



网络设备与配置实习报告

学院名称 网络安全学院

专业名称 网络空间安全

学生姓名 苏涤岚

学生学号 201817030103

任课教师 李冬芬

实习成绩

二○一九年 十二月

目录

[Day1: 3](#_Toc28863390)

[Day2 4](#_Toc28863391)

[DAY3 5](#_Toc28863392)

[DAY4 6](#_Toc28863393)

[DAY5 8](#_Toc28863394)

[DAY6 9](#_Toc28863395)

[DAY7 10](#_Toc28863396)

[DAY8 13](#_Toc28863397)

[DAY9 14](#_Toc28863398)

[DAY10 16](#_Toc28863399)

Day1:

实训第一天，张小平老师为我们讲解了过几天的学习内容，和考察内容和模式

成绩为上机+实验报告综合测评，他强调了我们每天的内容要听懂，才能为之后的学习奠定基础上课时间：9-12am和2-5pm

**阶段一：网络组建于安全配置实训 6天 张小平老师讲**

网络基础知识巩固

华为交换机网络与安全配置实训

华为路由器网络与安全配置

华为防火墙网络安全配置

一阶段期末考察（知识点考察+案例配置考察）

**阶段二:服务器安全与配置 许富强老师 4天**

windows服务器系统与安全

linux服务器系统与安全

vpn网络服务与安全

二阶段期末考察

配置服务器的系统与应用

3平时成绩 考勤+实训报告+问答

7期末：期末1+期末2

第一天，我们进行了一个训前测评（网络知识测评）。我发现自己的网络的基础十分薄弱，张老师在我们的成绩基础上决定为我们讲讲网络基础，张小平老师用淳朴、质朴的语言将难懂的交换机讲的淋漓尽致，清晰易懂。

张老师第一天，亲切的和蔼的手把手将我们如何安装ensp，华为网络模拟器。

他说：ensp是属于华为的，是安全的，而思科是国外的，虽然思科操作比较方便，命令行比较简洁，而且有时候ensp的设置很奇怪，但是我们还是要用ensp。毕竟安全为先嘛。（用国产，自主可控）

