

Private VLAN Settings

(GTL-2091)



Digital Data Communications GmbH, Germany.

<http://www.level1.com>

Table of Contents

Chapter 1 Private VLAN Settings	3
1.1 Overview of Private VLAN	3
1.2 Private VLAN Type and Port Type in Private VLAN	3
1.2.1 Having One Primary VLAN Type	3
1.2.2 Having Two Secondary VLAN Types	3
1.2.3 Port Types Under the Private VLAN Port	3
1.2.4 Modifying the Fields in VLAN TAG	4
1.3 Private VLAN Configuration Task List	4
1.4 Private VLAN Configuration Tasks	4
1.4.1 Configuring Private VLAN	4
1.4.2 Configuring the Association of Private VLAN Domains	5
1.4.3 Configuring the L2 Port of Private VLAN to Be the Host Port	5
1.4.4 Configuring the L2 Port of Private VLAN to Be the Promiscuous Port	5
1.4.5 Modifying Related Fields of Egress Packets in Private VLAN	6
1.4.6 Displaying the Configuration Information of Private VLAN	6
1.5 Configuration Example	6

Chapter 1 Private VLAN Settings

1.1 Overview of Private VLAN

Private VLAN has settled the VLAN application problems facing ISPs: If ISP provides each user with a VLAN, the support by each device of 4094 VLANs will restrict the total of ISP-supported users.

1.2 Private VLAN Type and Port Type in Private VLAN

Private VLAN subdivides the L2 broadcast domain of a VLAN into multiple sub-domains, each of which consists of a private VLAN pair: a primary VLAN and a secondary VLAN. One private VLAN domain may have multiple private VLAN pairs and each private VLAN pair stands for a sub-domain. There is only one primary VLAN in a private VLAN domain and all private VLAN pairs share the same primary VLAN. The IDs of secondary VLANs in each sub-domain differ with each other.

1.2.1 Having One Primary VLAN Type

- **Primary VLAN:** It is relevant to a promiscuous port and only one primary VLAN exists in the private VLAN. Each port in the primary VLAN is a member in the primary VLAN.

1.2.2 Having Two Secondary VLAN Types

- **Isolated VLAN:** No layer-2 communication can be conducted between two ports in the same isolated VLAN. Also, there is only one isolated VLAN in a private VLAN. The isolated VLAN must be related with the primary VLAN.
- **Community VLAN:** Layer-2 communication can be conducted between two ports in the same VLAN, but they have no communication with the ports in another community VLAN. One private VLAN may contain multiple community VLANs. The community VLAN must be related with the primary VLAN.

1.2.3 Port Types Under the Private VLAN Port

- **Promiscuous port:** it belongs to the primary VLAN. It can communicate with all other ports, including the isolated port and community port of a secondary VLAN in the same private VLAN.
- **Isolated port:** It is the host port in the isolated VLAN. In the same private VLAN, the isolated port is totally L2 isolated from other ports except the promiscuous port, so the flows received from the isolated port can only be forwarded to the promiscuous port.

- Community port: It is the host port in the community VLAN. In a private VLAN, the community ports of the same community VLAN can conduct L2 communication each other or with the promiscuous port, but not with the community ports of other VLANs and the isolated ports in the isolated VLANs.

1.2.4 Modifying the Fields in VLAN TAG

This functionality supports to modify the VLAN ID and priority in VLAN tag and decides whether the egress packets of private VLAN carry the tag or not.

1.3 Private VLAN Configuration Task List

- Configuring Private VLAN
- Configuring the association of private VLAN domains
- Configuring the L2 port of private VLAN to be the host port
- Configuring the L2 port of private VLAN to be the promiscuous port
- Modifying related fields of egress packets in private VLAN
- Displaying the configuration information of private VLAN

1.4 Private VLAN Configuration Tasks

The conditions for a private VLAN peer to take effect are listed below:

1. Having the primary VLAN
2. Having the secondary VLAN
3. Having the association between primary VLAN and secondary VLAN
4. Having the promiscuous port in primary VLAN

1.4.1 Configuring Private VLAN

Use the following commands to set VLAN to be a private VLAN.

