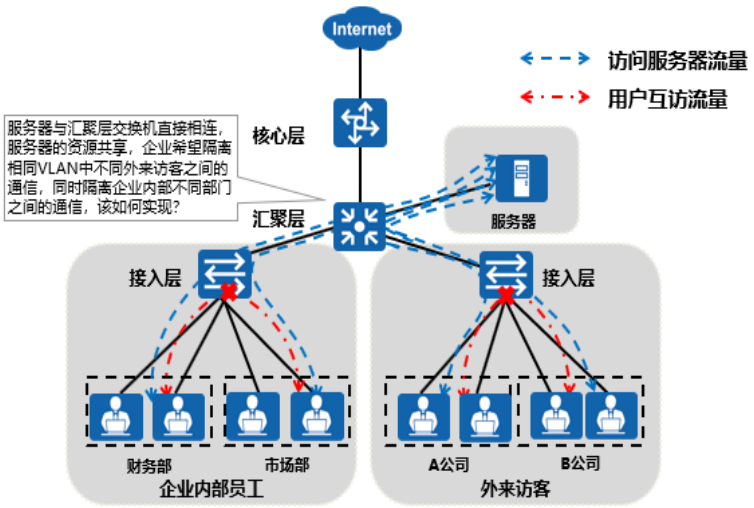
交换机高级特性简介

前言

- MUX VLAN（Multiplex VLAN）提供了一种通过VLAN进行网络资源控制的机制。通过MUX VLAN提供的二层流量隔离的机制可以实现企业内部员工之间互相通信，而企业外来访客之间的互访是隔离的。
- 为了实现报文之间的二层隔离，用户可以将不同的端口加入不同的VLAN，但这样会浪费有限的VLAN资源。采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。
- 在安全性要求较高的网络中，交换机可以开启端口安全功能，禁止非法MAC地址设备接入网络；当学习到的MAC地址数量达到上限后不再学习新的MAC地址，只允许学习到MAC地址的设备通信。

MUX VLAN应用场景

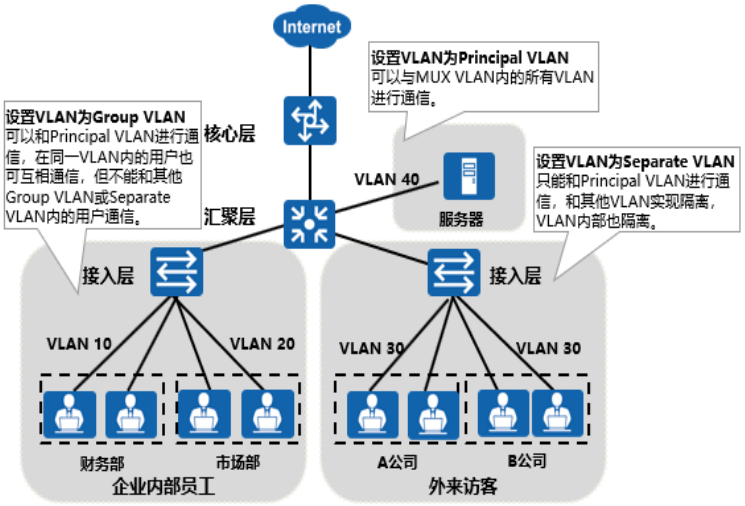


- 如图所示，服务器与汇聚层交换机相连，为了实现所有用户都可访问企业服务器，可通过配置 VLAN 间通信来实现。
- 对于企业来说，希望企业内部员工之间可以互相访问，而企业外来访客之间是隔离的，可通过配置每个访客使用不同

