Netkiller Cisco IOS 手札

netkiller Neo Chan

2009-12-12

文档出处: http://netkiller.sourceforge.net/ | http://netkiller.github.com

文档最近一次更新于 Thu Dec 1 12:51:46 UTC 2011

下面是我多年积累下来的经验总结，整理成文档供大家参考:

Netkiller Architect 手札	Netkiller Linux 手札	Netkiller Developer 手札	Netkiller Database 手札
Netkiller Debian 手札	Netkiller CentOS 手札	Netkiller FreeBSD 手札	Netkiller Shell 手札
Netkiller Web 手札	Netkiller Monitoring 手札	Netkiller Storage 手札	Netkiller Mail System 手札
Netkiller MySQL 手札	Netkiller LDAP 手札	Netkiller Security 手札	Netkiller Version 手札
Netkiller Intranet 手札	Netkiller Cisco IOS 手札	Netkiller Writer 手札	Netkiller Studio Linux 手札

Support this project

目录

范例清单

5.1. desirable

下一页
自述

自述

目录

1. 内容简介

当前文档档容比较杂，涉及内容广泛。

慢慢我会将其中章节拆成新文档.

文档内容简介:

1. Network
2. Security
3. Web Application
4. Database
5. Storage And Backup/Restore
6. Cluster
7. Developer

1.1. Audience(读者对象)

This book is intended primarily for Linux system administrators who are familiar with the following activities:

Audience

1. Linux system administration procedures, including kernel configuration
2. Installation and configuration of cluster, such as load balancing, High Availability,
3. Installation and configuration of shared storage networks, such as Fibre Channel SANs
4. Installation and configuration of web server, such as apache, nginx, lighttpd, tomcat/resin ...

本文档的读者对象:

文档面向有所有读者。您可以选读您所需要的章节,无需全篇阅读,因为有些章节不一定对你有用,用得着就翻来看看,暂时用不到的可以不看.

大体分来读者可以分为几类:

1. 架构工程师
2. 系统管理员
3. 系统支持,部署工程师

不管是谁,做什么的,我希望通过阅读这篇文档都能对你有所帮助。

1.2. 写给读者

欢迎提出宝贵的建议,如有问题请到 邮件列表 讨论

为什么写这篇文章

有很多想法,工作中也用不到所以未能实现，所以想写出来,和大家分享.有一点写一点,写得也不好,只要能看懂就行,就当学习笔记了.

开始零零碎碎写过一些文档，也向维基百科供过稿，但维基经常被ZF封锁，后来发现sf.net可以提供主机存放文档，便做了迁移。并开始了我的写作生涯。

这篇文档是作者8年来对工作的总结,是作者一点一滴的积累起来的，有些笔记已经丢失，所以并不完整。

因为工作太忙整理比较缓慢。目前的工作涉及面比较窄所以新文档比较少。

我现在花在技术上的时间越来越少，兴趣转向摄影，无线电。也想写写摄影方面的心得体会。

写作动力:

曾经在网上看到外国开源界对中国的评价，中国人对开源索取无度，但贡献却微乎其微.这句话一直记在我心中，发誓要为中国开源事业做我仅有的一点微薄贡献

另外写文档也是知识积累，还可以增加在圈内的影响力.

人跟动物的不同,就是人类可以把自己学习的经验教给下一代人.下一代在上一代的基础上再创新,不断积累才有今天.

所以我把自己的经验写出来,可以让经验传承

没有内容的章节:

目前我自己一人维护所有文档，写作时间有限，当我发现一个好主题就会加入到文档中，待我有时间再完善章节，所以你会发现很多章节是空无内容的.

文档目前几乎是流水帐试的写作，维护量很大，先将就着看吧.

我想到哪写到哪,你会发现文章没一个中心,今天这里写点,明天跳过本章写其它的.
文中例子绝对多,对喜欢复制然后粘贴朋友很有用,不用动手写,也省时间.
理论的东西,网上大把,我这里就不写了,需要可以去网上查.
我爱写错别字,还有一些是打错的,如果发现请指正.
文中大部分试验是在Debian/Ubuntu/Redhat AS上完成.

1.3. 获得文档

1.3.1. PDF

Download PDF Document 下载PDF文档1

Download PDF Document 下载PDF文档2

1.3.2. EPUB

http://netkiller.sourceforge.net/technology.html

1.3.3. 获得光盘介质

如有特别需要，请联系我

---

2. 作者简介

主页地址：http://netkiller.sourceforge.net, http://netkiller.github.com/

陈景峰 (ㄔㄣˊ ㄐㄧㄥ ㄈㄥ)

Nickname：netkiller | English name: Neo chen | Nippon name: ちんけいほう (音訳) | Korean name: | Thailand name:

IT民工， UNIX like Evangelist, 业余无线电爱好者（呼号：BG7NYT）,户外运动以及摄影爱好者。

《PostgreSQL实用实例参考》，《Postfix 完整解决方案》，《Netkiller Linux 手札》的作者

2001年来深圳进城打工,成为一名外来务工者.

2002年我发现不能埋头苦干,埋头搞技术是不对的,还要学会"做人".

2003年这年最惨,公司拖欠工资16000元,打过两次官司2005才付清.

2004年开始加入分布式计算团队,目前成绩

2004-10月开始玩户外和摄影

2005-6月成为中国无线电运动协会会员

2006年单身生活了这么多年,终于找到归宿.

2007物价上涨,金融危机，休息了4个月（其实是找不到工作）

2008终于找到英文学习方法，，《Netkiller Developer 手札》，《Netkiller Document 手札》

2008-8-8 08:08:08 结婚,后全家迁居湖南省常德市

2009《Netkiller Database 手札》,年底拿到C1驾照

2010对电子打击乐产生兴趣，计划学习爵士鼓

2011 职业生涯路上继续打怪升级

2.1. 联系作者

Mobile: +86 13113668890

Tel: +86 755 2981-2080

Callsign: BG7NYT QTH: Shenzhen, China

注：请不要问我安装问题!

E-Mail: openunix@163.com
IRC irc.freenode.net #ubuntu / #ubuntu-cn

Yahoo: bg7nyt
ICQ: 101888222
AIM: bg7nyt

TM/QQ: 13721218
MSN: netkiller@msn.com
G Talk: 很少开
网易泡泡：很少开

写给火腿:

欢迎无线电爱好者和我QSO,我的QTH在深圳宝安区龙华镇溪山美地12B7CD,设备YAESU FT-50R,FT-60R,FT-7800 144-430双段机,拉杆天线/GP天线 Nagoya MAG-79EL-3W/Yagi

如果这篇文章对你有所帮助,请寄给我一张QSL卡片,qrz.cn or qrz.com or hamcall.net

Personal Amateur Radiostations of P.R.China

ZONE CQ24 ITU44 ShenZhen, China

Best Regards, VY 73! OP. BG7NYT

---

3. 支持这个项目(Support this project)

Donations

招商银行(China Merchants Bank) 陈景峰 9555500000007459

部分 I. Cisco IOS

目录

第 1 章 Terminal

目录

1. Putty

点击Serial

Serial line中填写COM1， Speed中填写9600

点击Open按钮即可

2. minicom - friendly serial communication program

```
sudo apt-get install minicom
```

环境变量

```
MINICOM='-m -c on'
export MINICOM
```

setup

```
neo@debian:~$ sudo minicom -s
```

TUI

```
+-----[configuration]------+
| Filenames and paths      |
| File transfer protocols  |
| Serial port setup        |
| Modem and dialing        |
| Screen and keyboard      |
| Save setup as dfl        |
| Save setup as..          |
| Exit                     |
| Exit from Minicom        |
+--------------------------+
```

选择 Serial port setup

```
    +-----------------------------------------------------------------------+
    | A -    Serial Device      : /dev/ttyS0                                |
    | B - Lockfile Location     : /var/lock                                 |
    | C -   Callin Program      :                                           |
    | D -  Callout Program      :                                           |
    | E -    Bps/Par/Bits       : 9600 8N1                                  |
    | F - Hardware Flow Control : Yes                                       |
    | G - Software Flow Control : No                                        |
    |                                                                       |
    |    Change which setting?                                              |
    +-----------------------------------------------------------------------+
            | Screen and keyboard      |
            | Save setup as dfl        |
            | Save setup as..          |
            | Exit                     |
            | Exit from Minicom        |
            +--------------------------+
```

使用A键和E键分别修改串口设备和波特率，然后ESC间推出，再将光标移动到Exit处按Enter键

```

Welcome to minicom 2.3

OPTIONS: I18n
Compiled on Sep 25 2009, 23:45:34.
Port /dev/ttyS0

               Press CTRL-A Z for help on special keys
```

```
Translating "z"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Switch>AT S7=45 S0=0 L1 V1 X4 &c1 E1 Q0
        ^
% Invalid input detected at '^' marker.

Switch>en
Password:
Switch#show
Switch#show running-config
Building configuration...

Current configuration : 3265 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.
enable password 123456
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip dhcp snooping information option
!
 --More--

 CTRL-A Z for help |  9600 8N1 | NOR | Minicom 2.3    | VT102 |      Offline
```

3. kermit

下载安装

```
neo@ubuntu:~$ apt-cache search kermit
gkermit - A serial and network communications package
modemu - Telnet services for communication programs
ckermit - a serial and network communications package

neo@ubuntu:~$ sudo apt-get install ckermit
```

