H3C LA 系列无线网关

二层技术-以太网交换配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W101-20180328

前 言

H3C LA 系列无线网关 配置指导(V7)介绍了 LA 系列无线网关各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《二层技术-以太网交换配置指导》主要介绍以太网相关协议原理和配置，包括 VLAN、二层转发等。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格　式	意　义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

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	• 如果报文入接口与表项中的接口不同，则丢弃该报文 • 如果报文入接口与表项中的接口相同，则转发该报文
动态MAC地址表项	• 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 • 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

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	**system-view**	-

操作	命令	说明
添加或者修改静态/动态MAC地址表项	**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	缺省情况下，系统没有配置任何MAC地址表项 **interface**参数指定的接口必须属于*vlan-id*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	**system-view**	-
二层以太网接口视图	**interface** *interface-type interface-number*	-
在当前接口下添加或者修改静态/动态MAC地址表项	**mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*	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*vlan-id*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	**system-view**	-
添加或者修改黑洞MAC地址表项	**mac-address blackhole** *mac-address* **vlan** *vlan-id*	缺省情况下，系统没有配置任何MAC地址表项 *vlan-id*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	**system-view**	-

操作		命令	说明
进入接口视图	二层以太网接口视图	**interface** *interface-type interface-number*	-
关闭接口的MAC地址学习功能		**undo mac-address mac-learning enable**	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	**system-view**	-
配置动态MAC地址表项的老化时间	**mac-address timer** { **aging** *seconds* | **no-aging** }	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		**system-view**	-
进入接口视图	二层以太网接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置接口的MAC地址数学习上限	**mac-address max-mac-count** *count*	-

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		**system-view**	-
进入接口视图	二层以太网接口视图	**interface** *interface-type interface-number*	-
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		**mac-address max-mac-count enable-forwarding**	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		**system-view**	-
进入接口视图	二层以太网接口视图	**interface** *interface-type interface-number*	-
配置接口的MAC地址学习优先级		**mac-address mac-learning priority { high | low }**	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		**system-view**	-
开启MAC地址迁移上报功能		**mac-address notification mac-move** [**interval** *interval-value*]	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**snmp-agent trap enable mac-address**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		**mac-address notification mac-move suppression** { **interval** *interval-value* | **threshold** *threshold-value* }	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	**interface** *interface-type interface-number*	-
（可选）开启当前接口上的MAC地址迁移抑制功能		**mac-address notification mac-move suppression**	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	**system-view**	-

操作	命令	说明
开启MAC地址表的告警功能	**snmp-agent trap enable mac-address** [**mac-move**]	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	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]
显示MAC地址表动态表项的老化时间	**display mac-address aging-time**
显示MAC地址学习功能的使能状态	**display mac-address mac-learning** [**interface** *interface-type interface-number*]
显示MAC地址迁移记录	**display mac-address mac-move**

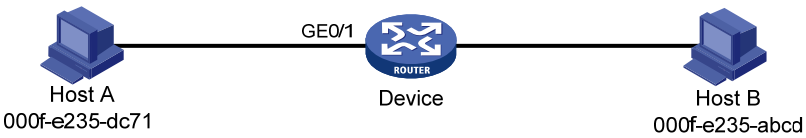
1.4 MAC地址表典型配置举例

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.