的 VLAN 来实现。但如果企业拥有大量的外来访客员工，此时不但需要耗费大量的 VLAN ID，还增加了网络维护的难度。

- MUX VLAN 提供的二层流量隔离的机制可以实现企业内部员工之间互相通信，而企业外来访客之间的互访是隔离的。

MUX VLAN基本概念

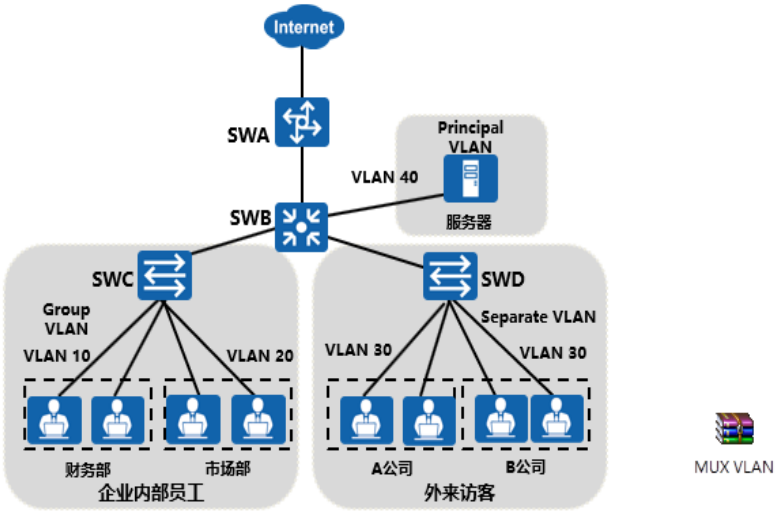


- MUX VLAN 的划分：
- 主 VLAN（Principal VLAN）：可以与 MUX VLAN 内的所有 VLAN 进行通信。
- 隔离型从 VLAN（Separate VLAN）：只能和 Principal VLAN 进行通信，和其他类型的 VLAN 完全隔离，Separate VLAN 内部也完全隔离。
- 互通型从 VLAN（Group VLAN）：可以和 Principal VLAN 进行通信，在同一 Group VLAN 内的用户也可互相通信，但不能和其他 Group VLAN 或 Separate VLAN 内的用户通信的 VLAN。
- 如图所示，根据 MUX VLAN 特性，解决方案如下：
- 企业管理员可以将服务器划分到 Principal VLAN。
- MUX VLAN 技术中只能将一个 VLAN 设置为 Separate V

LAN，所以可以将外来访客划分到 Separate VLAN。

- 由于可以将多个 VLAN 设置为 Group VLAN，所以可以将企业员工划分到 Group VLAN，企业内部不同部门之间通过划分到不同的 VLAN 进行隔离。
- 这样就能够实现：
- 企业外来访客、企业员工都能够访问企业服务器。
- 企业员工部门内部可以通信，而企业员工部门之间不能通信。
- 企业外来访客间不能通信、外来访客和企业员工之间不能互访。

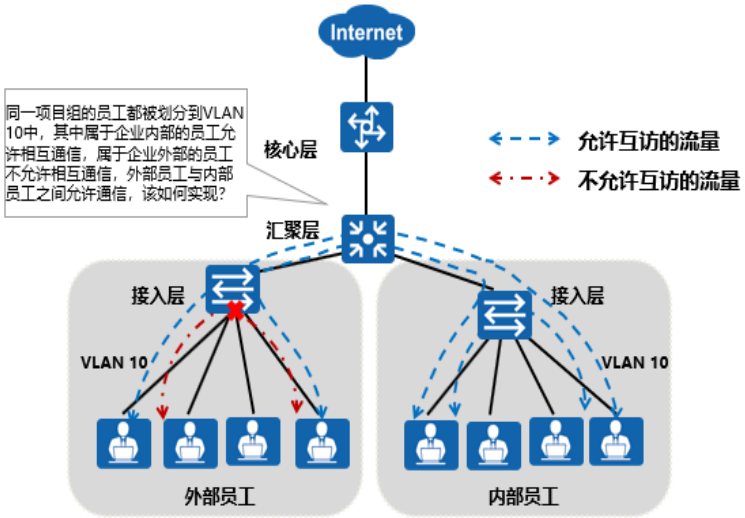
MUX VLAN配置实现



- 如图所示，希望实现企业外来访客、企业员工都能够访问企业服务器，而企业同部门员工可以通信，不同部门员工不能通信；企业外来访客间不能通信；企业外来访客和企业员工之间不能互访。
- 将企业服务器划分到 Principal VLAN，Principal VLAN 为 VLAN 40；
- 企业外来访客划分到 Separate VLAN，Separate VLAN 为 VLAN 30；

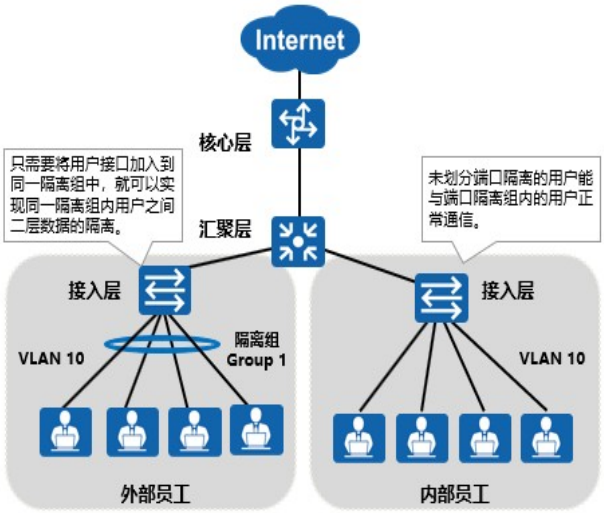
- 企业员工划分到 Group VLAN，Group VLAN 为 VLAN 10 与 VLAN 20，VLAN 10 分配给财务部，VLAN 20 分配给市场部，各部门之间二层隔离。
- SWB 配置：
- sysname SWB
- #
- vlan batch 10 20 30 40
- #
- vlan 10
- description Financial VLAN
- vlan 20
- description Marketing VLAN

