VLAN配置

目 录

第 1 章 VLAN配置 - 1 -
1.1 VLAN概述 - 1 -
1.2 Dot1Q Tunnel概述 - 1 -
1.2.1 前言 - 1 -
1.2.2 Dot1Q Tunnel实现方式 - 2 -
1.2.3 TPID值可修改特性 - 2 -
1.3 VLAN配置任务列表 - 3 -
1.4 VLAN配置任务 - 3 -
1.4.1 添加/删除VLAN - 3 -
1.4.2 配置交换机端口 - 3 -
1.4.3 创建/删除VLAN 接口 - 4 -
1.4.4 配置Super VLAN接口 - 4 -
1.4.5 监控VLAN的配置和状态 - 5 -
1.4.6 开启/关闭全局Dot1Q Tunnel和配置全局TPID - 5 -
1.4.7 配置端口下的VLAN翻译模式和表项 - 6 -
1.5 配置示例 - 6 -
1.5.1 SuperVLAN配置示例 - 6 -
附录A 缩略语 - 8 -

第1章 VLAN配置

1.1 VLAN概述

VLAN(Virtual Local Area Network)，即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分的交换网络。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案。VLAN 技术允许将一个物理的 LAN 逻辑地划分成不同的广播域（VLAN），每一个 VLAN 都包含一组有着相同需求的设备，与物理上形成的 LAN 有着相同的属性，但由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个设备无须被放置在同一个物理空间，即，这些设备不一定属于同一个物理 LAN 网段，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络安全。

- 支持基于端口的 VLAN
- 端口支持 802.1Q 的中继模式
- 支持访问型端口

  基于端口的 VLAN，就是将端口归属到交换机支持的 VLAN 的一个子集中。如果这个 VLAN 子集只有一个 VLAN，那么该端口就是访问模式（access）端口；如果这个 VLAN 子集中有多个 VLAN，该端口为中继（trunk）端口，其中有一个默认的 VLAN，它是该端口的 native VLAN，该 VLAN ID 就是 Port VLAN ID（PVID）。
- 支持端口 VLAN 的范围控制

  vlan-allowed 参数用于控制端口所归属的 VLAN 范围；vlan-untagged 参数用于控制端口发送不加上 VLAN 标签的报文到相应的 VLAN。

1.2 Dot1Q Tunnel概述

1.2.1 前言

Dot1Q Tunnel 是对基于 802.1 Q 封装的隧道协议的一种形象化的称呼，定义在 IEEE 802.1ad 中。其核心思想是将用户私网 VLAN tag 封装到公网 VLAN tag 上，报文带着两层 tag 穿越服务商的骨干网络，从而为用户提供一种较为简单的二层 VPN 隧道。Dot1Q Tunnel 协议是一种简单而易于管理的协议，它不需要信令的支持，仅仅通过静态配置即可实现，特别适用于小型的，以三层交换机为骨干的企业网或小规模城域网。

Dot1Q Tunnel 特性正好满足了这部分用户的需求，它提供了一种廉价、简洁的二层 VPN 解决方案，越来越多的小型用户倾向于使用该功能构建自己的 VPN 网络。在运营商网络的内部，P 设备也无需支持 Dot1Q Tunnel 功能，即传统的三层交换机完全可以满足需求，极大地保护了运营商的投资。

- 支持全局开启 Dot1Q Tunnel。
- 支持基本下连口的配置。
- 支持下连口对 Customer VLAN 与 SPVLAN 的相互翻译，包括支持平直（Flat）模式的翻译和双标签（QinQ）模式的翻译。
- 支持上连口的配置。

- 支持可变 TPID。

1.2.2 Dot1Q Tunnel实现方式

Dot1Q Tunnel 实现方式一种是基于端口的 Dot1Q Tunnel，一种是基于内层 CVLAN Tag 分类的 Dot1Q Tunnel。

1) 基于端口的 Dot1Q Tunnel：

当该设备端口接收到报文，无论报文是否带有 VLAN Tag，交换机都会为该报文打上本端口默认 VLAN 的 VLAN Tag。这样，如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为 Double Tag 的报文；如果接收到的是 untagged 的报文，该报文就成为带有端口默认 VLAN Tag 的报文。

带单层 VLAN Tag 的报文结构如图 1 所示：

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

图1 带单层VLAN Tag的报文

带双层 VLAN Tag 的报文结构如图 2 所示：

DA (6B)	SA (6B)	**ETYPE(8100) (2B)**	**SPVLAN Tag (2B)**	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