```

目 录

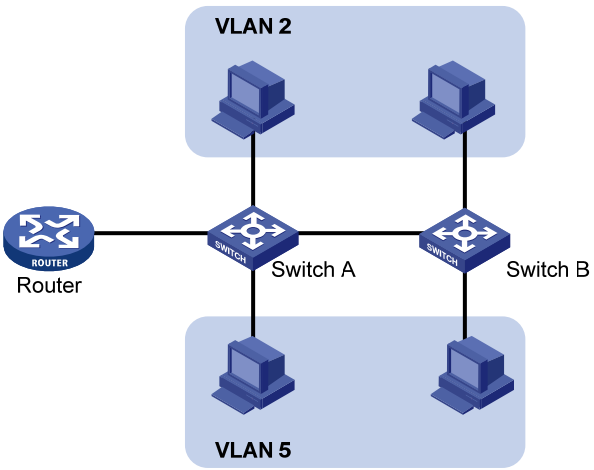
1 VLAN

1.1 VLAN简介

1.1.1 VLAN概述

以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问）技术的共享通讯介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域。当网络中主机数目较多时会导致冲突严重、广播泛滥、性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个物理LAN划分成多个逻辑的LAN——VLAN。处于同一VLAN的主机能直接互通，而处于不同VLAN的主机则不能直接互通。这样，广播报文被限制在同一个VLAN内，即每个VLAN是一个广播域。如 图 1-1 所示，VLAN 2 内的主机可以互通，但与VLAN 5 内的主机不能互通。

图1-1 VLAN 示意图



VLAN 的划分不受物理位置的限制：物理位置不在同一范围的主机可以属于同一个 VLAN；一个 VLAN 包含的主机可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由器。

VLAN 根据划分方式不同可以分为不同类型。基于端口划分 VLAN 是其中最简单、最有效的 VLAN 划分方式。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发该 VLAN 的报文。本章将介绍基于端口的 VLAN。

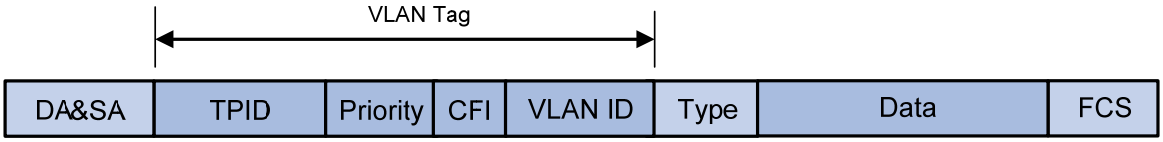
VLAN 的优点如下：

- 限制广播域。广播域被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强局域网的安全性。VLAN 间的二层报文是相互隔离的，即一个 VLAN 内的主机不能和其他 VLAN 内的主机直接通信，如果不同 VLAN 要进行通信，则需通过路由器或三层交换机等三层设备。
- 灵活构建虚拟工作组。通过 VLAN 可以将不同的主机划分到不同的工作组，同一工作组的主机可以位于不同的物理位置，网络构建和维护更方便灵活。

1.1.2 VLAN报文封装

要使网络设备能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 的字段。IEEE 802.1Q 协议规定，在以太网报文的目的 MAC 地址和源 MAC 地址字段之后、协议类型字段之前加入 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。

图1-2 VLAN Tag 的组成字段



如 图 1-2 所示，VLAN Tag包含四个字段，分别是TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和VLAN ID。

- TPID：协议规定 TPID 取值为 0x8100 时表示报文带有 VLAN Tag，但各设备厂商可以自定义该字段的值。当邻居设备将 TPID 值配置为非 0x8100 时，为了能够识别这样的报文，实现互通，必须在本设备上修改 TPID 值，确保和邻居设备的 TPID 值配置一致。如果报文的 TPID 值为配置值或 0x8100，则该报文被认为带有 VLAN Tag。
- Priority：用来表示报文的 802.1p 优先级，长度为 3 比特，相关内容请参见“ACL 和 QoS 配置指导/QoS”中的“附录”。
- CFI：用来表示 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1 比特。取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装。在以太网中，CFI 取值为 0。
- VLAN ID：用来表示该报文所属 VLAN 的编号，长度为 12 比特。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的取值范围为 1～4094。

网络设备根据报文是否携带VLAN Tag以及携带的VLAN Tag信息，来对报文进行处理，利用VLAN ID来识别报文所属的VLAN。详细的处理方式请参见“1.4.1 基于端口的VLAN简介”。

说明