端口隔离应用场景



- 为了实现用户之间的二层隔离，可以将不同的用户加入不同的 VLAN，但这样会浪费有限的 VLAN 资源。采用端口隔离功能，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到同一隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

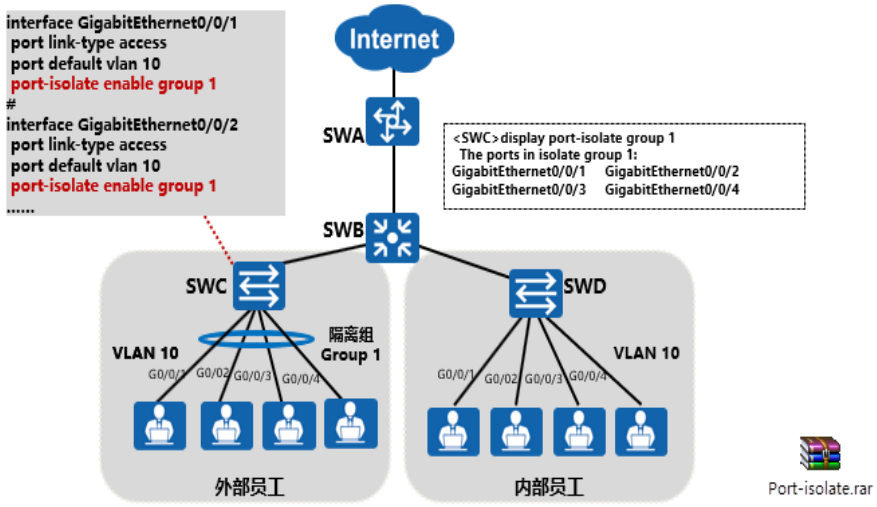
端口隔离基本概念



- 如图所示，同一端口隔离组内的用户不能进行二层的通信，但是不同端口隔离组内的用户可以进行正常通行；未划分端口隔离的用户也能与端口隔离组内的用户正常通信。
- 端口隔离分为二层隔离三层互通和二层三层都隔离两种模式：
- 如果用户希望隔离同一 VLAN 内的广播报文，但是不同端口下的用户还可以进行三层通信，则可以将隔离模式设置为二层隔离三层互通。
- 如果用户希望同一 VLAN 不同端口下用户彻底无法通信，则可以将隔离模式配置为二层三层均隔离。
- 配置注意事项：
- S 系列交换机均支持配置二层隔离三层互通模式。
- S 系列框式交换机均支持二层三层都隔离模式，S 系列盒式交换机仅 V100R006C05 版本仅 S2700SI、S2700EI 不支持二层三层都隔离模式，V100R002 及后续版本 S1720、S2720、S2750EI、S5700LI、S5700S-LI 不支持二层三层都隔离模式。
- 如果不是特殊情况要求，建议用户不要将上行口和下行