然后我们开始了玩耍网络模拟器的旅途！

我们做的第一个实验是**了解交换机启动，**Pc机器是用的串口，而交换机是console口

1. **建立华为网络模型，**

**一个交换机和pc相连接**

**二、终端连接通讯**

1 启动**PC**，并设置串口速率：  
2. 启动交换机，在pc上进行串口连接，即可看到交换机启动信息。

很神奇，竟然可以在一个软件上模拟真实环境，我感到惊讶于惊喜。

Day2

讲了ctl命令：

**?** 查看当前命令视图下可调用的命令列表和说明；

**命令** **？**  查看该命令的使用说明，如：ping ? p？、di**?**、display ver**?** 查看以这是字母开头的命令列表

**命令缩写**：只输入命令开头的前几个字母（条件是没有其他命令有相同的开头字母），提高输入效率；如：display ，可以缩写为：**dis**，但不能缩写为di，因为di开头的命令还有dir

**命令自动补全**：命令缩写时按TAB键能够自动补全，如有其他命令有相同的开头字母，再按TAB键则会显示其他命令。  


**讲了用户命令视图和系统命令的区别**在用户视图下只能执行一些简单的系统视图和查看的命令， 如：

Display current-configuration 查看当前运行生效的配置

Disp this 查看当前视图层下运行生效的配置

Display version 查看版本信息

Display interface brief 查看接口摘要

Clock 设置时间 Save 保存配置

Dir 查看文件 reboot 重启系统  
display saved-configuraiton 查看保存的配置

Reset saved-configuration 清楚保存的配置

系统命令下才有权限执行各种配置管理命令

设备命名：sysname s1

为了安全性 建议配置console连接口令

User-interface console 0

Authentication-mode password

Set authentication pass word cipher(加密型号) 口令

当配置完成后，连续输入：quti退出连接管理，再次进入就需要口令验证了

为了禁用消息弹出(免消息干扰）： undo info-center enable

DAY3

我们今天讲了远程管理这个实验和stelnet远程连接

实际工程中，网络进行初始配置完成后放置到网络中运行，配置管理都是通过

网络来进行的，这种方式成为带内管理方式（占用少量网络带宽）

一：配置管理IP

网络管理需要IP地址的支持，首先需要为交换机配置。

进入系统视图—> **vlan 1** 接口 （默认的管理网络）-> 配置管理ip地址  
 interface vlan 1

Ip address 192.168.1.254 255.255.255.0

二.配置VTY虚拟终端  
user-interface vty 0 1(编号从0开始)

Authentication-mode password (口令验证)

Set authentication password cipher 口令

为了增强安全性，建议：设置super口令，以便进入系统视图是进行验证

Super password cipher 口令‘’

三：远程管理连接

退出到用户视图

telnet x.x.x.x

安全telnet 远程连接

在前节使用的telnet登录是使用明文传输，存在较大的安全隐患。

 stelnet是一种安全的telnet，通过用户认证及双向的数据加密，为网络登录提供安全的远程连接和登录服务。

 stelnet服务使用的ssh 安全shell网络协议，通过对网络数据的加密，使能够在一个不安全的网络环境中，提供安全的网络连接服务。

1：启用stelnet服务：stelnet server enable

2：配置ssh用户

Ssh user admin

Ssh user admin authentication-type password

Ssh user admin service-type stelnet

:3：进入vty必须为aaa认证，允许ssh连入

Authentication-mode aaa

Protocol inbound ssh

4:进入aaa,配置口令,service-type

Local-user admin password cipher 口令

Local-user admin service-type ssh

Local-user admin privilege level 3

5::查验ssh

Display ssh server status

Display ssh user-information

6 交换机s2作为客户端登录

Ssh clinet first-time enable

Stelnet 192.168.1.254

DAY4

链路聚合

链路集合将多个以太网物理接口绑定在一起形成以太网逻辑接口称之为：eth-trunk

链路聚合实现了倍增带宽、负载均衡、冗余备份的作用

通过在设备间建立链路聚合组，提高更高的通信带宽和可靠性

链路聚合协议标准：ieee 802.3aad

基本上交换机都支持全双工

链路聚合只能使用全双工以太网接口

每组聚合链路最多能聚合8个以太网接口

交换机接口上不能配置任何业务功能、ip和mac地址

交换机接口连接类型已不是hybrid类型

交换机接口只能胶乳到一个eth-trunk

同一个eth-trunk组中的接口介质和传输率必须相同，不能混用

交换机之间互联的接口必须加入同一个eth-trunk

链路聚合模式分为lacp(链路聚合连接协议)模式和load-balance（负载均衡）模式。

* lacp:
  + 几根线走流量，几根线不走流量（空起来）
  + 等到了双十二，把其他几根线用起来。
  + 用时激活即可,可以控制利用率为多少

load-balance

* + 利用率为100%

LACP更受欢迎**。负载均衡**模式的链路聚合比较简单，聚合组中的所有接口都是活动状态,平均分担流量负载，不存在备份接口和优先级。

为了解决网络环路问题

启用stp(生成树协议，ieee802.1d协议)