- 以太网支持 Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式，本文以 Ethernet II 型封装为例。802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式添加 VLAN Tag 字段的方式请参见相关协议规范。
- 对于带有多层 VLAN Tag 的报文，设备会根据其最外层 VLAN Tag 进行处理，而内层 VLAN Tag 会被视为报文的普通数据部分。

1.1.3 协议规范

与 VLAN 相关的协议规范有：

- IEEE 802.1Q：IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 配置VLAN基本属性

表1-1 配置 VLAN 基本属性

配置	命令	说明
进入系统视图	**system-view**	-
（可选）创建一个VLAN并进入VLAN视图，或批量创建VLAN	**vlan** *vlan-id1* [**to** *vlan-id2*]	缺省情况下，系统只有一个缺省VLAN（VLAN 1）
进入VLAN视图	**vlan** *vlan-id*	批量创建VLAN时，为必选；否则，无需执行本命令
指定当前VLAN的名称	**name** *text*	缺省情况下，VLAN的名称为“VLAN *vlan-id*”，其中*vlan-id*为该VLAN的编号。例如，VLAN 100的名称为“VLAN 0100”
配置当前VLAN的描述信息	**description** *text*	缺省情况下，VLAN的描述信息为“VLAN *vlan-id*”，其中*vlan-id*为该VLAN的编号。例如，VLAN 100的描述信息为“VLAN 0100”

说明

- VLAN 1 为系统缺省 VLAN，用户不能手工创建和删除。
- 动态学习到的 VLAN，以及被其他应用锁定不让删除的 VLAN，都不能使用 **undo vlan** 命令直接删除。只有将相关配置删除之后，才能删除相应的 VLAN。

1.3 配置VLAN接口基本属性

不同 VLAN 间的主机不能直接通信，通过在设备上创建并配置 VLAN 接口，可以实现 VLAN 间的三层互通。

VLAN 接口是一种三层的虚拟接口，它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，在为 VLAN 接口配置了 IP 地址后，该 IP 地址即可作为本 VLAN 内网络设备的网关地址，对需要跨网段的报文进行基于 IP 地址的三层转发。

配置 VLAN 接口基本属性时，需要注意：在创建 VLAN 接口之前，对应的 VLAN 必须已经存在，否则将不能创建指定的 VLAN 接口。

表1-2 配置 VLAN 接口基本属性

配置	命令	说明
进入系统视图	**system-view**	-
创建VLAN接口并进入VLAN接口视图	**interface vlan-interface** *interface-number*	如果该VLAN接口已经存在，则直接进入该VLAN接口视图 缺省情况下，未创建VLAN接口
配置VLAN接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	缺省情况下，未配置VLAN接口的IP地址

配置	命令	说明
配置当前VLAN接口的描述信息	**description** *text*	缺省情况下，VLAN接口的描述信息为该VLAN接口的接口名，如“Vlan-interface1 Interface”
配置VLAN接口的MTU值	**mtu** *size*	缺省情况下，VLAN接口的MTU值为1500
（可选）配置VLAN接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbps）
（可选）恢复当前VLAN接口的缺省配置	**default**	-
（可选）取消手工关闭VLAN接口	**undo shutdown**	缺省情况下，未手工关闭VLAN接口

1.4 配置基于端口的VLAN

1.4.1 基于端口的VLAN简介

基于端口划分 VLAN 是最简单、最有效的 VLAN 划分方法。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，该端口就可以转发该 VLAN 的报文。

1. 端口的链路类型

根据端口在转发报文时对 VLAN Tag 的不同处理方式，可将端口的链路类型分为三种：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。一般用于和不能识别 VLAN Tag 的用户终端设备相连，或者不需要区分不同 VLAN 成员时使用。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。

