

PVLAN对比VLAN的优势及配置实例 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/250/2021_2022_PVLAN_E5_AF_B9_E6_AF_c101_250983.htm 交换机是网络的核心设备之一，其技术发展非常迅速，从10Mbit/s以太网、100Mbit/s快速以太网，进而发展到吉比特和10吉比特以太网。交换机在通信领域和企业中的应用向纵深发展，网络管理人员对掌握专用虚拟局域网PVLAN技术的需求也越来越迫切。本文通过实践经验对这方面的应用进行总结。VLAN的局限性随着网络的迅速发展，用户对于网络数据通信的安全性提出了更高的要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性；传统的解决方法是给每个客户分配一个VLAN和相关的IP子网，通过使用VLAN，每个客户被从第2层隔离开，可以防止任何恶意的行为和Ethernet的信息探听。然而，这种分配每个客户单一VLAN和IP子网的模型造成了巨大的可扩展方面的局限。这些局限主要有下述几方面。

(1) VLAN的限制：交换机固有的VLAN数目的限制；(2) 复杂的STP：对于每个VLAN，每个相关的Spanning Tree的拓扑都需要管理；(3) IP地址的紧缺：IP子网的划分势必造成一些IP地址的浪费；(4) 路由的限制：每个子网都需要相应的默认网关的配置。PVLAN技术现在有了一种新的VLAN机制，所有服务器在同一个子网中，但服务器只能与自己的默认网关通信。这一新的VLAN特性就是专用VLAN (Private VLAN)。在Private VLAN的概念中，交换机端口有三种类型：Isolated port，Community port，Promisc-uous port；它们分别对应不同的VLAN类型：Isolated port属于Isolated PVLAN

，Community port属于Community PVLAN，而代表一个Private VLAN整体的是Primary VLAN，前面两类VLAN需要和它绑定在一起，同时它还包括Promiscuous port.在Isolated PVLAN中，Isolated port只能和Promiscuous port通信，彼此不能交换流量；在Community PVLAN中，Community port不仅可以和Promiscuous port通信，而且彼此也可以交换流量

。Promiscuous port与路由器或第3层交换机接口相连，它收到的流量可以发往Isolated port和Community port.PVLAN的应用对于保证接入网络的数据通信的安全性是非常有效的，用户只需与自己的默认网关连接，一个PVLAN不需要多个VLAN和IP子网就提供了具备第2层数据通信安全性的连接，所有的用户都接入PVLAN，从而实现了所有用户与默认网关的连接，而与PVLAN内的其他用户没有任何访问。PVLAN功能可以保证同一个VLAN中的各个端口相互之间不能通信，但可以穿过Trunk端口。这样即使同一VLAN中的用户，相互之间也不会受到广播的影响。PVLAN的配置步骤

- (1) Put switch in VTP transparent mode
set vtp mode transparent
- (2) Create the primary private VLAN
set vlan vlan pvlan-type primary
- (3) Set the isolated or community VLAN (s)
set vlan vlan pvlan-type {isolated | community}
- (4) Map the secondary VLAN (s) to the primary VLAN
set pvlan primary_vlan {isolated_vlan | community_vlan} {mod/port | sc0}
- (5) Map each secondary VLAN to the primary VLAN on the promiscuous port (s)
set pvlan mapping primary_vlan {isolated_vlan | community_vlan} {mod/port} [mod/port ...]
- (6) Show PVLAN configuration
show pvlan [primary_vlan] show pvlan mapping show vlan

[primary_vlan] show port 例子 下面给出一个正在网络中运行的交换机的PVLAN的相关配置，仅供参考。其中，VLAN 100是Primary VLAN，VLAN 101是Isolated VLAN，VLAN 102和VLAN 103是Community VLAN.

```
N8-CSSW-2> (enable) show running-config
This command shows non-default configurations only.
set system name N8-CSSW-2
#vtp set vtp domain sdunicom
set vtp mode transparent
set vlan 1 name default type ethernet mtu 1500
said 100001 state active
set vlan 100 name VLAN0100 type ethernet
pvlantype primary mtu 1500 said 100100 state active
set vlan 101 name VLAN0101 type ethernet
pvlantype isolated mtu 1500 said 100101 state active
set vlan 102 name VLAN0102 type ethernet
pvlantype community mtu 1500 said 100102 state active
set vlan 103 name VLAN0103 type ethernet
pvlantype community mtu 1500 said 100103 state active
#module 2 : 50-port 10/100/1000 Ethernet
set pvlan 100 101 2/26-29,2/35-36,2/42-43
set pvlan mapping 100 101 2/49
set pvlan 100 102 2/1-13,2/30-34
set pvlan mapping 100 102 2/49
set pvlan 100 103 2/14-25
set pvlan mapping 100 103 2/49
end
```

N8-CSSW-2> (enable) show pvlan

Primary	Secondary	Secondary-Type	Ports
100	101	isolated	2/26-29,2/35-36,2/42-43
100	102	community	2/1-13,2/30-34
100	103	community	2/14-25

目前很多厂商生产的交换机支持PVLAN技术，PVLAN技术在解决通信安全、防止广播风暴和浪费IP地址方面的优势是显而易见的，而且采用PVLAN技术有助于网络的优化，再加上PVLAN在交换机上的配置也相对简单，PVLAN技术越来越得到网络管理人员的青睐。

100Test 下载频道开通，各类考试题目直接下载。详细

请访问 www.100test.com