浅谈交换机安全配置

◆沈云明

（云南省普洱卫生学校）

摘要：交换机在企业网络中占有重要地位，通常是整个网络的核心所在。在这个黑客入侵风起云涌、病毒肆虐的 IT 时代，作为网络运行核心的交换机理所当然要承担起网络安全的一部分责任。本文就交换机的运行安全做一些简单探讨。

关键词：交换机；VLAN；端口安全

交换机作为局域网中信息交换的关键设备，承载着大量的数据流量的交换，当出现异常情况，如网络攻击或 BT 大流量下载时，极有可能造成负载过重或宕机。以下就交换机的基本安全、VLAN、端口安全及 IP 与 MAC 绑定做一些介绍。

一、交换机基本安全设置

1、设置交换机登陆密码

为防止非法登入，需设置交换机登陆密码。配置方法如下：

SW1(config)enable secret 0 F8cME0 //设置高级用户登陆密码

2、配置 SSH 登陆服务

配置 SSH 登陆，关闭其他不用的管理方式。配置方法如下：

SW1(config) # no enable service web-server //关闭 Web 登陆

SW1(config) # enable service ssh-server //开启 ssh 登陆服务

SW1(config) # no ip ssh version //设置 ssh 工作在自适应模式

SW1(config) # username userA password F8cME0 //设置用户及密码

SW1(config) # crypto key generate rsa //生成本地 rsa 密钥对

SW1(config) # transport input ssh //远程只允许 ssh 登陆

3、配置 MAC 地址过滤

配置交换机在某一 VLAN 下过滤特定 MAC，配置方法如下：

SW1(config) # mac-address-table filter D43D.7E5A.BE52

二、划分 VLAN

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样。一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点： 网络设备的移动、添加和修改的管理开销减少；可以控制广播活动；可提高网络的安全性。本文就以图 1 所示拓扑结构讲解如何配置 VLAN：

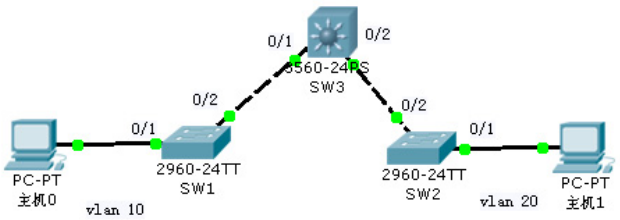

图 1

SW1(config) # vlan 10

SW1(config-if) # ip address 10.10.10.100 255.255.255.0 //设置 vlan 10 IP

SW1(config) # int f 0/1

SW1(config-if) # switch acc vlan 10 //端口 0/1 划入 vlan10

SW1(config-if) # int f 0/2

SW1(config-if) # sw mode trunk // 设置0/2端口模式设为 trunk 模式

SW2(config) # vlan 20

SW1(config-if) # ip address 10.10.20.100 255.255.255.0 //设置 vlan 20 IP

SW2(config) # int f 0/1

SW2(config-if) # switch acc vlan 20 //端口 0/1 划入 vlan20

SW2(config-if) # int f 0/2

SW1(config-f) # switch mode trunk // 设置端口 0/2 端口模式设为 trunk 模式

SW3(config) # vlan 10

SW3(config-if) # ip address 10.10.10.100 255.255.255.0 //设置 IP

SW3(config-if) # vlan 20

SW3(config-if) # ip address 10.10.20.100 255.255.255.0 //设置 IP

SW3(config-if) # int f 0/1

SW3(config-if) # switch acc vlan 10

SW3(config-if) # int f 0/2 //设置端口 0/2

SW3(config-if) # switch acc vlan 20 //将该端口加入 VLAN20

SW3(config) # int ran f0/1-2 //统一设置 0/1-0/2 端口口

SW3(config-range-if) # switchport mode trunk //设置端口模式为 trunk

三、端口安全设置

端口安全（Port Security），从基本原理上讲，Port Security 特性会通过 MAC 地址表记录连接到交换机端口的以太网 MAC 地址（即网卡号），并只允许某个 MAC 地址通过本端口通信。其他 MAC 地址发送的数据包通过此端口时，端口安全特性会阻止它。使用端口安全特性可以防止未经允许的设备访问网络，并增强安全性。另外，端口安全特性也可用于防止 MAC 地址泛洪造成 MAC 地址表填满。主要配置命令如下：

SW1(config) # int ran f 0/1-24 //统一设置 1-24 口端口安全

SW1(config-if-range) # switchport port-security //开启端口安全模式

SW1(config-if-range) # switchport port-security maximum 1 // 设置 MAC 数量

SW1(config-if-range) # switchport port-security mac-address sticky //启用粘滞获取

SW1(config-if-range) # switchport port-security violation //针对非法访问计算机，端口采取的处理模式

四、ACL 访问控制列表

访问控制列表（Access Control List，ACL） 是路由器和交换机接口的指令列表，用来控制端口进出的数据包。信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，为了保证内网的安全性，需要通过安全策略来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。简而言之，ACL 可以过滤网络中的流量，是控制访问的一种网络技术手段。配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。如可以配置 ACL，禁止局域网内的设备访问外部公共网络，或者只能使用 FTP 服务。ACL 是网络中保障系统安全性的重要技术，在设备硬件层安全基础上，通过对在软件层面对设备间通信进行访问控制，使用可编程方法指定访问规则，防止非法设备破坏系统安全，非法获取系统数据。

参考文献：

[1]朱晔《基于端口的 VLAN 技术及其配置》软件导报 2008

[2]刘晓辉《交换机•路由器•防火墙》电子工业出版社 2015