2. 端口缺省VLAN

除了可以配置端口允许通过的 VLAN 外，还可以配置端口的缺省 VLAN，即端口 VLAN ID（Port VLAN ID，PVID）。

- Access 端口的缺省 VLAN 就是它所在的 VLAN。
- Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，能够配置端口缺省 VLAN。
- 当执行 **undo vlan** 命令删除的 VLAN 是某个端口的缺省 VLAN 时，对 Access 端口，端口的缺省 VLAN 会恢复到 VLAN 1；对 Trunk 或 Hybrid 端口，端口的缺省 VLAN 配置不会改变，即它们可以使用已经不存在的 VLAN 作为端口缺省 VLAN。

说明

- 建议本端设备端口的缺省 VLAN ID 和相连的对端设备端口的缺省 VLAN ID 保持一致。
- 建议保证端口的缺省 VLAN 为端口允许通过的 VLAN。如果端口不允许某 VLAN 通过，但是端口的缺省 VLAN 为该 VLAN，则端口会丢弃收到的该 VLAN 的报文或者不带 VLAN Tag 的报文。

3. 端口对报文的处理方式

在配置了端口链路类型和端口缺省VLAN后，端口对报文的接收和发送的处理有几种不同情况，具体情况请参看 表 1-3。

表1-3 不同链路类型端口收发报文的差异

端口类型	对接收报文的处理		对发送报文的处理
	当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
Access端口	为报文添加端口缺省VLAN的Tag	• 当报文的 VLAN ID 与端口的缺省 VLAN ID 相同时，接收该报文 • 当报文的 VLAN ID 与端口的缺省 VLAN ID 不同时，丢弃该报文	去掉Tag，发送该报文
Trunk端口	• 当端口的缺省 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文，给报文添加端口缺省 VLAN 的 Tag • 当端口的缺省 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文	• 当报文的 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文 • 当报文的 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文	• 当报文的 VLAN ID 与端口的缺省 VLAN ID 相同，且是该端口允许通过的 VLAN ID 时：去掉 Tag，发送该报文 • 当报文的 VLAN ID 与端口的缺省 VLAN ID 不同，且是该端口允许通过的 VLAN ID 时：保持原有 Tag，发送该报文
Hybrid端口			当报文的VLAN ID是端口允许通过的VLAN ID时，发送该报文，并可以通过**port hybrid vlan**命令配置端口在发送该VLAN的报文时是否携带Tag

1.4.2 配置基于Access端口的VLAN

配置基于 Access 端口的 VLAN 有两种方法：一种是在 VLAN 视图下进行配置，另一种是在接口视图下进行配置。

表1-4 配置基于 Access 端口的 VLAN（在 VLAN 视图下）

配置	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-

配置	命令	说明
向当前VLAN中添加一个或一组Access端口	**port** *interface-list*	缺省情况下，系统将所有端口都加入到VLAN 1

表1-5 配置基于 Access 端口的 VLAN（在接口视图下）

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型为Access类型		**port link-type access**	缺省情况下，端口的链路类型为Access
将当前Access端口加入到指定VLAN		**port access vlan** *vlan-id*	缺省情况下，所有Access端口都属于VLAN 1 在将Access端口加入到指定VLAN之前，该VLAN必须已经存在

1.4.3 配置基于Trunk端口的VLAN

Trunk 端口可以允许多个 VLAN 通过，只能在接口视图下进行配置。