图2 封装了外层VLAN Tag的报文

2) 基于内层 CVLAN Tag 分类的 Dot1Q Tunnel：

根据 Dot1Q Tunnel 的内层 CVLAN Tag 的 CVLAN ID 区间实现业务分流。可以讲 CVLAN 区间翻译为某 SPVLAN ID，有 Flat VLAN 翻译和 QinQ VLAN 翻译两种模式。在 QinQ VLAN 翻译模式下，当同一用户不同业务使用不同的 CVLAN ID 时，可以根据 CVLAN ID 区间进行分流，比如宽带业务的 CVLAN ID 范围是 101～200，VOIP 业务的 CVLAN ID 范围是 201～300，IPTV 业务的 CVLAN ID 范围是 301～400，PE 设备收到用户数据后，根据 CVLAN ID 范围，对宽带业务打上 SPVLAN ID 为 1000 的 SPVLAN Tag，对 VOIP 打上 SPVLAN ID 为 2000 的 SPVLAN Tag，对 IPTV 打上 SPVLAN ID 为 3000 的 SPVLAN Tag。在 Flat VLAN 翻译模式与 QinQ VLAN 翻译模式的区别是，Flat VLAN 翻译模式中 SPVLAN Tag 不是叠加在 CVLAN Tag 外层，而是直接替换 CVLAN Tag，并且只支持将 CVLAN 与 SPVLAN 的一对一翻译。

1.2.3 TPID值可修改特性

IEEE 802.1Q 协议定义的以太网帧的 Tag 报文结构如下：

TPID	User Priority	CFI	VLAN ID
2 byte	3 bit	1 bit	12 bit

图3 以太网帧的VLAN Tag报文结构

TPID 是 VLAN Tag 中的一个字段，IEEE 802.1Q 协议规定该字段的取值为 0x8100。交换机缺省采用协议规定的 TPID 值（0x8100）。某些厂商的设备将 Dot1Q Tunnel 报文外层 Tag 的 TPID 值设置为非 0x8100。为了和这些设备兼容，BDCOM 绝大部分交换机提供了 Dot1Q Tunnel 报文 TPID 值可修改功能。PE 设备的 TPID 值可以由用户自行配置，这些设备的端口收到报文时会将报文外层 VLAN Tag 中的 TPID 值替

换为用户设定值再进行发送，从而使发送到公网中的 Dot1Q Tunnel 报文可以被其他厂商的设备识别。

1.3 VLAN配置任务列表

- 添加/删除 VLAN
- 配置交换机端口
- 创建/删除 VLAN 接口
- 配置 superVLAN 接口
- 监控 VLAN 的配置和状态
- 配置基于 VLAN 的访问控制模型
- 开启/关闭全局 Dot1Q Tunnel 和配置全局 TPID
- 配置端口下的 VLAN 翻译模式和表项

1.4 VLAN配置任务

1.4.1 添加/删除VLAN

VLAN 是一个按不同功能、不同项目组或不同的应用进行逻辑划分的交换网络，不区分这些用户的物理位置。 VLAN 拥有与物理局域网相类似的属性，利用 VLAN 可以将不在同一物理局域网的终端划分到一个 VLAN 组中。一个 VLAN 可以拥有多个端口，而所有的单播、组播、广播数据报文只能在同一个 vlan 中进行转发、扩散到终端。每一个 VLAN 就是一个逻辑上的网络，一个数据报文要到达另外一个 VLAN，则必须通过路由或桥转发。

使用下面的命令进行 vlan 的配置：

命令	目的
vlan *vlan-id*	进入到VLAN的配置模式。
name *str*	VLAN配置模式下的命名。
Exit	退出VLAN配置模式，同时创建该VLAN。
vlan *vlan-range*	同时创建多个VLAN
no vlan *vlan-id* | *vlan-range*	删除一个或多个VLAN

Vlan 也可以通过 VLAN 管理协议 GVRP 进行动态的添加删除。

1.4.2 配置交换机端口

交换机端口支持以下几种模式：访问模式、中继模式、VLAN 隧道模式、VLAN 翻译型隧道模式和 VLAN 隧道上连口模式。

- 访问模式表示该端口只从属于一个 VLAN，并且只发送和接收无标签的以太网帧。
- 中继模式表示该端口与其它交换机相连，可以发送和接收带标签的以太网帧。
- VLAN 隧道模式是基于访问模式的子模式。该端口收到的报文无论是否带有 VLAN tag，都认为其不带 tag，并由交换芯片自动加上该端口的 pvid 作为新 tag，

有的机型还支持在下连口修改新 tag 的 TPID 值。交换机从而能够忽略接入网络中的不同 vlan 划分，而将报文原样传递到同一客户在另外一个端口的另一个子网络中，实现透明传输。

