交换机高级特性

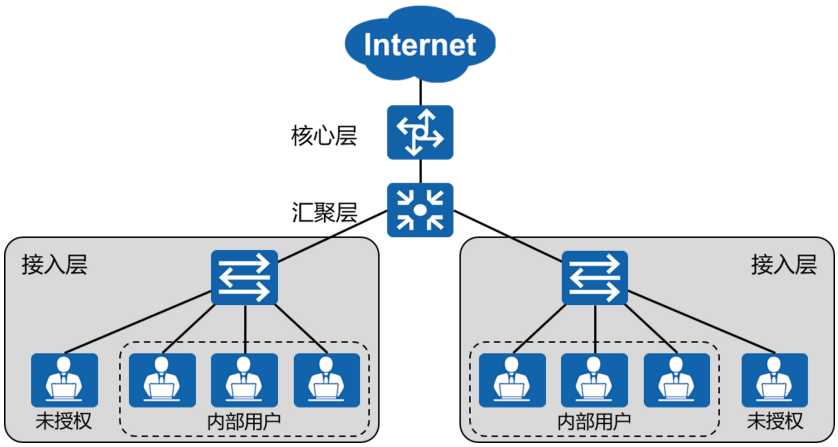
一、端口安全

1、端口安全的概念

1.1、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

1.2、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

1.3、保证只有授权主机可以接入并访问网络，而非授权设备无权接入当前网络



2、基于主机MAC地址的允许流量

2.1、端口安全能够基于主机MAC地址而允许流量

2.2、单个端口能允许1个以上到某个特定数字的MAC地址

3、端口安全的类型

端口安全【Port Security】通过将端口学习到的动态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】，以阻止非授权用户通过本端口与交换机通信，从而增强设备的安全性

类型	定义	特点
安全动态MAC地址	开启端口安全而未开启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的老化时间后才会被老化
安全静态MAC地址	开启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	开启端口安全后又同时开启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

3.1、端口开启【端口安全】功能时，端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

3.2、端口开启【Sticky MAC】功能时，端口上的安全动态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

3.3、端口关闭【端口安全】功能时，端口上的安全动态MAC地址将被删除，重新学习动态MAC地址

3.4、端口关闭【Sticky MAC】功能时，端口上的Sticky MAC地址会转换为安全动态MAC地址

4、端口安全的限制行为

4.1、端口上安全MAC地址数达到限制后，若收到源MAC地址不存在的报文，端口安全则认为有非授权用户攻击，则会根据配置的动作对端口做保护处理

4.2、缺省情况下，保护动作为restrict

动作	具体阐述
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	端口状态被置为error-down，并上报告警；默认情况下，端口关闭后不会自动恢复，只能由网络管理员在端口视图下使用【restart】命令重启端口进行恢复

5、端口安全的配置

5.1、端口配置模式下，开启端口安全服务

[Huawei-Ethernet0/0/1]port-security enable

5.2、端口配置模式下，配置每个端口所允许的最大MAC地址数量

[Huawei-Ethernet0/0/1]port-security max-mac-num {maximum-number}

5.3、端口配置模式下，手工配置MAC地址

[Huawei-Ethernet0/0/1]port-security mac-address sticky

[Huawei-Ethernet0/0/1]port-security mac-address sticky H-H-H vlan vlan-id

5.4、端口配置模式下，当该端口连接至其它未授权主机时，端口动作

[Huawei-Ethernet0/0/1]port-security protect-action [protect | restrict | shutdown]