改写kermit的配置文件/etc/kermit/kermrc

```
$ sudo vim /etc/kermit/kermrc

; This is /etc/kermit/kermrc
; It is executed on startup if ~/.kermrc is not found.
; See "man kermit" and http://www.kermit-project.org/ for details on
; configuring this file, and /etc/kermit/kermrc.full
; for an example of a complex configuration file

; If you want to run additional user-specific customisations in
; addition to this file, place them in ~/.mykermrc

; Execute user's personal customization file (named in environment var
; CKERMOD or ~/.mykermrc)
;

if def \$(CKERMOD) assign _myinit \$(CKERMOD)
if not def _myinit assign _myinit \v(home).mykermrc

xif exist \m(_myinit)  {                ; If it exists,
    echo Executing \m(_myinit)...       ; print message,
    take \m(_myinit)                    ; and TAKE the file.
}

set line /dev/ttyS0
set speed 9600
set carrier-watch off
set handshake none
set flow-control none
robust
set file type bin
set file name lit
set rec pack 1000
set send pack 1000
set window 5
```

console

```
$ kermit

C-Kermit>
C-Kermit>connect
```

现在就已经成功连接到串口com1了,并且你可以看到cisco console信息

切换

按下 Ctrl + \, 再按c可以跳回kermit

```
C-Kermit>
```

此时输入c,即connect即可连接到串口

```
neo@ubuntu:~$ kermit
C-Kermit 8.0.211, 10 Apr 2004, for Linux
 Copyright (C) 1985, 2004,
  Trustees of Columbia University in the City of New York.
Type ? or HELP for help.
(/home/neo/) C-Kermit>c
Connecting to /dev/ttyS0, speed 9600
 Escape character: Ctrl-\ (ASCII 28, FS): enabled
Type the escape character followed by C to get back,
or followed by ? to see other options.
----------------------------------------------------

Switch>
```

接下来你就可以配置交换机了

```


Switch>en
Password:
Switch#show running-config
Building configuration...

Current configuration : 3265 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.
enable password 123456
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip dhcp snooping information option
!
 --More--
```

4. 快捷键

快捷键:

```
1.Ctrl+A:把光标快速移动到整行的最开始
2.Ctrl+E:把光标快速移动到整行的最末尾
3.Esc+B:后退1个单词
4.Ctrl+B:后退1个字符
5.Esc+F:前进1个单词
6.Ctrl+F:前进1个字符
7.Ctrl+D:删除单独1个字符
8.Backspace:删除单独1个字符
9.Ctrl+R:重新显示1行
10.Ctrl+U:擦除1整行
11.Ctrl+W:删除1个单词
12. Ctrl+Z从全局模式退出到特权模式
13.Up arrow或者Ctrl+P:显示之前最后输入过的命令
14.Down arrow或者Ctrl+N:显示之前刚刚输入过的命令
```

第 2 章 show

目录

1. show version

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.4(3i), RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 28-Nov-07 21:09 by stshen

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

Router uptime is 49 minutes
System returned to ROM by power-on
System image file is "flash:c2800nm-ipbase-mz.124-3i.bin"

Cisco 2811 (revision 53.51) with 251904K/10240K bytes of memory.
Processor board ID FHK1152F1QF
2 FastEthernet interfaces
1 Channelized E1/PRI port
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2142
```

2. show line

3. show interfaces

FastEthernet0/0 is f0/0

```
Router#show interfaces
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 001e.7ae0.4740 (bia 001e.7ae0.4740)
  Internet address is 192.168.3.39/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 43000 bits/sec, 86 packets/sec
  5 minute output rate 6000 bits/sec, 9 packets/sec
     160163 packets input, 10159221 bytes
     Received 155086 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     6160 packets output, 732967 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 001e.7ae0.4741 (bia 001e.7ae0.4741)
  Internet address is 192.168.6.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 43000 bits/sec, 86 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     155406 packets input, 9677011 bytes
     Received 151563 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     509 packets output, 67569 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

3.1. show interfaces counters

```
# show interfaces counters

Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Fa0/1      2379327296184    10979280099            485         192752
```

```
Fa0/2       296014579556    1366095693           171         43447
Fa0/3      3183094910407    9958929000           315       3652593
Fa0/4      3390297882614   11050928174           208       3653027
Fa0/5       713746812545    2156063532           146       3506457
Fa0/6      5820647654184    5834009783            12         25417
Fa0/7      4082998183543    4738181544             8        664486
Fa0/8      3881386497397    3470425864           157         71607
Fa0/9      3448924790734    3574503546           258       1370329
Fa0/10     5359204222315    6336042807           219         61829
Fa0/11      443781559337     700314879           107         14633
Fa0/12      206467769769     474380960          1466          5332
Fa0/13     5014038301762    7032277335       1660694       1253268
Fa0/14     3328766937851    4771525509        115767        105209
Fa0/15      165277335824     150521964           141         27380
Fa0/16     6648033552242   34767920446             0        190169
Fa0/17       20059975664      37395851           130         34157
Fa0/18         959154299       5664538         12064         24836
Fa0/19      544011647073    1118388248           179          7907
Fa0/20        3198019694      43739891            47           597
Fa0/21    43920844537221   44221593064             0     126542762
Fa0/22                 0             0             0             0
Fa0/23     3591391278622   18628916636      16194340      45121928
Fa0/24     3089759856323   16570933097      16675291        952603
Gi0/1     19350417632314   23775137822      26153899      10372199
Gi0/2     26741429410404   32445020479       3709263       5652997

Port            OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Fa0/1      2314327534046   11138672916      29967451      30690533
Fa0/2       215863081281    1706941398      29983016      30883449
Fa0/3      6562564324539   11198668653      29982867      27270456
Fa0/4      8085972337363   12651412798      29982767      27270074
Fa0/5      1418549036203    2569992844      29972955      27396996
Fa0/6       912785966115    4805712756      29983511      30901354
Fa0/7       984705622618    3398551525      29983778      30262541
Fa0/8       425397050952    2912467841      29964019      30769573
Fa0/9       511529095198    3130871808      29983385      29556291
Fa0/10      828312555904    5667103408      29983198      30864778
Fa0/11      212566354130    1031479901      29983644      30912069
Fa0/12      233817196922     867262915      29984375      30922089
Fa0/13     4723454998834    7410676119      27180708      28269375

Port            OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Fa0/14     3623218726553    4971350097      28685555      29375918
Fa0/15      113927300309     356873845      11112762      16969115
Fa0/16    44239007226956   44566316209      29979292      30727856
Fa0/17      108413408330     277915584       5714898      13809813
Fa0/18       24028112089      29678877        423184         98235
Fa0/19      778949661871    1431822025       4716298      13693644
Fa0/20      183999500752     207737816       3321828       9477604
Fa0/21     6677881295074   35188153632      42517648      46074090
Fa0/22                 0             0             0             0
Fa0/23    43918173114274   44206559406      26657266     127495496
Fa0/24       20349553322      27745549      26176335     171664823
Gi0/1       4986490430392   21696238723       5500840      20555280
Gi0/2     14824142846314   28724855823      27944285      25274493
```

3.2. show ip interface brief

```
#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  172.16.0.254    YES NVRAM  up                    up
Vlan2                  unassigned      YES NVRAM  up                    up
Vlan3                  192.168.3.1     YES NVRAM  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
GigabitEthernet1/0/11  unassigned      YES unset  up                    up
GigabitEthernet1/0/12  unassigned      YES unset  up                    up
GigabitEthernet1/0/13  unassigned      YES unset  up                    up
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  up                    up
GigabitEthernet1/0/16  unassigned      YES unset  up                    up
GigabitEthernet1/0/17  unassigned      YES unset  up                    up
```

```
GigabitEthernet1/0/18  unassigned      YES unset  up                    up
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  up                    up
GigabitEthernet1/0/22  unassigned      YES unset  up                    up
GigabitEthernet1/0/23  unassigned      YES unset  up                    up
GigabitEthernet1/0/24  unassigned      YES unset  down                  down
GigabitEthernet1/0/25  unassigned      YES unset  down                  down
GigabitEthernet1/0/26  unassigned      YES unset  down                  down
GigabitEthernet1/0/27  unassigned      YES unset  down                  down
GigabitEthernet1/0/28  unassigned      YES unset  down                  down
GigabitEthernet2/0/1   unassigned      YES unset  up                    up
GigabitEthernet2/0/2   unassigned      YES unset  down                  down
GigabitEthernet2/0/3   unassigned      YES unset  down                  down
GigabitEthernet2/0/4   unassigned      YES unset  up                    up
GigabitEthernet2/0/5   unassigned      YES unset  up                    up
GigabitEthernet2/0/6   unassigned      YES unset  down                  down
GigabitEthernet2/0/7   unassigned      YES unset  up                    up
GigabitEthernet2/0/8   unassigned      YES unset  down                  down
GigabitEthernet2/0/9   unassigned      YES unset  down                  down
GigabitEthernet2/0/10  unassigned      YES unset  down                  down
GigabitEthernet2/0/11  unassigned      YES unset  down                  down
GigabitEthernet2/0/12  unassigned      YES unset  down                  down
GigabitEthernet2/0/13  unassigned      YES unset  up                    up
GigabitEthernet2/0/14  unassigned      YES unset  down                  down
GigabitEthernet2/0/15  unassigned      YES unset  up                    up
GigabitEthernet2/0/16  unassigned      YES unset  down                  down
GigabitEthernet2/0/17  unassigned      YES unset  up                    up
GigabitEthernet2/0/18  unassigned      YES unset  down                  down
GigabitEthernet2/0/19  unassigned      YES unset  up                    up
GigabitEthernet2/0/20  unassigned      YES unset  down                  down
GigabitEthernet2/0/21  unassigned      YES unset  up                    up
GigabitEthernet2/0/22  unassigned      YES unset  down                  down
GigabitEthernet2/0/23  unassigned      YES unset  up                    up
GigabitEthernet2/0/24  unassigned      YES unset  up                    up
GigabitEthernet2/0/25  unassigned      YES unset  down                  down
GigabitEthernet2/0/26  unassigned      YES unset  down                  down
GigabitEthernet2/0/27  unassigned      YES unset  down                  down
GigabitEthernet2/0/28  unassigned      YES unset  down                  down
Port-channel1          unassigned      YES unset  up                    up
Port-channel2          unassigned      YES unset  up                    up
Port-channel3          unassigned      YES unset  up                    up
Port-channel4          unassigned      YES unset  down                  down
Port-channel5          unassigned      YES unset  down                  down
Port-channel17         unassigned      YES unset  up                    up
Port-channel19         unassigned      YES unset  down                  down
```