- VLAN 翻译型隧道模式是基于中继模式的子模式。该端口根据收到报文的 VLAN tag，查找 VLAN 翻译表得到对应的 SPVLAN，并由交换芯片用 SPVLAN 替换原 tag 或者在原 tag 外层添加 SPVLAN tag。报文从该端口出来时，会将 SPVLAN 替换为原 tag 或者强制除去 SPVLAN tag。交换机从而能够忽略接入网络中的不同 vlan 划分，而将报文原样传递到同一客户在另外一个端口的另一个子网络中，实现透明传输。
- VLAN 隧道上连口模式是基于中继模式的子模式。报文从该端口出去时，应该配置 SPVLAN不在 untagged 的范围，保证所有报文原封不动的出去。报文从该端口进来时，会对报文的 TPID 进行检查，如果发现不符，或者是 untagged 的报文，则会强制加上包含自己的 TPID 的 SPVLAN tag 作为报文的外层标签。

每一个端口都有一个默认的 VLAN 及 PVID，端口下接收到的所有的没有 VLAN 标签的数据都是属于该 VLAN 的数据报文。

中继模式可以将端口归属于多个 VLAN，同时也可以配置转发何种报文和所属的 VLAN 的数量，即端口发送的报文是 Tagged 还是 unTagged，以及端口所属的 VLAN list。

使用如下的命令可以配置交换机端口：

命令	目的
switchport pvid *vlan-id*	配置交换机端口的PVID。
switchport mode {access | trunk | dot1q-tunnel *tpid* **| dot1q-tunnel-uplink** *tpid* **| dot1q-translating-tunnel}**	配置交换机端口的端口模式。
switchport trunk vlan-allowed …	配置交换机端口的VLAN归属范围。
switchport trunk vlan-untagged …	配置交换机端口的unTagged的VLAN范围。

1.4.3 创建/删除VLAN 接口

为了实现网络管理或三层的路由功能，可以创建 VLAN 接口上，该接口可以指定 IP 地址和掩码，使用如下的命令可以配置 VLAN 接口：

命令	目的
[no] interface vlan *vlan-id*	创建/删除一个VLAN接口。

1.4.4 配置Super VLAN接口

Super VLAN 接口只在三层交换机上支持。

Super VLAN 技术提供了这样一种机制：使处于同一个交换机不同 VLAN 中的主机能够实现分配在相同的 Ipv4 子网中进而使用相同的默认网关，这样可以节省大量的 IP 地址。Super VLAN 技术将多个不同的 VLAN 划分为一组，这组 VLAN 使用相同的管理接口；组内的主机使用相同的 IPv4 网段和网关。属于 Super VLAN 的 VLAN 称为 SubVLAN，任何 SubVLAN 不能通过配置 IP 地址而拥有管理接口。

可以通过命令行配置一个 Super VLAN 接口；配置 Super VLAN 接口步骤如下：

命令	说明
[no] interface supervlan *index*	进入该Super VLAN接口的接口配置模式。如果指定Super VLAN接口不存在，系统将创建该Super VLAN接口。 index为Super VLAN接口的索引，有效范围1~32。 no前缀表示删除该Super VLAN接口。
[**no**] **subvlan** [*setstr*] [**add** *addstr*] [**remove** *remstr*]	配置该Super VLAN下的SubVlan。被增加的Sub VLAN不能拥有管理接口，也不能属于其它的Super VLAN。初始状况下Super VLAN中不包含任何Sub VLAN。每次只能使用一个子命令 setstr表示设置Sub VLAN列表，Sub VLAN列表；例如列表2,4-6表示VLAN2、4、5、6。 add表示在原有Sub VLAN列表中新增VLAN列表，addstr为列表字符串，格式同上。 remove表示从原有SubVLAN列表中删除的VLAN的列表，remstr为列表字符串，格式同上。 no命令表示删除该SuperVLAN下的所有SubVLAN。no命令不能与任何其他子命令同时使用。

配置完成 Super VLAN 接口后，用户可以为该 Super VLAN 接口配置 IP 地址等；Super VLAN 接口也是一种路由端口，可以进行任何路由端口下的配置。

1.4.5 监控VLAN的配置和状态

为了监控 VLAN 及其 Dot1Q Tunnel 的配置和状态，可以在管理模式下使用下面的命令：

命令	目的
show vlan [id *x* **| interface** *intf* **| dot1q-tunnel [interface** *intf***]]**	显示VLAN或者Dot1Q Tunnel的配置和状态。
show interface {vlan | supervlan} *x*	显示vlan端口/supervlan端口的状态。

1.4.6 开启/关闭全局Dot1Q Tunnel和配置全局TPID

全局开启 Dot1Q Tunnel 后，对于一些单机、高端交换机系列的 LS24GE、LS48GE、LS2TE 线卡，他们所有的端口会默认成为 Dot1Q Tunnel 下连端口，对进入的报文强制加上 SPVLAN tag。