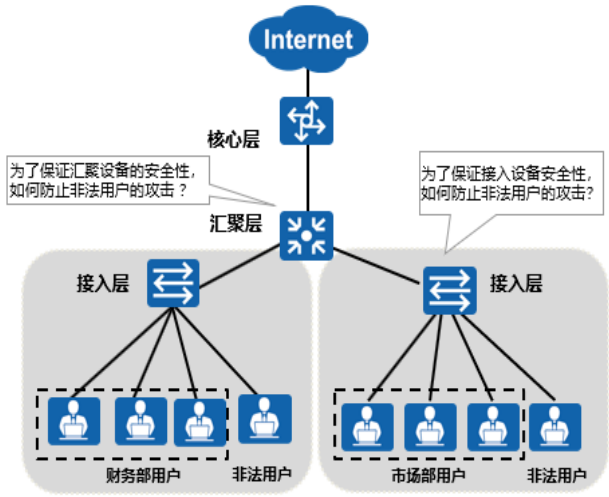
口加入到同一端口隔离组中，否则上行口和下行口之间不能相互通信。

端口隔离配置实现



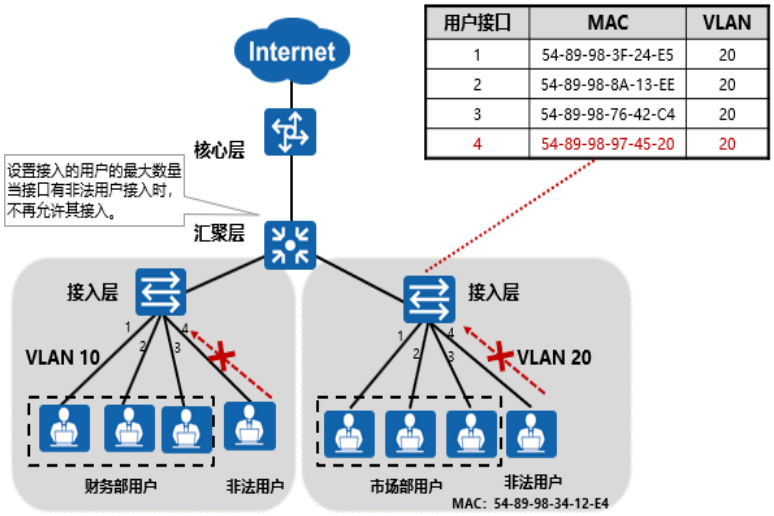
- 如图所示，同项目组的员工都被划分到 VLAN 10 中，其中属于企业内部的员工允许相互通信，属于企业外部的员工不允许相互通信，外部员工与内部员工之间允许通信。
- 配置命令：
- port-isolate enable 命令用来使能端口隔离功能，默认将端口划入隔离组 group 1。
- 如果希望创建新的 group 组，使用命令 port-isolate enable group 后面接所要创建的隔离组组号。
- 可以在系统视图下执行 port-isolate mode all 命令配置隔离模式为二层三层都隔离。
- 查看命令：
- 使用 display port-isolate group all 命令可以查看所有创建的隔离组情况。
- 使用 display port-isolate group X（组号）命令可以查看具体的某一个隔离组接口情况。

端口安全应用场景



- 如图所示，当网络中存在非法用户时，可以使用端口安全技术保证网络的安全。
- 端口安全经常使用在下列场景中：
- 应用在接入层设备，通过配置端口安全可以防止仿冒用户从其他端口攻击。
- 应用在汇聚层设备，通过配置端口安全可以控制接入用户的数量。

端口安全解决方案



- 在对接入用户的安全性要求较高的网络中，可以配置端口安全功能，将接口学习到的 MAC 地址转换为安全 MAC 地址，接口学习的最大 MAC 数量达到上限后不再学习新的 MAC 地址，只允许学习到 MAC 地址的设备通信。这样可以阻止其他非信任用户通过本接口和交换机通信，提高设备与网络的安全性。
- 如图所示，解决方案如下：
- 接入层交换机的每个接口都开启端口安全功能，并绑定接入用户的 MAC 地址与 VLAN 信息，当有非法用户通过已配置端口安全的接口接入网络时，交换机会查找对应的 MAC 地址表，发现非法用户的 MAC 地址与表中的不符，将数据包丢弃。
- 汇聚层交换机开启端口安全功能，并设置每个接口可学习到的最大 MAC 地址数，当学习到的 MAC 地址数达到上限时，其他的 MAC 地址的数据包将被丢弃。

端口安全类型

- 端口安全（Port Security）通过将接口学习到的动态MAC地址转换为安全MAC地址（包括安全动态MAC、安全静态MAC和Sticky MAC）阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

类型	定义	特点
安全动态MAC地址	使能端口安全而未使能Sticky MAC功能时转换的MAC地址。	设备重启后表项会丢失，需要重新学习。缺省情况下不会被老化，只有在配置安全MAC的老化时间后才可以被老化。
安全静态MAC地址	使能端口安全时手工配置的静态MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。
Sticky MAC地址	使能端口安全后又同时使能Sticky MAC功能后转换得到的MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。

- 说明：
- 接口使能端口安全功能时，接口上之前学习到的动态 MAC 地址表项将被删除，之后学习到的 MAC 地址将变为安全动态 MAC 地址。
- 接口使能 Sticky MAC 功能时，接口上的安全动态 MAC 地址表项将转化为 Sticky MAC 地址，之后学习到的 MAC 地址也变为 Sticky MAC 地址。
- 接口去使能端口安全功能时，接口上的安全动态 MAC 地址将被删除，重新学习动态 MAC 地址。
- 接口去使能 Sticky MAC 功能时，接口上的 Sticky MAC 地址会转换为安全动态 MAC 地址。