配置基于 Trunk 端口的 VLAN 时，需要注意：

- Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再配置为其他类型端口。
- 配置端口缺省 VLAN 后，必须使用 **port trunk permit vlan** 命令配置允许端口缺省 VLAN 的报文通过，接口才能转发端口缺省 VLAN 的报文。

表1-6 配置基于 Trunk 端口的 VLAN

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型为Trunk类型		**port link-type trunk**	缺省情况下，端口的链路类型为Access类型
允许指定的VLAN通过当前Trunk端口		**port trunk permit vlan** { *vlan-id-list* | **all** }	缺省情况下，Trunk端口只允许VLAN 1的报文通过
（可选）配置Trunk端口的缺省VLAN		**port trunk pvid vlan** *vlan-id*	缺省情况下，Trunk端口的缺省VLAN为VLAN 1

1.4.4 配置基于Hybrid端口的VLAN

Hybrid 端口可以允许多个 VLAN 通过，只能在接口视图下进行配置。

配置基于 Hybrid 端口的 VLAN 时，需要注意：

- Hybrid 端口和 Trunk 端口之间不能直接切换，只能先设为 Access 端口，再配置为其他类型端口。
- 在配置允许指定的 VLAN 通过 Hybrid 端口之前，允许通过的 VLAN 必须已经存在。
- 配置端口缺省 VLAN 后，必须使用 **port hybrid vlan** 命令配置允许端口缺省 VLAN 的报文通过，出接口才能转发端口缺省 VLAN 的报文。

表1-7 配置基于 Hybrid 端口的 VLAN

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	二层以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型为Hybrid类型		**port link-type hybrid**	缺省情况下，端口的链路类型为Access类型
允许指定的VLAN通过当前Hybrid端口		**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	缺省情况下，Hybrid端口只允许该端口在链路类型为Access时的所属VLAN的报文以Untagged方式通过
（可选）配置Hybrid端口的缺省VLAN		**port hybrid pvid vlan** *vlan-id*	缺省情况下，Hybrid端口的缺省VLAN为该端口在链路类型为Access时的所属VLAN

1.5 配置VLAN组

VLAN 组是一组 VLAN 的集合。VLAN 组内可以添加多个 VLAN 列表，一个 VLAN 列表表示一组 VLAN ID 连续的 VLAN。

表1-8 配置 VLAN 组

操作	命令	说明
进入系统视图	**system-view**	-
创建一个VLAN组，并进入VLAN组视图	**vlan-group** *group-name*	缺省情况下，不存在任何VLAN组
在当前VLAN组内添加VLAN成员	**vlan-list** *vlan-id-list*	缺省情况下，当前VLAN组中不存在任何VLAN列表

1.6 VLAN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 VLAN 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 VLAN 接口统计信息。

表1-9 VLAN 显示和维护

操作	命令
显示VLAN接口相关信息	**display interface vlan-interface** [*interface-number*] [**brief** [**description** | **down**]]
显示VLAN相关信息	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]
显示创建的VLAN组及其VLAN成员列表	**display vlan-group** [*group-name*]
显示设备上当前存在的Hybrid或Trunk端口	**display port** { **hybrid** | **trunk** }