Stp协议通过阻塞网络中多余的连接端口，将物理的环形网络修剪成逻辑的属性网络，消除网络环路

启用交换机stp协议，清除网络环路

快速stp(rstp) (ieee 802.1d标准)网络收敛速度慢，网络通信回复时间也比较长。

ppp三个特点优势：扩展性，适用性，安全性

DAY5

vlan 虚拟局域网技术 链路层 802.1q

采用vlan技术，就是讲单个物理的局域网划分成多个逻辑的额局域网

这样就将原来规模较大的广播域划分为若干的规模较小的广播域，从而显著地降低了局域网的广播通信量，减少广播报文对网络通信的影响

Vlan技术优势

限制广播域 ：网络广播被限制在单个的逻辑局域网vlan内

增强安全性：不同vlan之间不能直接通信，起到网络隔离的作用

提高可靠性：网络故障只影响单个valn，起到故障隔离的作用

增强灵活性：灵活的规划和部署vlan,便于网络管理和安全控制

Vlan 接口烈性

Access烈性：仅用于连接计算机，仅仅属于单个vlan

Trunk类型：仅仅用于网络设备胡连接，属于多个vlan

Hybrid类型：综合了access和trunk两个类型的功能（华为交换机接口默认类型）

**VLAN接口类型**

**查看vlan接口类型**

**Display port vlan**

**Display port vlan Ethernet 0/0/1**

**设置vlan接口类型**

**Interface Ethernet0/0/1**

**Port link-type access|trunk|hybrid**

**Gvrp:gvrp不传递vlan接口配置，每个交换机的vlan接口划分都是独立的**

**Gvrp信息传递都是双向对等的，即在启用gvrp功能的交换机上创建新的vlan，则在其他交换机上会创建一样的动态vlan**

**通过gvrp创建爱你的动态vlan是不能删除和修改的**

只能原创者删除动态vlan,除非把它变成普通vlan（加端口）才能删除和修改。往其中加端口，就变成了common本地vlan了

* 安全区域（security zone),简称区域zone 是一个安全概念，大部分用于安全区域，一个安全区域就是若干接口所连接网络的合集，这些网络中的
* untrust 外网 安全级别：5
* dmz 隔离区 安全级别：50
* trust 高安全 eg:内网 安全级别：85
* local 高安全 eg:防火墙本身 安全级别：100
* 防火墙控制两个区域之间的，就是控制 域间的
* 内外网构成一个安全域间
* 安全域间与方向
* 安全域间这个概念用来描述流量的传输通道。它是两个“区域”之间的唯一“道路”，如果希望对经过这条通道的流量进行控制，就必须在通道上设立“关卡”，也就是安全策略。但是对于不需要经过这条通道的流量，例如在同一个安全域间内转发的流量，在安全域间下发的安全策略是不起作用的。
* 任意两个安全区域都构成一个安全域间（Interzone），并具有单独的安全域间视图，大部分的安全策略都需要在安全域间视图下配置。
* 安全域间的数据流动具有方向性，包括入方向（Inbound）和出方向（Outbound）。
* 入方向：数据由低优先级的安全区域向高优先级的安全区域传输。
* 出方向：数据由高优先级的安全区域向低优先级的安全区域传输。

DAY6

* 上午讲了一个简单的实验，复习了一下，然后考理论知识
* 下午做了一个 期末测验
* 没什么好写的，就写一些复习的知识吧

在IPv4中，私有地址的范围分别是：

A类地址范围：10.0.0.0—10.255.255.255

B类地址范围：172.16.0.0---172.31.255.555

C类地址范围：192.168.0.0---192.168.255.255

特殊ip地址：

0.0.0.0 默认路由，缺省网络 表示所有网络，默认网络

环回地址：loopback, 仅用于本机测试

169.254.x.x:ip分配失败，主机保留地址

255.255.255.255 网络广播地址

smtp:25 邮件传输

pop3:110 邮件接收

ftp:20 21 文件传输

dhcp:67 68(udp) 地址配置

dns:53 (udp+tcp) 域名解析

telnet:23 远程登录

http:80 网页浏览

https:443 加密的网络浏览 ssl加密

snmp:udp161 162 网络管理 网络运维状态

DAY7

**讲了服务器硬件-硬盘的认识+阵列+dhcp+dns**

**讲了ide接口，sata接口，并行scsi接口，并行scsi接口，sas接口**

**磁盘整列：**

**常见RAID**

**RAID0**

* 多块硬盘同时写与读，速度很快raid0是 raid中速度中最大的
* 没有数据冗余功能
* 物理的一个硬盘坏了，逻辑硬盘还是一个，数据块损失，数据就损坏了用不了
* 通常用于测试
* 不能存储关键数据在其中，有很大风险
* 至少一个硬盘