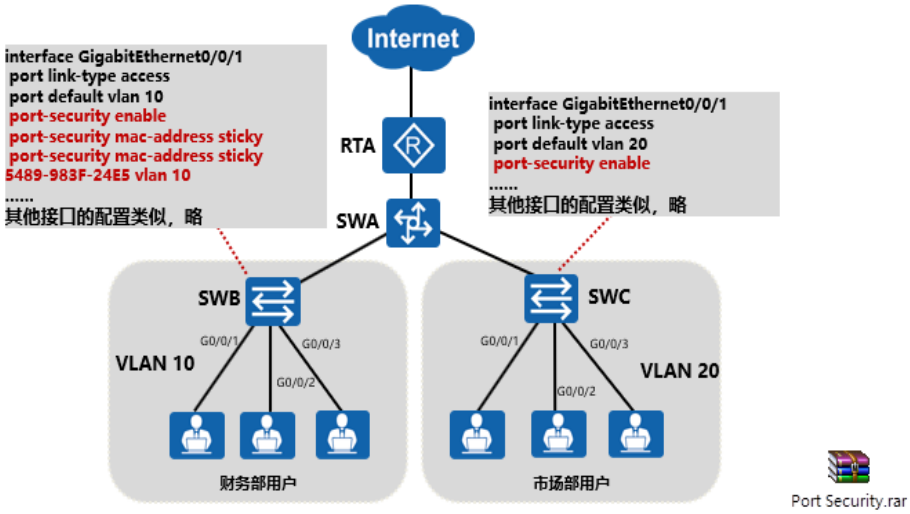
端口安全限制动作

- 超过安全MAC地址限制数后的动作：

动作	实现说明
restrict	丢弃源MAC地址不存在的报文并上报告警。推荐使用restrict动作。
protect	只丢弃源MAC地址不存在的报文，不上报告警。
shutdown	接口状态被置为error-down，并上报告警。默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用**restart**命令重启接口进行恢复。

- 接口上安全MAC地址数达到限制后，如果收到源MAC地址不存在的报文，端口安全则认为有非法用户攻击，就会根据配置的动作对接口做保护处理。缺省情况下，保护动作是restrict。

端口安全配置实现



- 如图所示，园区网络要求保障接入用户的安全性。财务部人员流动性较低，可以使用端口安全技术静态绑定接入用户的 MAC 与 VLAN 信息；市场部的人员流动性较高，使用端口安全技术的动态 MAC 地址学习保证接入用户的合法性。
- 命令解释：
- 执行命令 interface interface-type interface-number，进

入接口视图。

- 执行命令 port-security enable，使能端口安全功能。
- 缺省情况下，未使能端口安全功能。
- 执行命令 port-security mac-address sticky，使能接口 Sticky MAC 功能。
- 缺省情况下，接口未使能 Sticky MAC 功能。
- 执行命令 port-security max-mac-num max-number，配置接口 Sticky MAC 学习限制数量。
- 使能接口 Sticky MAC 功能后，缺省情况下，接口学习的 MAC 地址限制数量为 1。
- （可选）执行命令 port-security protect-action { protect | restrict | shutdown }，配置端口安全保护动作。
- 缺省情况下，端口安全保护动作为 restrict。
- （可选）执行命令 port-security mac-address sticky mac-address vlan vlan-id，手动配置一条 sticky-mac 表项。

端口安全配置验证

- 在SWB上使用命令查看绑定的MAC地址表:

```
<SWB>display mac-address sticky
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/    PEVLAN CEVLAN Port          Type      LSP/LSR-ID    VSI/SI
MAC-Tunnel
-------------------------------------------------------------------------------
5489-988a-13ee 10       -      -      GE0/0/2           sticky    -
5489-983f-24e5 10       -      -      GE0/0/1           sticky    -
-------------------------------------------------------------------------------
```

- 在SWC上使用命令查看动态学习到的MAC地址表:

```
<SWC>display mac-address security
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/    PEVLAN CEVLAN Port          Type      LSP/LSR-ID    VSI/SI
MAC-Tunnel
-------------------------------------------------------------------------------
5489-9876-42c4 20       -      -      GE0/0/1           security  -
5489-9897-4520 20       -      -      GE0/0/2           security  -
-------------------------------------------------------------------------------
```

思考题

1. 在MUX VLAN中，可以与所有VLAN进行通信的是下列哪个选项？（ ）

A. Principal VLAN　　B. Separate VLAN

C. Group VLAN　　D. Subordinate VLAN

2. 端口安全技术中安全MAC地址类型有以下哪几种？（ ）

A. 安全动态MAC地址　　B. 安全静态MAC地址

C. Sticky MAC地址　　D. Protect MAC地址

- 答案：A。
- 答案：ABC。