清除VLAN接口的统计信息	**reset counters interface vlan-interface** [*interface-number*]

目 录

1 VLAN终结

1.1 VLAN终结简介

VLAN 终结是指对接收到的报文，按照报文携带的 VLAN Tag 信息匹配对应的接口后，去除报文 VLAN Tag，再将报文进行三层转发或交由其他业务处理。转发出去的报文是否带有 VLAN Tag 由出接口决定，对从配置了 VLAN 终结的接口发送的报文，按照该接口上的终结配置，将相应的 VLAN Tag 添加到报文中后发送该报文。

1.1.1 VLAN终结分类

根据对所终结的报文的不同处理方式，VLAN 终结分为以下四种：

- Dot1q 终结：用来终结带有一层及以上 VLAN Tag 的报文（要求最外层 VLAN ID 必须匹配配置值），从配置了 Dot1q 终结的接口发送的报文，都添加一层 VLAN Tag。
- Untagged 终结：用来终结收到的不带 VLAN Tag 的报文，从配置了 Untagged 终结的接口发送的报文，都不添加 VLAN Tag。
- Default 终结：用来终结同一主接口上其他子接口上无法处理的报文，从配置了 Default 终结的接口发送的报文，都不添加 VLAN Tag。

说明

为便于描述，本特性部分内容对带有两层及以上 VLAN Tag 的报文，将其最外两层 VLAN Tag 按从外层到内层的方向，分别用第一层 VLAN Tag、第二层 VLAN Tag 表示，对 VLAN ID 的描述类似。

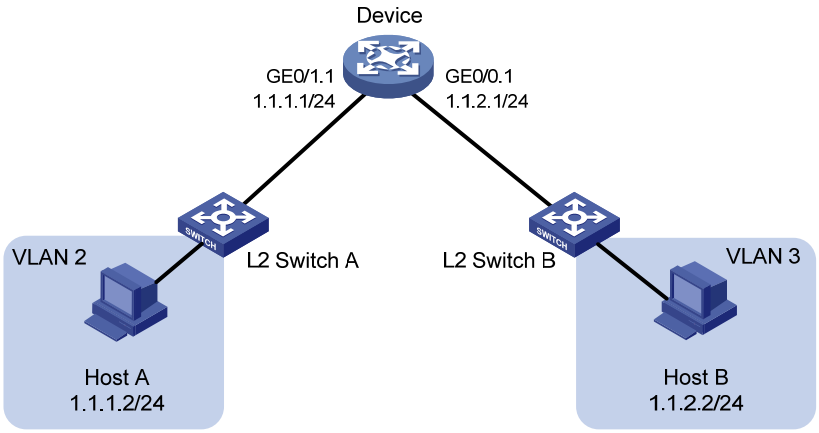
1.1.2 VLAN终结应用场景

1. 指定VLAN间的互通

划分 VLAN 后，不同 VLAN 间的主机不能直接通信，使用三层路由技术可以实现所有 VLAN 间报文的互通。此时如果要对互通的 VLAN 范围做限制，即要求只有指定的部分 VLAN 间可以互通，可以借助 VLAN 终结功能来实现。目前可以通过 VLAN 接口/三层以太网子接口实现指定 VLAN 间的互通。

如下图所示，Host A 属于 VLAN 2，Host B 属于 VLAN 3，将 Host A 的网关地址指定为 1.1.1.1/24，Host B 的网关地址指定为 1.1.2.1/24，就可以通过在三层以太网子接口 GigabitEthernet0/1.1 和 GigabitEthernet0/0.1 上配置 VLAN 终结来实现 Host A 和 Host B 之间的互通了。

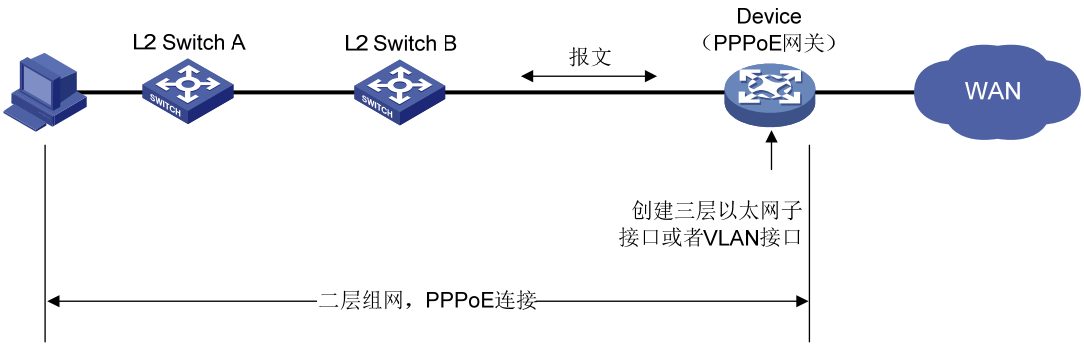
图1-1 VLAN 终结用于不同 VLAN 之间互通



2. 局域网和广域网的互联

局域网内的报文大多数都带有 VLAN Tag，但一些广域网协议并不能识别 VLAN 报文，比如 PPP 等，这种情况下，如果局域网的 VLAN 报文要转发到广域网，需要在本地记录并去掉报文的 VLAN 信息后再转发，可以借助 VLAN 终结功能来实现。目前可以通过 VLAN 接口/三层以太网子接口实现局域网和广域网的互联。

图1-2 VLAN 终结用于 LAN 和 WAN 的互联



1.2 VLAN终结配置任务简介

表1-1 VLAN 终结配置任务简介

配置任务		说明	详细配置
配置Dot1q终结	配置明确的Dot1q终结	请根据设备的支持情况选择一种方式	1.3.1
	配置模糊的Dot1q终结		1.3.2
配置Untagged终结			1.4
配置Default终结			1.5

配置任务	说明	详细配置
配置VLAN终结支持广播	可选	1.6
配置VLAN Tag的TPID值	可选	1.7

配置 VLAN 终结时，需要注意：

- 主接口本身不能对 VLAN 报文做终结处理，在主接口创建子接口后，由子接口来处理。
- VLAN 接口、三层以太网子接口、三层虚拟以太网子接口都可以终结匹配最外层 VLAN ID 的报文或匹配最外两层 VLAN ID 的报文。其中，VLAN 接口只能终结最外层 VLAN ID 与接口编号相同的 VLAN 报文，不能通过命令行修改，比如 Vlan-interface10 只能终结最外层 VLAN ID 为 10 的报文。
- 在三层以太网子接口/三层虚拟以太网子接口视图下修改已有的 VLAN 终结配置后，该子接口会 down/up 一次，设备 ARP 表中与该子接口相关的动态表项也会被全部删除。

配置 VLAN 终结后，对收到的报文按照如下优先级顺序匹配接口：