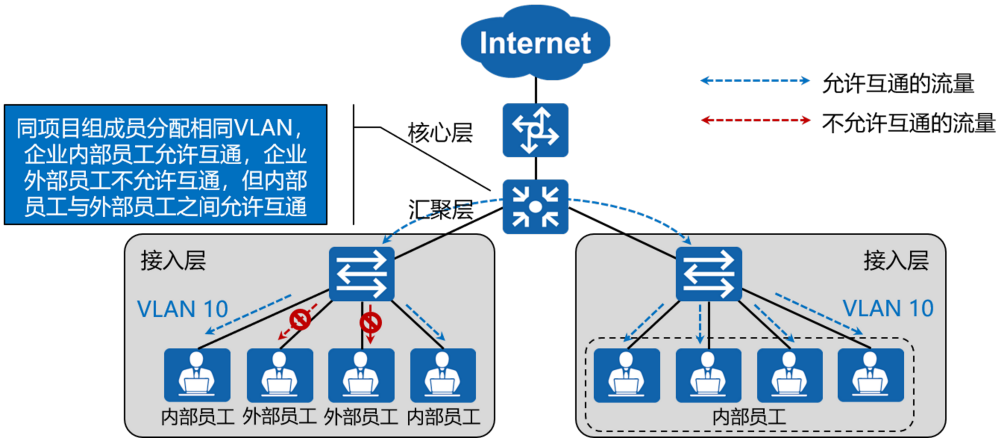
二、端口隔离

1、端口隔离的概念

1.1、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

1.2、采用端口隔离功能，可以实现同一VLAN内端口之间的隔离

1.3、端口隔离功能为用户提供了更安全、更灵活的组网方案



2、端口隔离的基本原理

2.1、同一VLAN隔离组内的用户不能进行二层通信

2.2、不同VLAN隔离组内的用户可正常通信

2.3、未划分VLAN隔离的用户也可与VLAN隔离组内的用户正常通信

3、VLAN隔离组分为2种模式：

3.1、二层隔离三层互通：隔离同一VLAN内的广播，但不同端口下的用户仍可进行三层通信

3.2、二层三层均隔离：同一VLAN不同端口下的用户完全无法通信

4、端口隔离的配置

4.1、系统视图模式下，配置端口隔离的模式

port-isolate mode [l2 | all]

4.2、进入端口配置模式

[Huawei]interface Ethernet 0/0/2

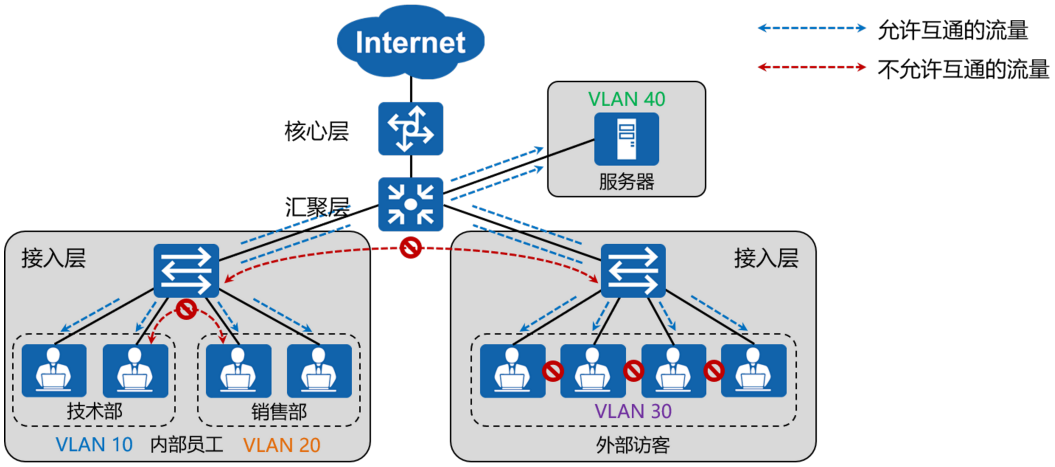
4.3、端口配置模式下，将链路配置为接入模式

[Huawei-Ethernet0/0/2]port link-type access

4.4、端口配置模式下，将端口加入进VLAN 10
[Huawei-Ethernet0/0/2]port default vlan 10

4.5、端口配置模式下，开启端口隔离功能
[Huawei-Ethernet0/0/2]port-isolate enable group 1

三、MUX VLAN
1、MUX VLAN的概念
1.1、MUX VLAN【Multiplex VLAN】提供了一种通过VLAN进行网络资源控制的机制
1.2、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
1.3、服务器连接在汇聚层交换机上提供共享资源，企业希望隔离相同VLAN中不同外部访客之间的通信，同时隔离企业内部不同部门之间的通信



2、MUX VLAN的基本原理
2.1、MUX VLAN分为两大子VLAN：
a、主VLAN【Principal VLAN】
b、从VLAN【Subordinate VLAN】

2.2、从VLAN又分为两种类型：
a、互通型从VLAN【Group VLAN】
b、隔离型从VLAN【Separate VLAN】

3、MUX VLAN的通讯范围
3.1、主VLAN【Principal VLAN】：可与MUX VLAN内的所有VLAN通讯
3.2、互通型从VLAN【Group VLAN】：可与Principal VLAN进行通讯，可与同一Group VLAN内的用户通讯，不能与其它Group VLAN或Separate VLAN内的用户通讯
3.3、隔离型从VLAN【Separate VLAN】：只能与Principal VLAN通讯，与其它VLAN完全隔离，Separate VLAN内部也完全隔离

4、MUX VLAN的配置
4.1、创建并进入VLAN配置模式
[Huawei]vlan 40

4.2、VLAN配置模式下，开启MUX VLAN功能
[Huawei-vlan40]mux-vlan

4.3、VLAN配置模式下，关联互通型从VLAN
[Huawei-vlan40]subordinate group 10 20

4.4、VLAN配置模式下，关联隔离型从VLAN
[Huawei-vlan40]subordinate separate 30

4.5、端口配置模式下，开启MUX VLAN功能
[Huawei-Ethernet0/0/3]port mux-vlan enable

四、交换机高级特性的实验配置
详细配置见实验手册