以下是华为交换机端口隔离命令的详细使用说明及配置要点：

‌一、端口隔离类型‌

‌双向隔离（端口隔离组）‌

同一隔离组内端口完全隔离（默认二层隔离三层互通，可配置为二层三层全隔离）。

‌适用场景‌：隔离同一VLAN内需互访控制的设备（如企业内不同部门终端）。

‌单向隔离‌

仅限制源端口到目标端口的流量（反向流量允许通行）。

‌适用场景‌：允许监控摄像头单向传输数据至服务器，但禁止服务器主动访问摄像头。

‌二、核心配置命令‌

‌1. 双向隔离配置流程‌

system-view # 进入系统视图

[Switch] port-isolate mode { l2 | all } # 设置隔离模式（默认l2）

# l2：二层隔离三层互通（常用）:ml-citation{ref="6,8" data="citationList"}；all：二三层全隔离:ml-citation{ref="3,5" data="citationList"}

[Switch] interface gigabitethernet 0/0/1 # 进入接口视图

[Switch-GigabitEthernet0/0/1] port-isolate enable group 1 # 加入隔离组1

[Switch-GigabitEthernet0/0/1] quit

[Switch] interface gigabitethernet 0/0/2

[Switch-GigabitEthernet0/0/2] port-isolate enable group 1 # 同组端口互相隔离

[Switch] interface gigabitethernet 0/0/24

[Switch-GigabitEthernet0/0/24] port-isolate uplink-port group 1 # 设为上行口（允许隔离组访问外部）:ml-citation{ref="3,6" data="citationList"}

‌

2. 单向隔离配置‌

[Switch] interface gigabitethernet 0/0/1 # 在源端口配置

[Switch-GigabitEthernet0/0/1] am isolate gigabitethernet 0/0/2 # 隔离目标端口:ml-citation{ref="1,6" data="citationList"}

# 效果：从0/0/1发出的报文无法到达0/0/2，反之允许:ml-citation{ref="1,11" data="citationList"}

‌三、关键注意事项‌

‌混合隔离限制‌

不支持端口自身隔离、管理网口隔离、Eth-Trunk与成员端口隔离1。

不同类型接口（如GE与10GE）可混合隔离。

‌隔离范围限制‌

端口隔离仅在同一设备生效，跨设备需结合VLAN或ACL36。

同一VLAN内生效，不同VLAN需先划分VLAN35。

‌上行口配置‌

避免将上行口与下行口加入同一隔离组，否则导致通信中断。

上行口需显式指定（port-isolate uplink-port）。

‌四、验证与维护命令‌

display port-isolate group 1 # 查看隔离组成员:ml-citation{ref="3,6" data="citationList"}

display mac-address | include GigabitEthernet0/0/1 # 检查隔离端口MAC表项（应无互访记录）:ml-citation{ref="3" data="citationList"}

ping测试：同组PC互ping应不通，但均可ping通网关:ml-citation{ref="3,5" data="citationList"}。

‌五、典型场景示例‌

‌需求‌：隔离PC1（0/0/1）与PC2（0/0/2），二者均可访问服务器（0/0/24）。

[Switch] port-isolate mode l2 # 二层隔离三层互通

[Switch] interface range gigabitethernet 0/0/1 to 0/0/2

[Switch-if-range] port-isolate enable group 1

[Switch] interface gigabitethernet 0/0/24

[Switch-GigabitEthernet0/0/24] port-isolate uplink-port group 1

‌结果‌：PC1与PC2无法互访，但均可访问服务器。

六、高保密要求场景下只保留上行端口，其他端口相互之间完全隔离配置说明

‌在华为交换机上实现除了上行端口外其他所有端口隔离的具体步骤如下‌：

‌创建端口隔离组‌：首先，进入系统视图，然后创建一个端口隔离组。例如，创建一个默认的隔离组，模式为二层+三层隔离（可选）。命令如下：

system-view

port-isolate mode all

‌将端口加入隔离组‌：接下来，将需要隔离的端口加入到隔离组中。例如，将端口1到端口23加入到隔离组1

interface range GigabitEthernet 0/0/1 to 0/0/23

port-isolate enable group 1

‌配置上行端口‌：将上行端口（如端口24）设置为隔离组的上行端口，允许这些端口与隔离组内的端口通信

interface GigabitEthernet 0/0/24

port-isolate uplink-port group 1

‌验证配置‌：最后，验证配置是否成功。可以使用以下命令查看隔离组成员：

display port-isolate group 1

通过以上步骤，可以实现除了上行端口外，其他所有端口之间的通信被隔离，但这些端口仍然可以通过上行端口访问外部网络或公共资源‌

此时0-23端口组内任意用户都不能相互之间通讯，只能与24号端口设备相互通讯。

‌七、模式选择建议‌

办公网用户隔离：port-isolate mode l2（节省VLAN资源）。

高安全需求场景（如摄像头网络）：port-isolate mode all 或单向隔离