3.3. show interface status

```
#show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      connected    100        a-full a-1000
10/100/1000BaseTX
Gi1/0/2                      connected    100        a-full a-1000
10/100/1000BaseTX
Gi1/0/3                      notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/5                      notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/6                      notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/7                      connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/8                      connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/9                      connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/10                     connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/11                     connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/12                     connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/13                     connected    10         a-half   a-10
10/100/1000BaseTX
Gi1/0/14                     notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/15                     connected    11         a-full a-1000
```

```
10/100/1000BaseTX
Gi1/0/16                  connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/17                  connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/18                  connected    1          a-full a-1000
10/100/1000BaseTX
Gi1/0/19                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/20                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/21                  connected    2          a-full  a-100
10/100/1000BaseTX
Gi1/0/22                  connected    2          a-full a-1000
10/100/1000BaseTX
Gi1/0/23                  connected    2          a-full a-1000
10/100/1000BaseTX
Gi1/0/24                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi1/0/25                  notconnect   1            auto   auto Not Present
Gi1/0/26                  err-disabled 1            auto   auto Not Present
Gi1/0/27                  notconnect   1            auto   auto Not Present
Gi1/0/28                  err-disabled 1            auto   auto Not Present
Gi2/0/1                   connected    70         a-full  a-100
10/100/1000BaseTX
Gi2/0/2                   notconnect   70           auto   auto
10/100/1000BaseTX
Gi2/0/3                   notconnect   80           auto   auto
10/100/1000BaseTX
Gi2/0/4                   connected    80         a-full  a-100
10/100/1000BaseTX
Gi2/0/5                   connected    1          a-full  a-100
10/100/1000BaseTX
Gi2/0/6                   notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/7                   connected    trunk      a-full a-1000
10/100/1000BaseTX
Gi2/0/8                   notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/9                   notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/10                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/11                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/12                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/13                  connected    trunk      a-full a-1000
10/100/1000BaseTX

Port      Name              Status       Vlan       Duplex  Speed Type
Gi2/0/14                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/15                  connected    trunk      a-full a-1000
10/100/1000BaseTX
Gi2/0/16                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/17                  connected    trunk      a-full a-1000
10/100/1000BaseTX
Gi2/0/18                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/19                  connected    trunk      a-full a-1000
10/100/1000BaseTX
Gi2/0/20                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/21                  connected    trunk      a-full a-1000
10/100/1000BaseTX
Gi2/0/22                  notconnect   1            auto   auto
10/100/1000BaseTX
Gi2/0/23                  connected    trunk      a-full a-1000
10/100/1000BaseTX
Gi2/0/24                  connected    1          a-full a-1000
10/100/1000BaseTX
Gi2/0/25                  notconnect   1            auto   auto Not Present
Gi2/0/26                  notconnect   1            auto   auto Not Present
Gi2/0/27                  notconnect   1            auto   auto Not Present
Gi2/0/28                  notconnect   1            auto   auto Not Present
Po1                       connected    1          a-full a-1000
Po2                       connected    1          a-full a-1000
Po3                       connected    1          a-full a-1000
Po4                       notconnect   1            auto   auto
Po5                       notconnect   1            auto   auto
Po17                      connected    1          a-full a-1000
Po19                      notconnect   1            auto   auto
```

4. show ip arp

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.3.123          21   001c.23f9.d931  ARPA   FastEthernet0/0
Internet  192.168.3.75            7   0025.648f.c6be  ARPA   FastEthernet0/0
Internet  192.168.3.39            -   001e.7ae0.4740  ARPA   FastEthernet0/0
Internet  192.168.3.10           24   0025.64a3.59bf  ARPA   FastEthernet0/0
Internet  192.168.3.1             0   001f.1255.a902  ARPA   FastEthernet0/0
Internet  192.168.6.5            10   0025.648f.c6be  ARPA   FastEthernet0/1
Internet  192.168.6.1             -   001e.7ae0.4741  ARPA   FastEthernet0/1

#show arp | in 172.16.1.2

#show mac-address-table dynamic interface Fa0/3
```

5. show mac-address-table

```
#show mac-address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    000d.482c.183e    DYNAMIC     Gi1/0/24
   1    000f.e207.f2e0    DYNAMIC     Gi1/0/16
   1    000f.e285.0b10    DYNAMIC     Gi1/0/16
   1    0024.e834.29ea    DYNAMIC     Gi1/0/24
...
...
 100    f04d.a2d9.9b30    DYNAMIC     Gi1/0/22
 200    04fe.7f45.c31a    DYNAMIC     Gi1/0/22
Total Mac Addresses for this criterion: 501
```

5.1. 通过mac查找端口

```
Switch-2960-WAN-0#show mac-address-table dynamic add 001c.58b5.6e81
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    001c.58b5.6e81    DYNAMIC     Fa0/16
Total Mac Addresses for this criterion: 1
```

6. show mac address dy

```
Switch-2960-WAN-0#show mac address dy
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    001b.789e.0fd8    DYNAMIC     Gi0/1
   1    001b.789e.0fda    DYNAMIC     Fa0/9
   1    001c.58b5.6e81    DYNAMIC     Fa0/16
   1    001c.c45e.5f68    DYNAMIC     Fa0/10
   1    001d.0922.7438    DYNAMIC     Fa0/8
   1    001d.0922.743a    DYNAMIC     Gi0/1
   1    001d.0926.1cce    DYNAMIC     Fa0/3
   1    001d.0926.1cd0    DYNAMIC     Gi0/1
   1    001d.0926.e5e7    DYNAMIC     Fa0/4
   1    001d.0926.e5eb    DYNAMIC     Fa0/4
   1    001d.0926.fa35    DYNAMIC     Fa0/5
   1    001d.0926.fac6    DYNAMIC     Gi0/2
   1    001d.09f0.ac07    DYNAMIC     Fa0/2
   1    001d.09f0.ad12    DYNAMIC     Fa0/1
   1    001d.09f0.ad13    DYNAMIC     Gi0/1
   1    001e.0bd9.f4c2    DYNAMIC     Fa0/12
   1    001e.c9b4.62cc    DYNAMIC     Gi0/2
   1    001e.c9b4.62ce    DYNAMIC     Gi0/1
   1    001e.c9b8.9124    DYNAMIC     Gi0/2
   1    001e.c9df.4843    DYNAMIC     Gi0/2
   1    001e.c9df.4fde    DYNAMIC     Gi0/2
   1    001e.c9df.50f5    DYNAMIC     Fa0/6
   1    001e.c9df.5104    DYNAMIC     Fa0/7
   1    001e.c9df.5106    DYNAMIC     Gi0/1
   1    001e.c9df.5113    DYNAMIC     Gi0/2
```

7. show ip route

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

C    192.168.6.0/24 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.3.1
```

8. show ip protocols

9. show access-lists

```
Router#show access-lists
```

```
asa5550# sh access-list | include udp
asa5550# sh access-list | exclude 172.16.1.254
```

10. show vlans

```
Router# show vlans

No Virtual LANs configured.
```

11. show log

```
Router#show log
Syslog logging: enabled (1 messages dropped, 3 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 22 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: disabled, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 26 message lines logged
```

12. show flash

```
Router#show flash
-#- --length-- -----date/time------ path
1     15679252 Dec 27 2007 01:37:22 +00:00 c2800nm-ipbase-mz.124-3i.bin
2         1823 Dec 27 2007 01:45:46 +00:00 sdmconfig-2811.cfg
3      6036480 Dec 27 2007 01:46:24 +00:00 sdm.tar
4       861696 Dec 27 2007 01:46:46 +00:00 es.tar
5      1164288 Dec 27 2007 01:47:04 +00:00 common.tar
6         1038 Dec 27 2007 01:47:20 +00:00 home.shtml
7       113152 Dec 27 2007 01:47:36 +00:00 home.tar
8      1697952 Dec 27 2007 01:48:04 +00:00 securedesktop-ios-3.1.1.45-k9.pkg
9       416354 Dec 27 2007 01:48:24 +00:00 sslclient-win-1.1.3.173.pkg

38027264 bytes available (25989120 bytes used)
```