**RAID1**

* 主要功能为了(实现了完全冗余）数据冗余，每一个都有一个备份，不是为了性能
* 坏一个，数据还有一个备份，坏两个就要换硬盘了
* 实际使用空间要n\*单个硬盘/2
* 至少2个硬盘

**RAID10**

* raid10 结合raid1和raid0
* 两两做raid1，再做raid0
* 数据库通常用raid10
* 磁盘空间少一半
* 至少4个硬盘

**RAID5**

* 从性能 磁盘空间，实际磁盘空间（n-1）\*单个空间，允许有一个硬盘数据损坏（数据冗余）
* 至少3个硬盘
* 校验值会在多个硬盘中打散读写
* n个硬盘=n-1个+1个校验值

**RAID6**

* 实际空间n-2个空间
* 至少4个硬盘
* 每个阵列都有两个校验值
* 只要只要n-2份数据知道计算出其他的损坏的数据
* 允许两块硬盘坏，安全性高
* 4个硬盘，坏两个装真实数据的硬盘，两块校验值可以推算出其他两个

wrthru直通模式：

* + 阵列卡不存储数据，（即使有缓存也不用）数据直接存到硬盘（当os提交数据给阵列卡，整列卡不存储数据，不做缓存，直接传给硬盘）
  + 优点：不怕断电，只要写了数据，就到硬盘上面去了，即使断电也在硬盘上，不做缓存
  + 缺点：os提交给阵列卡后，只有当提交到硬盘之后，阵列卡才告诉操作系统已经完成（延迟稍慢）

wrtback直连模式：

* 不做缓存，延迟慢一点
* os提交数据给阵列卡，阵列卡接收数据（有缓存），直接告诉操作系统已经完成，风险是还没到硬盘，如果这时刻停电，如果阵列卡这时候没电，数据就会丢失

wrtback with BBU(满载电池的直连模式）：

* + 性能与安全并存的模式
  + 很多阵列卡默认都是BBU模式
  + 检测到你阵列卡上有电池，并且是好的，就使用WRTBACK模式
  + 没有的话，就以wrthru工作

正向解析：域名查询ip，反向解析：ip查域名

根服务器：13 个 1+12

服务器：无数个，dns: 512byte，udp53 客户查询 当信息大于512byte时候也用tcp53，tcp:53 dns服务器相互查询

dns查询模式：

客户机与dns服务器之间:递归查询模式，dns服务器之间：迭代查询

* 顺序：hosts（最优先）>Dns>wins

DAY8

Win server架设wins服务+linux历史讲解以及简单命令+有趣的一个软件toilet的使用

red hat 很多版本发布都是以gpl协议开放的 当然还有没开源的版本

发行版中三大使用版本1：red hat 2：suse 3:ubuntu

版本管理系统发展 cvs->svn->git

rhel(RedHat Enterprise Linux Server)

rhel (red hat enterprise linux)企业版现在到8了（几年进一个版本）收服务费，提供技术支持，升级需要收费

red hat->fedora(free)（新技术先放进去，不稳定）事业型

* workstation
* server

red hat（现已被ibm收购，ibm为了云计算发展而收购）->centos 社区操作系统（free)(重新编译开发的（红帽收编）

* 关键业务用收费的版本：rhel
* 不关键用free的版本：centos

red hat 分支

* oracle enterprise linux(单独内核版本，）都是基于red hat重新编译的 几星期 ，剔除掉red hat 闭源的
* centos 三个月左右

suse:与red hat 运行模式相同 yast(打包工具）（反复被收购）

* + sles(SUSE Linux Enterprise Server):服务器版本 suse linux enterprise server 卖服务 一年4000yuan左右
  + seld desktop 桌面版