- 配置带 loose 属性的 QinQ 终结的子接口
- 配置 Dot1q 终结或者缺省支持 Dot1q 终结的子接口
- 配置带 loose 属性的 Dot1q 终结的子接口
- 配置 Untagged 终结的子接口
- 配置 Default 终结的子接口
- 主接口

说明

与 VLAN 接口绑定的主接口在收到 VLAN 报文后，根据 VLAN 接口的配置对报文进行处理。

1.3 配置Dot1q终结

根据每个子接口所能终结的 VLAN 报文中最外层 VLAN ID 范围的不同，Dot1q 终结分为：

- 明确的 Dot1q 终结：只允许接收最外层 VLAN ID 为指定值的 VLAN 报文，其他 VLAN 报文则不允许通过该子接口。收到报文后，将报文最外层 VLAN Tag 剥离。发送报文时，给报文添加一层 VLAN Tag，VLAN ID 为指定值。
- 模糊的 Dot1q 终结：只允许接收最外层 VLAN ID 在指定范围内的 VLAN 报文，不属于该范围的 VLAN 报文则不允许通过该子接口。收到报文后，将报文最外层 VLAN Tag 剥离。发送报文时，会给报文添加一层 VLAN Tag，VLAN ID 字段取值为：对于 PPPoE 报文，通过查找 PPPoE 会话表项获取相应的 VLAN ID。

1.3.1 配置明确的Dot1q终结

表1-2 配置明确的 Dot1q 终结

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网子接口视图	**interface** *interface-type interface-number.subnumber*	-
	三层虚拟以太网子接口视图	**interface virtual-ethernet** *interface-number.subnumber*	
使能当前接口的Dot1q终结功能，并指定当前子接口能够终结的VLAN报文最外层VLAN ID		**vlan-type dot1q vid** *vlan-id* [**loose**]	-

1.3.2 配置模糊的Dot1q终结

表1-3 配置模糊的 Dot1q 终结

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网子接口视图	**interface** *interface-type interface-number.subnumber*	-
	三层虚拟以太网子接口视图	**interface virtual-ethernet** *interface-number.subnumber*	
使能当前接口的Dot1q终结功能，并指定当前子接口能够终结的VLAN报文的最外层VLAN ID范围		**vlan-type dot1q vid** *vlan-id-list* [**loose**]	-

1.4 配置Untagged终结

表1-4 配置 Untagged 终结

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网子接口视图	**interface** *interface-type interface-number.subnumber*	-
	三层虚拟以太网子接口视图	**interface virtual-ethernet** *interface-number.subnumber*	
使能当前接口的Untagged终结功能，使当前接口可以处理不带VLAN Tag的报文		**vlan-type dot1q untagged**	-

1.5 配置Default终结

表1-5 配置 Default 终结

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网子接口视图	**interface** *interface-type interface-number.subnumber*	-
	三层虚拟以太网子接口视图	**interface virtual-ethernet** *interface-number.subnumber*	
使能当前接口的Default终结功能，使当前接口可以处理其他子接口都无法处理的报文		**vlan-type dot1q default**	-

1.6 配置VLAN终结支持广播

当接口下配置了模糊的 Dot1q 终结功能后，不允许发送广播报文。只有配置了 VLAN 终结支持广播功能，这些接口才能发送广播报文。

表1-6 配置 VLAN 终结支持广播