13. show cdp nei

```
show cdp nei
show cdp ne de
```

14. config

```
Router#show running-config
Router#show startup-config
```

第 3 章 Debug

目录

1. DHCP

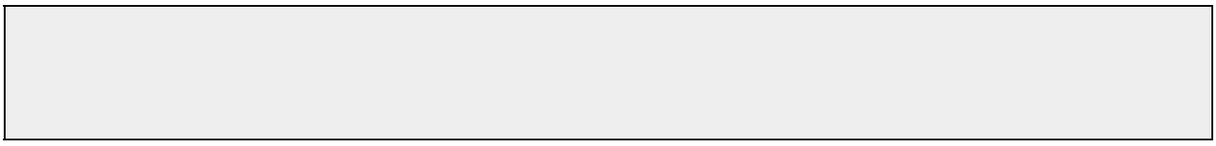
```
debug ip dhcp server packet
```

2. debug ip rip

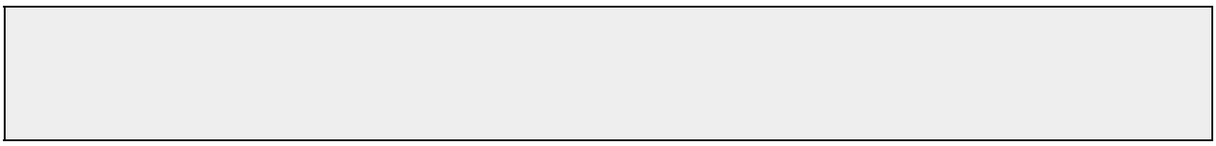
```
Router# debug ip dhcp server packet

*Dec 19 04:51:25.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Dec 19 04:51:26.583: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Dec 19 04:51:41.275: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Dec 19 04:51:42.643: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:51:46.643: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:51:55.643: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:52:10.639: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:52:47.639: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:52:50.635: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:52:58.635: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:53:13.635: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/0.
*Dec 19 04:53:14.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Dec 19 04:53:17.271: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
*Dec 19 04:53:19.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Dec 19 04:53:26.339: DHCPD: DHCPDISCOVER received from client 0100.50ba.eefa.d0
on interface FastEthernet0/1.
*Dec 19 04:53:26.339: DHCPD: Sending DHCPOFFER to client 0100.50ba.eefa.d0
(10.10.0.2).
*Dec 19 04:53:26.339: DHCPD: Including FQDN option name 'NEO.' rcode1=0, rcode2=0
flags=0x0
*Dec 19 04:53:26.339: DHCPD: broadcasting BOOTREPLY to client 0050.baee.fad0.
*Dec 19 04:53:26.343: DHCPD: DHCPREQUEST received from client 0100.50ba.eefa.d0.
*Dec 19 04:53:26.343: DHCPD: No default domain to append - abort update
*Dec 19 04:53:26.343: DHCPD: Sending DHCPACK to client 0100.50ba.eefa.d0
(10.10.0.2).
*Dec 19 04:53:26.343: DHCPD: broadcasting BOOTREPLY to client 0050.baee.fad0.
*Dec 19 04:53:31.143: DHCPD: DHCPREQUEST received from client 0100.50ba.eefa.d0.
*Dec 19 04:53:31.143: DHCPD: No default domain to append - abort update
*Dec 19 04:53:31.143: DHCPD: Sending DHCPACK to client 0100.50ba.eefa.d0
(10.10.0.2).
*Dec 19 04:53:31.143: DHCPD: unicasting BOOTREPLY to client 0050.baee.fad0
(10.10.0.2).
```

3. debug ip igrp

debug ip igrp events



debug ip igrp transactions



4. nat

debug nat

```
Router#term mon
Router#debug ip nat detailed
```

5. Switch all debugging off no debug all

```
no debug all
undebug all
```

第 4 章 Route

目录

1. reset password

reboot route and then pass Ctrl + Break

```
rommon 3 > confreg 0x2142
rommon 4 > reset
```

```
Router>enable
```

```
Password:
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#config-register 0x2102
Router(config)#end
Router#reload
```

2. config

```
Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

2.1. copy

Cisco Router Copy Commands

```
Requirement     Cisco Command
Save the current configuration from DRAM to NVRAM
copy running-config startup-config

Merge NVRAM configuration to DRAM
copy startup-config running-config

Copy DRAM configuration to a TFTP server
copy runing-config tftp

Merge TFTP configuration with current router configuration held in DRAM
copy tftp runing-config

Backup the IOS onto a TFTP server
copy flash tftp

Upgrade the router IOS from a TFTP server
copy tftp flash
```

3. hostname

```
Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Neo
Neo(config)#
```

4. Password

更改路由器名、密码

```
Router(config)#
Router(config)#enable password cisco            enable password和enable secret命令可以修改特权模式的密码。
Router(config)#enable secret cisco                          进入line console局部配置模式下，修改console登录密码；进入line vty局部配置模式，修改telnet登录的密码。login命令指出需要登录，修改密码的命令都是password。
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password cisco
```

5. Interface

2811

```
Controller Timeslots D-Channel Configurable modes Status
E1 0/0/0   31        15        pri/channelized     Administratively up

Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            192.168.3.123   YES manual up                    up
FastEthernet0/1            172.16.0.254    YES manual up                    down
```

controller E1 0/0/0

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#controller E1 0/0/0
Router(config)#channel-group 0 unframedINIT2U
Router(config)#interface Serial0/0/0:0%][
Router(config)#ip address 144.*.*.* 255.255.255.252
```

f0/0 ~ f0/1

```
Router>en
Router#conf t
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#int s0/0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#host R1
R1(config)#ip route 192.168.2.0 255.255.255.0 s0/0
R1(config)#end
```

default gateway

```
ip default-gateway 210.22.111.193
```

5.1. description

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/1
Router(config-if)#des
Router(config-if)#description Connect to Cisco 2960 Switch f0/24
Router(config-if)#end
```

running-config

```
Router#show running-config

!
interface FastEthernet0/1
 description Connect to Cisco 2960 Switch f0/24
 ip address 172.16.0.254 255.255.255.0
 duplex auto
 speed auto
!
```

5.2. bandwidth

```
Router(config-if)bandwidth 64
Note that the zeroes are not missing
```

5.3. primary/secondary

```
Router#sh run

interface Serial0
ip address 10.250.1.10 255.255.255.252
no ip proxy-arp
encapsulation ppp
no fair-queue
no cdp enable
hold-queue 150 out
!
interface FastEthernet0
ip address 61.63.15.190 255.255.255.192 primary
ip address 61.63.44.190 255.255.255.192 secondary
no ip proxy-arp
speed auto
```

6. DHCP

```
ip dhcp excluded 192.168.0.1 （排除的IP）
ip dhcp pool xxx（随便你定义的名字）
network 192.168.0.0 255.255.255.0 （你分配的IP段）
default-router 192.168.0.1 （关网的网内）
dns-server 202.96.64.68 （DNS服务器的IP）
lease 7
netbios-name-server

Router>en
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded 10.10.0.1 10.10.0.254
Router(config)#ip dhcp pool office
Router(dhcp-config)#network 10.10.0.0 255.255.255.0
Router(dhcp-config)#default-router 10.10.0.254
Router(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Router(dhcp-config)#netbios-name-server 10.10.0.2
Router(dhcp-config)#lease 7
Router(dhcp-config)#end
Router#
```

6.1. OpenDNS

```
dns-server 208.67.222.222
dns-server 208.67.220.220
```

7. 路由协议

7.1. 静态路由

enable routing

```
Router(config)#ip routing
```

```
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.3.1
Router(config)#ip route 172.16.0.0 255.255.255.0 172.16.0.254
Router(config)#ip route 192.168.5.0 255.255.255.0 192.168.5.1
```

```
!--- The default route is configured and points to 192.168.1.2.
ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

remove route

```
no ip route 1.1.1.0 255.255.255.0 fastEthernet 0/0
```

save

```
copy run sta
```

debug rip

```
testBJ#debug ip rip
```

7.2. RIP

enable rip

```
Switch>en                           //进入特权模式
Switch#conf t                       //进入全局模式
Switch(config)#router rip   //启动rip进程
Switch(config-router)#network 192.168.1.0    //宣告网络192.168.1.0
Switch(config-router)#ex    //退出到全局模式
```

disable rip

```
Router(config)#no router rip
```

7.3. IGRP

enable igrp

```
Router(config)#router igrp 200
Router(config-router)#network 172.16.0.0
```

Disable IGRP

```
Router(config)#no router igrp 200
```

7.4. PBR

---

8. NAT

```
需求如下:
CISCO2621路由器需要做NAT地址转换
内网是192.168.1.0 192.168.2.0 两个网段上网
外口是218.98.0.1
NAT地址是外口地址


配置:
interface Fastethernet 0/0
ip address 218.98.0.1 255.255.255.0
ip nat outside

interface fastethernet 0/1
ip address 192.168.1.1 255.255.254.0
ip nat inside

ip nat pool aaa 218.98.0.1 218.98.0.1 netmask 255.255.255.0
ip nat inside source list 1 pool aaa
access-list 1 permit 192.168.1.0 0.0.1.255


ip nat pool office 192.168.3.123 192.168.3.123 netmask 255.255.255.0
ip nat inside source list 1 pool office
access-list 1 permit 192.168.3.0 0.0.0.255
```

port mapped

```
ip nat inside source static tcp 172.16.1.1 80 192.168.1.3 500 extendable
```

show ip nat translation

```
Router#show ip nat translation
```

8.1. IP 映射

```
ena

conf t

ip nat inside source static 192.168.1.4 200.200.200.200

int f0/0

ip nat outside

no shut

int f0/1

ip nat inside

no shut
```

8.2. 端口映射

```
至少做两条NAT，因为FTP有两个端口，20，21，一个数据，一个指令

端口映射:
ip nat inside source static tcp 192.168.1.4 21 200.200.200.200 21
ip nat inside source static tcp 192.168.1.4 20 200.200.200.200 20

在外网的接口（你的f0/0）上配置
Router（config-if）#ip nat outside（只能有一个出接口）
在内网的接口（你的f0/1）上配置
Router（config-if）#ip nat inside（可以有多个进接口）
```