与redhat 和fedoral关联大相比，suse 与opensuse 相关联会更少

* + opensuse (free)（和suse内核用相同的）

DAY9

Linux系统网站架设+防火墙开放端口+设置selinux

ctrl +z暂停应用程序，丢到后台，退回shell

* 调回shell 中按fg命令

ctrl+c结束运行的任务，即需要重新跑

* ps -au
* -a 所有进程
* -u 用户信息名字

find 处于路径 -name 查找姓名

env 列出用户所有的环境变量

.bash\_history:历史操作记录下来 （默认是记录下最近的1000条）：看用户做了什么

* hack:渗透进系统，看历史找是否有passwd
* 保护人员：查看history,查看用户输入了哪些命令
* 等保测试时要求： fro safyty history不超过5条

link文件就是软连接，类似于windows10的快捷方式

/bin 和/usr/bin普通用户可以使用的可执行程序

/sbin 和/usr/sbin 超级管理员用的可执行程序 管理的命令经常放在其中

/usr 放系统相关的程序，和用户自己安装的程序

/lib 和/lib64库文件

* + .a静态库文件
  + .so 动态链接库文件

windows: dll 动态链接文件

/var 存 用户数据的分区

* /var/log 看日志文件，看自己犯了什么错
* /var/lib/run
* /var/spool/mail lpq打印队列

/proc 和/sys

* 不能写any东西，不能删除，有关内存的东西（不准确），**不是硬盘的东西**，根据情况加载，很多参数，网卡参数什么的
* 防火墙只开启了连接icmp和ssh功能
* web连接不了，firewalld 开启的
* systemctl stop firewalld
* systemctl disable firewalld 永久关闭，（最好不用）
* 以下可以方式开启web
* firewall-cmd --add-port =80/tcp
* firewall-cmd --add-port =80/tcp --permanent
* firewall-cmd --add-service =http
* firewall-cmd --add-service=http ==permanent

windows修改hosts文件:/system32/drivers/etc/hosts

linux修改hosts文件：/etc/hosts

DAY10

**Linux下面架设vsftp+Vpn技术+考试**

linux下两个免费的数据库

* mysql 和postgre sql
* Mysql
  + 为了小巧，不是参照数据库92标准
  + 四物功能
  + 之前不是按gpl协议发布的，后来商业公司也可以用（要单独收费）
* postgre sql
  + 参照了数据库标准

ls /home可以看当前系统中有哪些用户

**安装vsftpd，yum install vsftpd**

**开启vsftpd服务 systemctl start vsftpd**

**设置匿名用户的完全浏览器、删除等权限**

**Vi /etc/vsftpd/vsftpd.conf**

**Tail -2 /etc/vsftpd/vsftpd.conf**

**每次修改了配置文件都要重新启动vsftpd才能生效修改过的内容**

**当然要让防火墙开启ftp服务，外界主机才能ftp连接到**

**Firewall-cmd –add-service=ftp –permanent**

**查看防火墙开启的服务 Fireawall-cmd –list-service**

**客户端访问测试，chroot功能将用户锁定到自己的HOME目录**

**Vi /etc/vsftpd/vsftpd.conf**

**取消注释掉以下三条语句**

**chroot\_local\_-user=YES**

**chroot\_list\_enable=YES**

**chroot\_list\_file=/etc/vsftpd/chroot\_list**

**添加语句  
 allow\_writeable\_chroot=YES**

**再创建一个文本,touch /etc/vsftpd/chroot\_list 🡪加入的用户不做chroot，即ftp登录这个用户就可以不锁定，可以越权去到其他目录，例如根目录。可以下载很多不是该用户目录下的东西**

**然后再重启vsftpd就可以生效了**