Command	Purpose
vlan <i>vlan-id</i>	Enters the VLAN mode.
private-vlan {primary community isolated}	Configures the features of private VLAN.
no private-vlan {primary community isolated}	Deletes the features of private VLAN.
show vlan private-vlan	Displays the configuration of private VLAN.
exit	Exits from Vlan configuration mode.

1.4.2 Configuring the Association of Private VLAN Domains

Run the following commands to associate the primary VLAN and the secondary VLAN.

Command	Purpose
vlan <i>vlan-id</i>	Enters the primary VLAN configuration mode.
private-vlan association { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	Sets the to-be-associated secondary VLAN.
no private-vlan association	Clears all associations between the current primary VLAN and all secondary VLANs.
exit	Exits the VLAN configuration mode.

1.4.3 Configuring the L2 Port of Private VLAN to Be the Host Port

Run the following commands to set the L2 port of private VLAN to be the host port:

Command	Purpose
Interface <i>interface</i>	Enters the interface configuration mode.
switchport mode private-vlan host	Sets the layer-2 port to be in host's port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan host-association <i>p_vid</i> <i>s_vid</i>	Associates the L2 host port with private VLAN.
no switchport private-vlan host-association	Deletes the association between L2 host port and private VLAN.
exit	Exits from the interface configuration mode.

1.4.4 Configuring the L2 Port of Private VLAN to Be the Promiscuous Port

Run the following commands to set the L2 port of private VLAN to be the promiscuous port:

Command	Purpose
Interface <i>interface</i>	Enters the interface configuration mode.
switchport mode private-vlan promiscuous	Sets the layer-2 port to be in promiscuous port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan mapping <i>p_vid</i> { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	Associates the L2 promiscuous port with private VLAN.
no switchport private-vlan mapping	Deletes the association between L2 promiscuous port and private VLAN.
exit	Exits from the interface configuration mode.

1.4.5 Modifying Related Fields of Egress Packets in Private VLAN

Run the following commands to modify related fields of the egress packets in private VLAN:

Command	Purpose
Interface <i>interface</i>	Enters the interface configuration mode.
switchport private-vlan tag-pvid <i>vlan-id</i>	Sets the VLAN ID field in the tag of egress packet.
switchport private-vlan tag-pri <i>pri</i>	Sets the priority field in the tag of egress packet.
[no] switchport private-vlan untagged	Sets whether the egress packets have the tag or not.
exit	Exits from interface configuration mode.

1.4.6 Displaying the Configuration Information of Private VLAN

Run the following commands in global, interface or VLAN configuration mode to display the private VLAN configuration information of private VLAN and L2 port:

Command	Purpose
show vlan private-vlan	Displays the configuration of private VLAN.
show vlan private-vlan interface <i>interface</i>	Displays the configuration of the L2 port in the private VLAN.