8.3. example 1

cisco上做端口映射，要求192.168.0.180:8000和192.168.0.181：8000分别映射外网202.122.111.66的3000和3002端口 其他192.168.0.0/24的主机可以上网，具体配置

```
int fa0/0
ip nat inside
int fa0/1
ip nat outside

全局模式:
access-list 10 permit any
ip nat inside source list 10 interface fa0/1 overload

端口映射:
ip nat inside source static tcp 192.168.0.180 8000 interface fa0/1 3000
ip nat inside source static tcp 192.168.0.181 8000 interface fa0/1 3002

interface fa0/1是外网的端口
```

9. 限制流量

9.1. rate-limit

在Cisco设备中，只有支持思科快速转发（CEF，Cisco Express Forward)的路由器或交换机才能使用rate-limit来限制流量，具体设置分三步

1. 在全局模式下开启cef:
```
configure terminal
Router(config)#ip cef
```
2. 定义标准或者扩展访问列表（定义一个方向就可以了）:
```
Router(config)#access-list 111 permit ip 192.168.1.0 0.0.0.255 any
```
3. 在希望限制的端口上进行rate-limit:
```
Router(config)#interface FastEthernet 0/1
Rounter(config-if)#rate-limit input access-group 111 2000000 40000 60000 conform-action transmit exceed-action drop
```

这样我们就对192.168.1.0网段进行了限速，速率为2Mbps。注意，是对整个网段，因为你定义的ACL就是针对整个网段的。

rate-limit命令格式:

```
#rate-limit {input|output} [access-group number] bps burst-normal burst-max conform-action action exceed-action action
```

input|output：这是定义数据流量的方向。

access-group number：定义的访问列表的号码。

bps：定义流量速率的上限，单位是bps。

burst-normal burst-max：定义的数据容量的大小，一般采用8000，16000，32000，单位是字节，当到达的数据超过此容量时，将触发某个动作，丢弃或转发等，从而达到限速的目的。

conform-action和exceed-action：分别指在速率限制以下的流量和超过速率限制的流量的处理策略。

action：是处理策略，包括drop和transmit等

10. PPPoE

```
假设E0接内网，E1接ADSL上外网
第一步:配置vpdn
vpdn enable(启用路由器的虚拟专用拨号网络---vpnd)
vpdn-group office(建立一个vpdn组,)
request-dialin(初始化一个vpnd tunnel,建立一个请求拨入的vpdn子组,)
protocol pppoe(vpdn子组使用pppoe建立会话隧道)

第二步: 配置路由器连接adsl modem的接口
interface Ethernet1
no ip address
pppoe enable允许以太接口运行pppoe
pppoe-client dial-pool-number 1将以太接口的pppoe拨号客户端加入拨号池1

第三步:配置逻辑拨号接口:
interface Dialer1
ip address negotiated从adsl服务商动态协商得到ip地址
ip nat outside为该接口启用NAT
encapsulation ppp为该接口封装ppp协议
dialer pool 1该接口使用1号拨号池进行拨号
dialer-group 1该命令对于pppoe是意义不大的
ppp authentication pap callin启用ppp pap验证
ppp pap sent-username bnnXXXXX password  XXXXX使用已经申请的用户名和口令

第四步:配置内部网络接口
interface Ethernet0(内部网络接口)
ip address 10.1.1.1 255.255.255.0
ip nat inside为该接口启用NAT

第五步:配置路由器为内部网络主机提供dhcp服务
ip dhcp excluded-address 10.1.1.1
ip dhcp pool ABC
import all(导入dns和wins server)
network 10.1.1.0 255.255.255.0
default-router 10.1.1.1

第六步:配置NAT:
access-list 1 permit 10.1.1.0 0.0.0.255
ip nat inside source list 1 interface Dialer1 overload

第七步:配置缺省路由
ip route 0.0.0.0 0.0.0.0 Dialer1
```

11. ACLs

11.1. 基本配置

show access-list

```
Extended IP access list 101
    10 permit tcp any any eq www (534 matches)
    20 deny tcp any any (111 matches)
```

Removing ACLs

```
no access-list <list number>
```

Here is an example:

permit all

```
access-list 101 permit tcp any any
access-list 101 permit udp any any
access-list 101 permit icmp any any
```

deny all

```
access-list 101 deny tcp any any
access-list 101 deny udp any any
access-list 101 deny icmp any any
```

Applying Access Lists

```
conf t
int f0/0
access-group 101 out
access-group 102 in
```

11.2. www

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny tcp any any
Router(config)#access-list 101 deny udp any any
Router(config)#access-list 101 deny icmp any any
Router(config)#int f0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#end
```

www

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit tcp any any eq www
Router(config)#access-list 101 deny tcp any any
```

```
Router(config)#end
Router#
```

11.3. show access-list

```
# sh access-list | include udp
```

上一页
10. PPPoE

上一级
起始页

下一页
12. reload

12. reload

```
Router#reload
```

第 5 章 Switch

目录

Cisco 固定配置交换机命名规则

对于Cisco的固定配置的交换机，一般有3750，3550，3560，2960，2970这几个系列。

它们在型号命令上有自己相应的规则，特总结如下：

eg: WS-C3750G-48TS-S

C3750表明这款产品属于3750这个系列，也就是产品的型号。

G----表明其所有接口都是支持千兆或以上，如果没有这个就表明其主要端口都是10/100M的或者100M的

48----表明其拥有主要的端口数量为48个

T----表明其主要端口是电口（也就是所谓的Twirst Pair的端口

P----表明其主要端口是电口，同时支持PoE以太网供电

S----表明其带的扩展的接口为SFP类型的接口

最后部分的-S表明交换机带的软件是SMI标准影像的,-E表明是EMI影像的

1. 交换机初始化

Cisco Catalyst 2960 Series Switches

```
Press RETURN to get started!


*Mar  1 00:00:25.073: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to down
*Mar  1 00:00:26.189: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for typ
e vlan
*Mar  1 00:00:47.102: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, REL
EASE SOFTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 18:10 by gereddy


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]:

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: chen

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: chen
% Please choose a password that is different from the enable secret
  Enter enable password: chen

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: chen
  Configure SNMP Network Management? [no]: yes
    Community string [public]:

Current interface summary
```

```
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  up                    down
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down

Enter interface name used to connect to the
management network from the above interface summary: FastEthernet0/24

Configuring interface FastEthernet0/24:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 172.16.0.253
    Subnet mask for this interface [255.255.0.0] :
    Class B network is 172.16.0.0, 16 subnet bits; mask is /16
Would you like to enable as a cluster command switch? [yes/no]: yes
Enter cluster name: cl1

The following configuration command script was created:

hostname Switch
enable secret 5 $1$W1RW$ZdWR.sS/g2RwJMv4F5sRq0
enable password chen
line vty 0 15
password chen
snmp-server community public
!
!
interface Vlan1
shutdown
no ip address
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
 --More--
```

1.1. 密码设置

基本操作

```
Switch command
Switch > en 进入特权模式
Switch # conf t 进入全局配置模式
Switch (config) # interface interface-num 进入接口
Switch (config) # hostname name 给交换机命名
Switch (config) # enable password password 设置明文密码
Switch (config) # enable secret password 设置加密的启用秘密口令。如果设置则取代明文口令
Switch # copy running-config startup-config
Switch # write 保存设置
```

1.2. 域名，网管

初始化设置

```
Switch setup
switch (config) # ip default-gateway ip-address
switch (config) # ip domain-name domain-name
switch (config) # ip name-server IP-address 交换机上设置远程访问,用于交换机管理
```

1.3. Telnet

通过Telnet进入命令行接口

```
Switch>enable
Switch#conf t
Switch(config)#line vty 0 4
Switch(config－line)#login
Switch(config－line)#password cisco
```

1.3.1. privilege level

```
line vty 5 15
 privilege level 15
 password neo
 login
!
```

1.4. 保存当前配置

Save

```
Switch#wr
Building configuration...
[OK]
```

1.5. 恢复交换机出厂值

```
Switch# erase startup-config
```

2. interface

2.1. show interfaces status

```
show interfaces status
```

2.2. ip address

DHCP

```
ip address dhcp
```

指定IP地址

```
ip address 192.20.135.21 255.255.255.0
```

2.3. 配置端口速率及双工模式

Step 1 configure terminal 进入配置状态.
Step 2 interface interface-id 进入端口配置状态.
Step 3 speed {10 | 100 | 1000 | auto | nonegotiate} 设置端口速率 注 1000 只工作在千兆口. GBIC模块只工作在1000 Mbps下. nonegotiate 只能在这些GBIC上用 1000BASE-SX, -LX, and -ZX GBIC.
Step 4 duplex {auto | full | half} 设置全双工或半双工.
Step 5 end 退出
Step 6 show interfaces interface-id 显示有关配置情况
Step 7 copy running-config startup-config 保存

```
Switch# configure terminal
Switch(config)# interface fastethernet0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

2.4. range

```
Switch# configure terminal

Switch(config)# interface range fastethernet0/1 - 5

Switch(config-if-range)# no shutdown
Switch(config-if-range)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/05,
changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed
state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/4, changed
state to up
```

同时选择多个端口

