b> 命令开启MAC地址表的告警功能，系统才会显示MAC地址迁移日志
(可选) 配置MAC地址迁移抑制功能的相关参数		<b>mac-address notification mac-move suppression { interval interval-value   threshold threshold-value }</b>	MAC地址迁移抑制功能的相关参数未配置，采用缺省抑制时间间隔30秒和缺省阈值3次 配置本命令后，当接口上开启了MAC地址迁移抑制功能时，本命令配置的参数才能生效
进入接口视图	二层以太网接口视图	<b>interface interface-type interface-number</b>	-
(可选) 开启当前接口上的MAC地址迁移抑制功能		<b>mac-address notification mac-move suppression</b>	缺省情况下，MAC地址迁移抑制功能处于关闭状态

## 1.2.8 开启MAC地址表告警功能

开启 MAC 地址表的告警功能后，MAC 地址表模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，请通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

关闭 MAC 地址表的告警功能后，设备将发送日志信息到信息中心模块，此时请配置信息中心的输出规则和输出方向来查看 MAC 地址表模块的日志信息。

有关 SNMP 和信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”和“信息中心”。

表1-11 开启 MAC 地址表告警功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-



操作	命令	说明
开启MAC地址表的告警功能	<b>snmp-agent trap enable mac-address [ mac-move ]</b>	缺省情况下，MAC地址表的告警功能处于开启状态 当MAC地址表的告警功能关闭后，将采用Syslog方式上报信息

## 1.3 MAC地址表显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MAC 地址表的运行情况，通过查看显示信息验证配置的效果。

表1-12 MAC 地址表显示和维护

操作	命令
显示MAC地址表信息	<b>display mac-address [ mac-address [ vlan vlan-id ]   [ [ dynamic   static ] [ interface interface-type interface-number ]   blackhole ] [ vlan vlan-id ] [ count ] ]</b>
显示MAC地址表动态表项的老化时间	<b>display mac-address aging-time</b>
显示MAC地址学习功能的使能状态	<b>display mac-address mac-learning [ interface interface-type interface-number ]</b>
显示MAC地址迁移记录	<b>display mac-address mac-move</b>

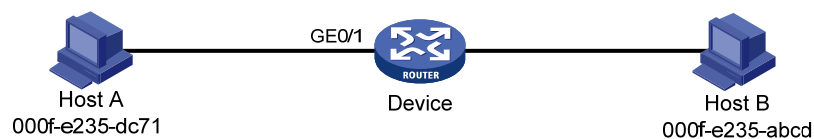
## 1.4 MAC地址表典型配置举例

### 1. 组网需求

- 现有一台用户主机，它的 MAC 地址为 000f-e235-dc71，属于 VLAN 1，连接 Device 的端口 GigabitEthernet0/1。为防止假冒身份的非法用户骗取数据，在设备的 MAC 地址表中为该用户主机添加一条静态表项。
- 另有一台用户主机，它的 MAC 地址为 000f-e235-abcd，属于 VLAN 1。由于该用户主机曾经接入网络进行非法操作，为了避免此种情况再次发生，在设备上添加一条黑洞 MAC 地址表项，使该用户主机接收不到报文。
- 配置设备的动态 MAC 地址表项老化时间为 500 秒。

### 2. 组网图

图1-1 MAC 地址表典型配置组网图





### 3. 配置步骤

# 增加一个静态 MAC 地址表项，目的地址为 000f-e235-dc71，出接口为 GigabitEthernet0/1，且该接口属于 VLAN 1。

```
<Device> system-view
```

```
[Device] mac-address static 000f-e235-dc71 interface gigabitethernet 0/1 vlan 1
```

# 增加一个黑洞 MAC 地址表项，地址为 000f-e235-abcd，属于 VLAN 1。

```
[Device] mac-address blackhole 000f-e235-abcd vlan 1
```

# 配置动态 MAC 地址表项的老化时间为 500 秒。

```
[Device] mac-address timer aging 500
```

### 4. 验证配置

# 查看端口 GigabitEthernet0/1 上的静态 MAC 地址表项信息。

```
[Device] display mac-address static interface gigabitethernet 0/1
```

MAC Address	VLAN ID	State	Port/NickName	Aging
000f-e235-dc71	1	Static	GE0/1	N

# 查看黑洞 MAC 地址表信息。

```
[Device] display mac-address blackhole
```

MAC Address	VLAN ID	State	Port/NickName	Aging
000f-e235-abcd	1	Blackhole	N/A	N

# 查看动态 MAC 地址表项的老化时间。

```
[Device] display mac-address aging-time
```

```
MAC address aging time: 500s.
```