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网子接口视图	**interface** *interface-type interface-number.subnumber*	-
	三层虚拟以太网子接口视图	**interface virtual-ethernet** *interface-number.subnumber*	
	VLAN接口视图	**interface vlan-interface** *interface-number*	
配置允许当前接口发送广播报文		**vlan-termination broadcast enable**	缺省情况下，当前接口配置了模糊的Dot1q终结或者模糊的QinQ终结功能后，不允许发送广播报文

1.7 配置VLAN Tag的TPID值

如果要在三层以太网子接口/三层虚拟以太网子接口/VLAN 接口上使用 VLAN 终结功能，可以通过以下配置指定接口接收和发送报文的最外层 VLAN Tag 的 TPID 值。在配置 TPID 值后，当接收报文时，只有报文最外层 VLAN Tag 的 TPID 值为 0x8100 或者指定值的报文才会作为 VLAN 报文来处理；发送报文时，会给报文最外层 VLAN Tag 的 TPID 值填入指定值，如果报文带有两层及以上 VLAN Tag，则给报文其他层 VLAN Tag 的 TPID 值都填入 0x8100。

表1-7 配置 VLAN Tag 的 TPID 值

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图	三层以太网接口视图	**interface** *interface-type interface-number*	在三层以太网接口、三层虚拟以太网接口或L3VE视图下配置，会对相应接口的所有子接口生效；在VLAN接口视图下配置，会对该VLAN接口生效
	三层虚拟以太网接口视图	**interface virtual-ethernet** *interface-number*	
	VLAN接口视图	**interface vlan-interface** *interface-number*	
配置当前接口接收和发送的报文最外层VLAN Tag的TPID值		**dot1q ethernet-type** *hex-value*	缺省情况下，当前接口接收和发送的报文最外层VLAN Tag的TPID值均为0x8100

目 录

1 二层转发

1.1 配置普通二层转发

1.1.1 普通二层转发的工作机制

如果设备接收到的报文的目的 MAC 地址匹配三层接口的 MAC 地址，则通过设备的三层接口进行三层转发；否则通过设备的二层接口进行二层转发。

二层转发根据报文的目的 MAC 地址查找 MAC 地址表，得到报文的出接口，然后将报文发送出去。

普通二层转发是设备默认启用的特性，不需要配置。

1.1.2 普通二层转发显示和维护

在任意视图下执行 **display** 命令可以显示二层转发过程中的统计信息，查看转发的结果。

在用户视图下执行 **reset** 命令可以清除二层转发的统计信息。

表1-1 普通二层转发显示和维护

操作	命令
显示二层转发统计信息	**display mac-forwarding statistics** [**interface** *interface-type interface-number*]
清除二层转发统计信息	**reset mac-forwarding statistics**

1.2 配置快速二层转发

1.2.1 快速二层转发的工作机制

快速二层转发采用高速缓存来处理报文，采用了基于数据流的技术，可以大大提高转发效率。

快速二层转发用源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号、输入接口号、输出接口号和 VLAN 来标识一条数据流。在二层转发过程中，会根据设备规则，对需要进行三层业务处理的报文，获取其 IP 地址等信息，生成 IP 快速转发表。

1.2.2 快速二层转发显示和维护

在任意视图下执行 **display** 命令可以显示快速二层转发表信息。

表1-2 快速二层转发显示和维护

操作	命令
显示IP快速转发表信息	**display mac-forwarding cache ip** [*ip-address*]
显示分片报文快速转发表信息	**display mac-forwarding cache ip fragment** [*ip-address*]