```
Switch# configure terminal

Switch(config)# interface range fastethernet0/1 - 3, gigabitethernet0/1 - 2

Switch(config-if-range)# no shutdown
Switch(config-if-range)#
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to
up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/ 1,
changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/
2,
changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/
3,
changed state to up
```

2.5. 端口隔离

```
Switch(config)# interface 端口号
Switch(config-if)# switchitchport protected //开启端口保护功能
```

注：思科个别型号交换机采用PVLAN来实现端口保护功能

3. DHCP

关闭DHCP服务

```
no service dhcp
```

开启DHCP服务

```
Switch(config)#service dhcp
```

```
ip dhcp pool global //global是pool name， 由用户指定

   network 10.1.0.0 255.255.0.0 //动态分配的地址段

        default-router 10.1.1.100 10.1.1.101 //为客户机配置默认网关

   domain-name client.com //为客户机配置域后缀

   dns-server 10.1.1.1 10.1.1.2 //为客户机配置dns服务器

   netbios-name-server 10.1.1.5 10.1.1.6 //为客户机配置wins服务器

   netbios-node-type h-node //为客户机配置节点模式（影响名称解释的顺利,如h-node=先通过wins服务器解释...）

   lease 3 //地址租用期限: 3天
```

VLAN 指定DHCP地址

```
 ip helper-address 10.1.1.8 //假设这是DHCP客户机所在的VLAN
```

3.1. Gateway

显示地址分配情况

```
show ip dhcp binding
```

显示地址冲突情况

```
show ip dhcp conflict
```

观察DHCP服务器工作情况

```
debug ip dhcp server {events | packets | linkage}
```

3.2. snooping

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 2
```

```
Switch(config)#ip dhcp snooping vlan 3
or
Switch(config)#ip dhcp snooping vlan 2-3
Switch(config)#ip dhcp snooping verify mac-address
Switch(config)#ip dhcp snooping information option
Switch(config)#int range f0/1-12
Switch(config-if-range)#ip dhcp snooping trust
Switch(config-if-range)#ip dhcp snooping limit rate 15
```

3.3. DHCP中继代理

```
Switch(config)#service dhcp
Switch(config)#ip dhcp replay infomation option
```

4. Route port

no switchport

```
Switch# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2

Switch(config-if)# no switchport

Switch(config-if)# ip address 192.20.135.21 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# end
```

5. 交换机端口镜像配置

举例：通过交换机的第2号口监控第1号口的流量

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
Switch(config)# end
```

删除一个span会话:

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end
```

6. Ethernet Port Groups

SwitchA

```
SwitchA# configure terminal
SwitchA (config)# interface range GigabitEthernet1/1-2
SwitchA (config-if-range)# switchport mode access
SwitchA (config-if-range)# switchport access vlan 10
SwitchA (config-if-range)# channel-group 5 mode on
Switch(config-if-range)# end
```

SwitchB

```
SwitchB# configure terminal
SwitchB(config)#interface range GigabitEthernet1/0/1-2
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 10
SwitchB(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1

SwitchB(config-if-range)#int port-channel 1
SwitchB(config-if)#exit
SwitchB(config)#do show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Gi1/0/1(P) Gi1/0/2(P)
```

6.1. LACP

channel-group 4 mode active 这个命令控制是否用LACP的。

```
c4506(config)#inter g6/5
c4506(config-if)#channel-group 4 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected

c4506(config-if)#channel-group 4 mode active
```

6.2. desirable

例 5.1. desirable

switch A

```
Switch(config)#interface range fa0/1-4
#range配置二个以上的接口
Switch(config-if-range)#channel-group 1 mode desirable          #封装为自动协商模式
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport trunk allowed vlan all       #允许所以vlan通过
```

switch B

```
Switch(config)#interface range fa0/1-4
Switch(config-if-range)#channel-group 1 mode desirable
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport trunk allowed vlan all
```

7. VLAN

7.1. vlan database

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#
*Mar  1 00:29:54.407: %SYS-5-CONFIG_I: Configured from console by console
Switch(vlan)#show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 2
    Name: server
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 3
    Name: office
    Media Type: Ethernet
    VLAN 802.10 Id: 100003
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 1003
    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 1500
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    STP Type: IEEE
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No
```

```
  VLAN ISL Id: 1005
    Name: trnet-default
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    STP Type: IBM
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

Switch(vlan)#
```

7.2. 两层Switch配置讲解

路由器配制

```
Router#configure terminal

Router(config)#interface f0/0

Router(config-if)#no shutdown

Router(config-if)#interface f0/0.1 ---------------- 创建子接口1

Router(config-subif)#encapsulation dot1q 2  ------ 2为VLAN号 对应VLAN 2

Router(config-subif)#ip address 10.10.11.1 255.255.255.0

Router(config-if)#interface f0/0.2 ----------------- 创建子接口2

Router(config-subif)#encapsulation dot1q 3  ------- 3为VLAN号 对应VLAN 3

Router(config-subif)#ip address 10.10.10.1 255.255.255.0

路由器已经配制完毕，可以在Router#show run 看一下当前的配制，用Router#show interfaces 看当前端口的状态，f0/0.1 和f0/0.2两个子

接口是否为up状态。
```

交换机配制

```
Switch#vlan database

Switch(vlan)#vlan 2  name 财务部 ------- 创建vlan 2为财务部

Switch(vlan)#vlan 3 name  市场部----------创建vlan 3为市场部

Switch(vlan)#exit

Switch configure terminal

Switch(coning)#interface  range f0/2 - 9

Switch(coning-if)#switch port access vlan 2 ------- 将f0/-f0/9端口分到vlan 2中

Switch(config-if)#interface range f0/10 - 14

Switch(config-if)#switchport access vlan 3 --------将端f0/10至f0/14口3分到vlan 3中

Switch(config-if)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q ------将端口封装

Switch(config-if)#switchport mode trunk  -------- 将端口配制为trunk模式
```

客户端配制：

```
WorKstation 1 配制为: 10.10.11.3 255.255.255.0 网关: 10.10.11.1
Workstation 2 配制为: 10.10.10.3 255.255.255.0 网关: 10.10.10.1
```

7.3. 3 Layer Switch

3560交换机VLAN间路由的具体设置

路由, VLAN, 交换机, 设置 在3560交换机上划三个VLAN，并且要求其中两个VLAN间能够互相访问，操作如下，请指点：

过程 5.1. Switch VLan 配置步骤

1. 激活vlan路由

```
Switch1#config t
Switch1(config)#ip routing
```

2. 创建三个VLAN

```
Switch1#

Switch1#vlan database

Switch1(vlan)#vlan 2

Switch1(vlan)#vlan 3

Switch1(vlan)#vlan 10

Switch1(vlan)#exit
```

3. 给VLAN分配IP

```
Switch1#config t

Switch1(config)#config vlan2

Switch1(config-if)#ip address 192.168.2.1 255.255.255.0

Switch1(config-if)#no shutdown


Switch1#config t

Switch1(config)#config vlan3

Switch1(config-if)#ip address 192.168.3.1 255.255.255.0

Switch1(config-if)#no shutdown
```

4. 配VTP

```
Switch1#

Switch1#config t

Switch1(config)#vtp domain SMG

Switch1(config)#vtp mode server

Switch1(config)#end
```

5. 交换机通往路由器的接口配IP

```

Switch1#

Switch1#config t

Switch1(config)#interface fastethernet0/1
```

```
Switch1(config-if)#no switchport
Switch1(config-if)#ip address 200.1.1.1 255.255.255.0
Switch1(config-if)#no shutdown
```

6. 交换机配置缺省路由

```
Switch1#
Switch1#config t
Switch(config)#ip route 0.0.0.0 0.0.0.0 200.1.1.2
```

7. 把VLAN号分配给IP接口

```
Switch1#
Switch1#config t
Switch1(config)#interface fastethernet0/2
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan2
Switch1(config-if)#spanning-tree portfast
… …
Switch1#
Switch1#config t
Switch1(config)#interface fastethernet0/13
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan3
Switch1(config-if)#spanning-tree portfast
```

8. 配访问控制列表ACL禁VLAN3子网的客户机访问服务器

```
Switch1#
Switch1#config t
Switch1(config)#access-list 1 deny 192.168.3.0 0.0.0.255
Switch1(config)#access-list 1 permit any
Switch1(config)#interface fastethernet0/13 （此接口接服务器）
Switch1(config-if)#ip access-group 1 out
```

9. 检查上述配置

```
Switch1#show vlan
Switch1#show ip route
Switch1#show interface gigabitethernet0/1 switchport
Switch1#show run
```

```
Switch1#show vtp status
```

10. 存配置

```
Switch1#copy running-config startup-config
```

7.4. VTP

VLAN Trunking Protocol（VLAN 中继协议）

7.4.1. Configuring a VTP Server

Server

```
Switch# config terminal
Switch(config)# vtp mode server
Switch(config)# vtp domain cisco
Switch(config)# vtp password mypassword
Switch(config)# end
```

```
Switch# vlan database
Switch(vlan)# vtp server
Switch(vlan)# vtp domain cisco
Switch(vlan)# vtp password mypassword
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

7.4.2. Configuring a VTP Client

```
2960#conf t
2960(config)#int f0/15
2960(config-if)#switchport mode trunk
2960(config-if)#end
2960#vlan database
2960(vlan)#vtp client
2960(vlan)#vtp domain eng_group
2960(vlan)#vtp password mypassword
2960(vlan)#exit
```