1.5 Configuration Example

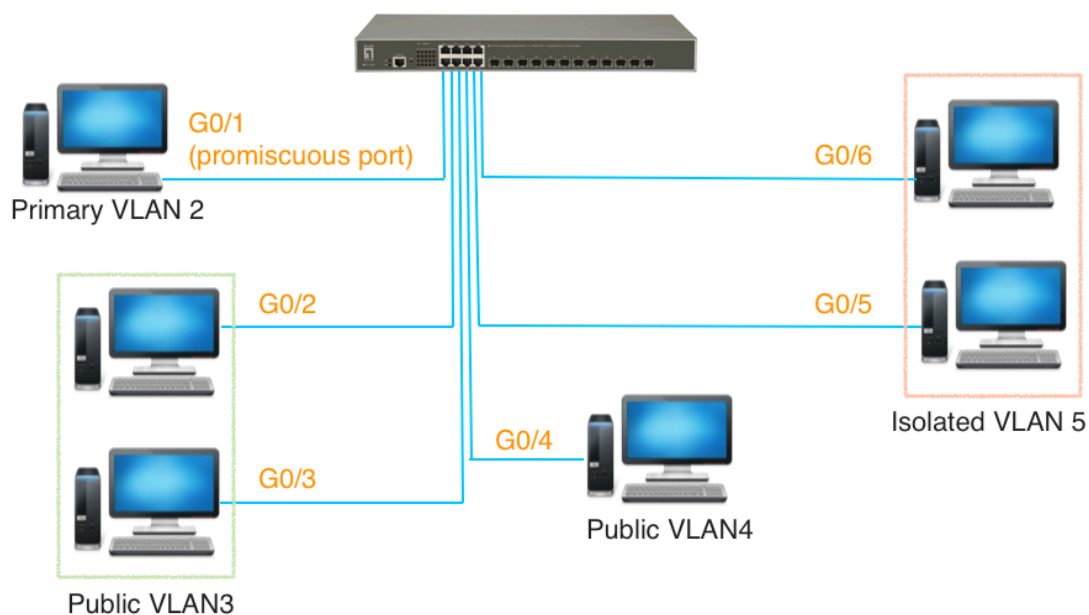


Figure 1: Typical Configuration of Private VLAN

As shown in figure 1, port G0/1 is the promiscuous port in primary VLAN 2 and ports G0/2-G0/6 are host ports, among which ports G0/2 and G0/3 are host ports (public ports) of Community VLAN 3, port G0/4 is that of Community VLAN 4, and ports G0/5 and G0/6 are host ports of Isolated VLAN 5.

According to the definition of private VLAN, L2 communication can be conducted between promiscuous port G0/1 and host ports of all sub-VLAN domains, so it is between host ports G0/2 and G0/3 of community VLAN 3, but they cannot conduct L2 communication with other host ports of secondary VLANs. L2 communication cannot go on between ports G0/5 and G0/6 in Isolated VLAN 5, but the two ports can conduct L2 communication with promiscuous port G0/1.

The commands requiring to be entered in a switch are shown below:

```
Console_config#interface GigaEthernet0/1
Console_config_g0/1#switchport mode private-vlan promiscuous
Console_config_g0/1#switchport private-vlan mapping 2 3-5
Console_config_g0/1#switchport pvid 2

Console_config#interface GigaEthernet0/2
Console_config_g0/2#switchport mode private-vlan host
Console_config_g0/2#switchport private-vlan host-association 2 3
Console_config_g0/2#switchport pvid 3

Console_config#interface GigaEthernet0/3
Console_config_g0/3#switchport mode private-vlan host
Console_config_g0/3#switchport private-vlan host-association 2 3
Console_config_g0/3#switchport pvid 3

Console_config#interface GigaEthernet0/4
Console_config_g0/4#switchport mode private-vlan host
Console_config_g0/4#switchport private-vlan host-association 2 4
Console_config_g0/4# switchport pvid 4

Console_config#interface GigaEthernet0/5
Console_config_g0/5#switchport mode private-vlan host
Console_config_g0/5#switchport private-vlan host-association 2 5
Console_config_g0/5#switchport pvid 5

Console_config#interface GigaEthernet0/6
Console_config_g0/5#switchport mode private-vlan host
Console_config_g0/5#switchport private-vlan host-association 2 5
Console_config_g0/5#switchport pvid 5
```

```
Console_config#vlan 2
Console_config_vlan2#private-vlan primary
Console_config_vlan2#private-vlan association 3-5
```

```
Console_config#vlan 3
Console_config_vlan3#private-vlan community
```

```
Console_config#vlan 4
Console_config_vlan4#private-vlan community
```

```
Console_config#vlan 5
Console_config_vlan5#private-vlan isolated
```

```
Console_config#show vlan private-vlan
```

Primary	Secondary	Type	Ports
-----	-----	-----	-----
2	3	community	g0/1, g0/2, g0/3
2	4	community	g0/1, g0/4
2	5	isolated	g0/1, g0/5, g0/6