配置全局 TPID 后，报文从交换机的上连端口出来时会修改 SPVLAN tag 的 TPID 为所设置的全局 TPID，报文进入上连口时，会识别其 SPVLAN tag 是否为所设置的全局 TPID，如果不符，或者是 untagged 的报文，则会强制加上包含自己的 TPID 的 SPVLAN tag 作为报文的外层标签。

全局启用 dot1q-tunnel 和全局 TPID 的命令是：

命令	目的

dot1q-tunnel *tpid*	配置交换机全局的dot1q-tunnel特性和全局TPID。

1.4.7 配置端口下的VLAN翻译模式和表项

VLAN 翻译模式和 VLAN 翻译表项配置后，会在端口模式 dot1q-translating-tunnel 下生效。翻译模式分为 2 种：Flat 模式和 QinQ 模式。Flat 模式会将进入 dot1q-translating-tunnel 下连端口的报文的 CVLAN tag 作为索引，查找 VLAN 翻译表，将查找到的 SPVLAN 替换 CVLAN，报文从此端口出来时，会再进行 SPVLAN 到 CVAN 的转换。QinQ 模式会将进入 dot1q-translating-tunnel 下连端口的报文的 CVLAN tag 作为索引，查找 VLAN 翻译表，将查找到的 SPVLAN 形成 SPVLAN tag 叠加在 CVLAN tag 外层，报文从此端口出来时，会除去 SPVLAN tag。端口下默认的 VLAN 翻译模式为 QinQ。

在端口下配置 VLAN 翻译表项时，Flat 模式仅可以配置 CVLAN 与 SPVLAN 的一一映射。QinQ 模式可以配置 CVLAN 与 SPVLAN 的多对一映射。

配置 VLAN 翻译模式和表项的命令是：

命令	目的
switchport dot1q-translating-tunnel {mode [flat | qinq] | translate {*oldvlanlist* **|** *oldvlanid***} *newvlan* [***priority***]}**	配置VLAN翻译模式和表项。

1.5 配置示例

1.5.1 SuperVLAN配置示例

有如下网络环境：

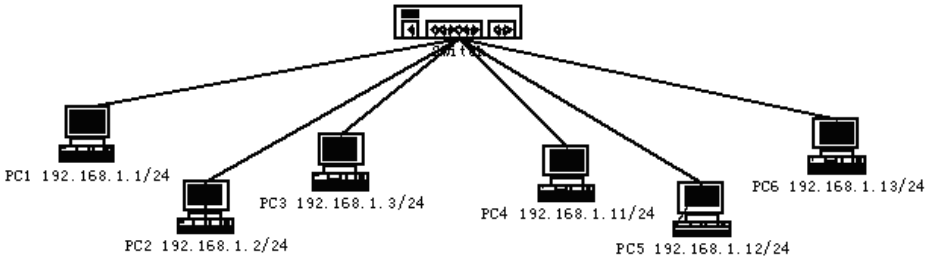

图 8 SuperVLAN 示意图

用户 PC1~ PC6 连接在交换机 1~6 端口下，这些 PC 机的 ip 地址同属于 192.168.1.0/24 网段。要求 PC1~PC6 相互之间可以互相 PING 通，并且可以通过 ip 地址 192.168.1.100 对交换机进行管理，但是 PC1~PC3 与 PC4~PC6 两组机器处在不同的二层广播域内。这样可以将 1~3 端口配置到 VLAN 1，将 4~6 端口配置到 VLAN 2，将 VLAN 1、2 增加为同一个 SuperVlan 的 SubVlan；需要在交换机上进行如下的配置：

```
interface fastethernet 0/4
switchport pvid 2
!
interface fastethernet 0/5
switchport pvid 2
```

```
!
interface fastethernet 0/6
switchport pvid 2
!
interface supervlan 1
subvlan 1,2
ip address 192.168.1.100 255.255.255.0
ip proxy-arp subvlan
!
```

附录A 缩略语

英文缩写	英文全称	中文全称
VPN	Virtual Private Network	虚拟专用网络
TPID	Tag Protocol Identifier	标签协议标识符
QoS	Quality of Service	服务质量
P	provider bridged network core	提供商桥网核心设备
PE	provider bridged network edge	提供商桥网边缘设备
CE	customer network edge	用户网络边缘设备
UNI	user-network interface	用户-网络接口
NNI	network-network interface	网络-网络接口
CVLAN	Customer VLAN	用户 VLAN
SPVLAN	Service provider VLAN	服务提供商 VLAN