7.4.3. example for vtp

```
cisco3750>en
cisco3750#conf t
cisco3750(config)#vtp domain cisco（创建域名）
cisco3750(config)#vtp password 123（设置密码）
cisco3750(config)#vtp mode server(改成服务器模式)

cisco3750(config-if)#int g0/0（进入千兆端口）
cisco3750(config-if)#switchport trunk encapsulation dot1q(封装)
cisco3750(config-if)#switch mode trunk(改成trunk模式)

3560>en
3560#conf t
3560(config)#vtp domain cisco（要以前面一致）
3560(config)#vtp password 123（要以前面一致）
3560(config)#vtp mode client（改成客户机模式）
```

```
3750G-1.240#show vtp stat
VTP Version                     : 2
Configuration Revision          : 4
```

```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x5D 0x64 0xFF 0xB1 0x87 0xF7 0x5B 0x0E
Configuration last modified by 0.0.0.0 at 3-1-93 00:17:47
Local updater ID is 0.0.0.0 (no valid interface found)


3750G-1.240#show vtp password
VTP Password: 123
```

8. 流量控制

8.1. 粗糙的流量限制

```
Switch(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration

Switch(config-if)#speed 10
```

9. stack-manager

察看当前堆叠状态:
show platform stack-manager all 显示所有交换堆叠的信息
show switch 显示堆叠交换机的汇总信息
show switch 1 显示一号交换机的信息
show switch detail 显示堆叠成员明细的信息
show switch neighbors 显示堆叠邻居的完整信息
show switch stack-ports 显示堆叠交换机的完整端口信息

```
3750#show platform stack-manager all
Switch/Stack Mac Address : aca0.165f.9800
                                           H/W   Current
Switch#  Role    Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Member 0000.0000.0000     0      0       Provisioned
 2       Member 40f4.ec3c.6780     1      0       Ready
*3       Master aca0.165f.9800     1      0       Ready



         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  2        Ok         Ok                3        3
  3        Ok         Ok                2        2


               Stack Discovery Protocol View
================================================================


Switch   Active   Role    Current   Sequence   Dirty
Number                   State     Number     Bit
-------------------------------------------------------------------------
2        TRUE    Member   Ready       055       FALSE
3        TRUE    Master   Ready       055       FALSE



                 Stack State Machine View
================================================================

Switch   Master/   Mac Address          Version    Current
Number   Member                         (maj.min)  State
-----------------------------------------------------------
2        Member    40f4.ec3c.6780          1.34        Ready
3        Master    aca0.165f.9800          1.34        Ready

Last Conflict Parameters

Switch Master/ Cfgd Default Image H/W  # of    Mac Address
Number Member  Prio Config   Type Prio Members
-------------------------------------------------------------------------

            Stack Discovery Protocol Counters
        Messages Sent                  Messages Recvd
        UP       DOWN                  UP         DOWN
-----------------------------------------------------------
 1: 0000000000 0000000000          0000000000 0000000000
 2: 0000004122 0000004114          0000004906 0000004892
*3: 0000006311 0000006321          0000004121 0000004113
 4: 0000000000 0000000000          0000000000 0000000000
 5: 0000000000 0000000000          0000000000 0000000000
 6: 0000000000 0000000000          0000000000 0000000000
 7: 0000000000 0000000000          0000000000 0000000000
 8: 0000000000 0000000000          0000000000 0000000000
 9: 0000000000 0000000000          0000000000 0000000000
```

```
Stack Changes: 11
Internal Stack Link changes: 0
Internal Stack Link state: 0x0
Sync Not OK Resets A: 624  B: 618

             Misc  Counters
   Counter                       Up          Down
-------------------------------------------------

 Wrong Ver Number: Send:    0000000000    0000000000
 Wrong Ver Number: Recv:    0000000000    0000000000
 Missed Messages:           0000000000    0000000000
 Orphaned Messages          0000000000    0000000000
 Supressed Messages         0000000784    0000000778
 No Available Messages      0000006660    0000006660
 Link Present               0000000003    0000000007
 Link Not Present           0000000003    0000000007
 Link RxReset               0000000013    0000000014
 RAC Not OK Resets: 0
 Duplicates:                0000001434    0000001425
 Switch Number of last duplicate:     2
 Sequence Number Failures:     0000000000
 Switch Number of last Failure:     256  Last Difference 0
 Reciprocal Efficiency Changes: Upgrade 0  Downgrade 0
 Switch Number Conflicts: 0

             Resource Counters
-----------------------------------------
 Chunk Alloc's        0000000006
 Chunk Free's         0000000005
 Enqueue Failures:    0000000000
 Null Queue Failures: 0000000000
 Chunk Alloc Errors:  0000000000


           Stack State Machine Counters
   Messages Sent              Messages Recvd
-------------------------------------------------
 1: 0000000000                 0000000000
 2: 0000000006                 0000000006
*3: 0000000000                 0000000000
 4: 0000000000                 0000000000
 5: 0000000000                 0000000000
 6: 0000000000                 0000000000
 7: 0000000000                 0000000000
 8: 0000000000                 0000000000
 9: 0000000000                 0000000000

3750#show switch
Switch/Stack Mac Address : aca0.165f.9800
                                           H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Member 0000.0000.0000     0      0       Provisioned
 2       Member 40f4.ec3c.6780     1      0       Ready
*3       Master aca0.165f.9800     1      0       Ready



3750#show switch 1
Switch/Stack Mac Address : aca0.165f.9800
                                           H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Member 0000.0000.0000     0      0       Provisioned



3750#show switch detail
Switch/Stack Mac Address : aca0.165f.9800
                                           H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Member 0000.0000.0000     0      0       Provisioned
 2       Member 40f4.ec3c.6780     1      0       Ready
*3       Master aca0.165f.9800     1      0       Ready



         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  2        Ok          Ok                3        3
```

```
  3        Ok          Ok                 2        2

3750#show switch neighbors
  Switch #    Port 1       Port 2
  --------    ------       ------
      2         3            3
      3         2            2

3750#show switch stack-ports
  Switch #    Port 1       Port 2
  --------    ------       ------
    2           Ok           Ok
    3           Ok           Ok
```

更改设备在堆叠中的编号

```
switch 5 renumber 4      把5号改为4号
switch 1 priority 2      (1号设备的优先改为2) 默认优先级是1
```

更改优先级命令

```
更改优先级步骤:
switch 1 priority 2 (1号设备的优先改为2)
end
reload slot 1  (调用配置变更)
show switch 1  (察看1号设备的成员信息)
```

强制指定Master设备

在主堆叠交换机上设置顺序

```
cluster member 1 mac-address <第一个堆叠交换机的mac>
cluster member 2 mac-address <第二个堆叠交换机的mac>
```

在各个堆叠交换机上使用下面的命令:

```
cluster command-address <主交换机的mac>
```

10. HSRP(Hot Standby Router Protocol)

Switch A

```
interface Vlan1
 ip address 172.16.1.252 255.255.255.0
 standby 1 ip 172.16.1.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan2
 ip address 172.16.2.252 255.255.255.0
 standby 2 ip 172.16.2.254
 standby 2 priority 150
 standby 2 preempt
```

Switch B

```
interface Vlan1
 ip address 172.16.1.253 255.255.255.0
 standby 1 ip 172.16.1.254
 standby 1 priority 140
 standby 1 preempt
!
interface Vlan2
 ip address 172.16.2.253 255.255.255.0
 standby 2 ip 172.16.2.254
 standby 2 priority 140
 standby 2 preempt
```

11. 4506/4507 专有命令

11.1. 用户认证

创建用户

```
username root password 0 chen
```

创建拥有超级权限的用户

```
username cisco privilege 15 password 0 cisco
```

查看用户

```
#sh user
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
   1 vty 0     cisco      idle                 00:01:01 172.16.2.1

  Interface      User         Mode                    Idle     Peer Address
```

11.2. PoE

关闭以太网供电

```
interface GigabitEthernet1/41
 power inline never
```

11.3. show module

显示4507已经安装的模块信息

```
# sh module
Chassis Type : WS-C4507R+E

Power consumed by backplane : 40 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1    48  10/100/1000BaseT Premium POE E Series  WS-X4648-RJ45V+E   JAE15330G3F
 2    18  10GE (X2), 1000BaseX (SFP)             WS-X4606-X2-E      JAE152801HI
 3     6  Sup 6L-E 10GE (X2), 1000BaseX (SFP)    WS-X45-SUP6L-E     JAE15280145

 M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 44d3.ca6a.8e40 to 44d3.ca6a.8e6f 2.0                                 Ok
 2 0007.7dd3.e793 to 0007.7dd3.e7a4 1.2                                 Ok
 3 0007.7d67.eb40 to 0007.7d67.eb45 3.0 12.2(44r)SG9 12.2(54)SG1        Ok
 5 Seeprom Not Programmed

Mod  Redundancy role     Operating mode      Redundancy status
----+------------------+------------------+----------------------------------
 3   Active Supervisor   SSO                 Active
```

```
4507R-A#show module all
Chassis Type : WS-C4507R+E
```

```
Power consumed by backplane : 40 Watts

Mod Ports Card Type                                Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1    48  10/100/1000BaseT Premium POE E Series  WS-X4648-RJ45V+E   JAE15330HYU
 2    18  10GE (X2), 1000BaseX (SFP)             WS-X4606-X2-E      JAE15260G8R
 3     4  Sup 7-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP7-E      CAT1535L0HG
 5    12  10GE SFP+                              WS-X4712-SFP+E     CAT1523L0BK

 M MAC addresses                     Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 7081.0527.5c00 to 7081.0527.5c2f 2.0                                Ok
 2 0007.7dd3.6350 to 0007.7dd3.6361 1.2                                Ok
 3 44d3.ca21.e2c0 to 44d3.ca21.e2c3 1.0 15.0(1r)SG2  03.01.01.SG      Ok
 5 4055.39da.3054 to 4055.39da.305f 1.1                                Ok

Mod  Redundancy role     Operating mode      Redundancy status
----+------------------+------------------+----------------------------------
 3   Active Supervisor   RPR                 Active
```

第 6 章 Firewall

目录

1. Cisco PIX Firewall

Cisco PIX 515E

过程 6.1. Login Pix515E

1. 登陆

```
1.、telnet 192.168.0.1
   User Access Verification
   Password:（输入密码出现如下信息：）
   Type help or '?' for a list of available commands.
   weibo>
    （此时是PIX 515E的无特权模式，此模式只能查看，并且只能查看防火墙的系统信息）
  /**************chase*********************/
```

2. Then do this.

```
2.、enable（进入特权模式，出现如下信息）
   password:（输入密码进入特权模式）
   weibo#（weibo>变为weibo#）
    （在特权模式下只能查看放火墙的配置不能修改防火墙的配置，用disable退出特权模式返回无特权模式）
  /*************chase*********************/
```

3. And now do this.

```
conf t（进入配置模式，出现如下信息）
```

```
firewall(config)#（weibo#变为weibo(config)#）
    （在配置模式才能修改防火墙的配置，用exit、quit退出配置模式到特权模式）
```

1.1. cisco PIX 515E的全部数据与配置

show tech-support

```
firewall(config)# show tech-support

Cisco PIX Firewall Version 6.3(5)

Compiled on Thu 04-Aug-05 21:40 by morlee

firewall up 36 mins 41 secs

Hardware:   PIX-515E, 128 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0x300, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

0: ethernet0: address is 001c.58b5.6e80, irq 10
1: ethernet1: address is 001c.58b5.6e81, irq 11
Licensed Features:
Failover:                       Disabled
VPN-DES:                        Enabled
VPN-3DES-AES:                   Enabled
Maximum Physical Interfaces: 3
Maximum Interfaces:             5
Cut-through Proxy:              Enabled
Guards:                         Enabled
URL-filtering:                  Enabled
Inside Hosts:                   Unlimited
Throughput:                     Unlimited
IKE peers:                      Unlimited

This PIX has a Restricted (R) license.

Serial Number: 810323551 (0x304c8e5f)
Running Activation Key: 0x1512d3bb 0xdbb4b468 0xb28e1dc9 0x1b826959
Configuration last modified by enable_15 at 23:06:10.370 UTC Thu Sep 2 2010

------------------ show clock ------------------

23:08:58.073 UTC Thu Sep 2 2010

------------------ show memory ------------------

Free memory:        79151528 bytes
Used memory:        55066200 bytes
-------------     ----------------
Total memory:      134217728 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550    933    667    676

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 001c.58b5.6e80
  IP address 172.16.0.30, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        2 packets output, 120 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        2 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
```

```
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 001c.58b5.6e81
  IP address 172.16.1.254, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        3 packets output, 180 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        3 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC        SP        STATE       Runtime    SBASE     Stack Process
Hsi 001f02c9 00953044 0056ed50           0 009520bc 3916/4096 arp_timer
Lsi 001f5a95 009f623c 0056ed50           0 009f52c4 3928/4096 FragDBGC
Lwe 0011a13f 00a0236c 005724b8           0 00a01504 3688/4096 dbgtrace
Lwe 003fb2fd 00a044fc 00567688           0 00a025b4 8008/8192 Logger
Hwe 003ff4b8 00a075f4 00567938           0 00a0567c 8024/8192 tcp_fast
Hwe 003ff431 00a096a4 00567938           0 00a0772c 8024/8192 tcp_slow
Lsi 00314885 028e9924 0056ed50           0 028e899c 3916/4096 xlate clean
Lsi 00314793 028ea9c4 0056ed50           0 028e9a4c 3884/4096 uxlate clean
Mwe 0030be5f 02d7edc4 0056ed50           0 02d7ce2c 7908/8192
tcp_intercept_timer_process
Lsi 00452ee5 02e2b79c 0056ed50           0 02e2a814 3900/4096 route_process
Hsi 002fb6fc 02e2c82c 0056ed50          20 02e2b8c4 3780/4096 PIX Garbage
Collector
Hwe 0021e529 02e36d5c 0056ed50           0 02e32df4 16048/16384 isakmp_time_keeper
Lsi 002f929c 02e5069c 0056ed50           0 02e4f714 3944/4096 perfmon
Mwe 00214d39 02e7aacc 0056ed50           0 02e78b54 7860/8192 IPsec timer handler
Hwe 003b105b 02e8ee14 00591c90           0 02e8cecc 7000/8192 qos_metric_daemon
Mwe 0026d0dd 02ea996c 0056ed50           0 02ea5a04 15592/16384 IP Background
Lwe 0030cad6 02f5c2bc 00585368           0 02f5b444 3704/4096 pix/trace
Lwe 0030cd0e 02f5d36c 00585a98           0 02f5c4f4 3704/4096 pix/tconsole
H*  0011fa67 0009ff2c 0056ed38        1310 02f63784 13136/16384 ci/console
Csi 003048fb 02f6878c 0056ed50           0 02f67834 3432/4096 update_cpu_usage
Hwe 002ef791 03019534 0054e100           0 030156ac 15884/16384 uauth_in
Hwe 003fdf05 0301b634 00892508           0 0301975c 7896/8192 uauth_thread
Hwe 0041553a 0301c784 00567c88           0 0301b80c 3960/4096 udp_timer
Hsi 001e7d4e 0301e444 0056ed50           0 0301d4cc 3800/4096 557mcfix
Crd 001e7d03 0301f504 0056f1c8     1638450 0301e57c 3632/4096 557poll
Lsi 001e7dbd 030205a4 0056ed50           0 0301f62c 3848/4096 557timer
Cwe 001e99a9 0332267c 007f1058           0 03320784 7928/8192 pix/intf0
Mwe 004152aa 0332378c 008dc6f8           0 03322854 3896/4096 riprx/0
Msi 003ba8a1 0332489c 0056ed50           0 03323924 3888/4096 riptx/0
Cwe 001e99a9 03426aa4 00779ae0           0 03424bac 7928/8192 pix/intf1
Mwe 004152aa 03427bb4 008dc6b0           0 03426c7c 3896/4096 riprx/1
Msi 003ba8a1 03428cc4 0056ed50           0 03427d4c 3888/4096 riptx/1
Hwe 003fe199 0344d67c 00868c90           0 0344d034 1196/2048 listen/telnet_1
Mwe 0038707e 0344f85c 0056ed50           0 0344d8e4 7960/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 2214.880 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 2214.880 secs):
                2 packets       120 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 2214.880 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 2214.880 secs):
                3 packets       180 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------
```

```
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s

------------------ show running-config ------------------

: Saved
:
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500
no ip address outside
no ip address inside
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:00000000000000000000000000000000
: end
firewall(config)#
```

1.2. 清除所有配置

```
zoshowpix# conf t
zoshowpix(config)# clear config all
pixfirewall(config)# quit
```

```
pixfirewall# show run
: Saved
:
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500
no ip address outside
no ip address inside
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:00000000000000000000000000000000
: end
pixfirewall#
```

1.3. 配置防火墙的用户信息

```
enable password chen
hostname pix515
domain-name example.com

pixfirewall# conf t
pixfirewall(config)# enable password chen
pixfirewall(config)# hostname firewall
firewall(config)# domain-name example.com
firewall(config)#
```

1.4. 接口设置

激活以太端口

```
interface ethernet0 auto
interface ethernet1 auto
```

```
interface ethernet2 auto
interface ethernet3 auto


firewall(config)# interface ethernet0 auto
firewall(config)# interface ethernet1 auto
```

下面两句配置内外端口的安全级别

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100

firewall(config)# nameif ethernet0 outside security0
firewall(config)# nameif ethernet1 inside security100
```

配置以太端口ip 地址

```
ip address outside 61.144.203.114 255.255.255.244
ip address inside 192.168.0.1 255.255.255.0
ip address dmz 172.16.0.1 255.255.255.0
ip address e3 61.233.203.47 255.255.255.192
```

1.5. 配置NAT配置映射

```
global (outside) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0 0 0
```

1.5.1. 端口映射

WAN IP:PORT --> LAN IP:PORT

```
static (inside,outside) tcp 61.144.203.40 80 192.168.0.116 80 netmask
255.255.255.255 0 0
static (inside,outside) tcp 61.144.203.40 20 192.168.0.116 20 netmask
255.255.255.255 0 0
static (inside,outside) tcp 61.144.203.41 21 192.168.0.116 21 netmask
255.255.255.255 0 0
pix515(config)# static (inside,outside) tcp 61.144.23.50 22 192.168.0.11 22
netmask 255.255.255.255 0 0
```

1.5.2. IP 映射

WAN IP --> LAN IP

```
static (inside,outside) 120.13.14.28 172.16.1.28 netmask 255.255.255.255 0 0
```

1.6. 配置路由

配置outside使用的网关

```
route outside 0.0.0.0 0.0.0.0 120.13.14.1 1
route e3 0.0.0.0 0.0.0.0 61.233.203.1 2
```

1.7. 策略

conduit permit tcp host 公网IP eq ssh 信任IP 255.255.255.255 (这种写法，是信任某个IP)

1.7.1. Ping

下面这句允许ping

```
```

```
pix515(config)#conduit permit icmp any any
```

1.7.2. SSH

```
pix515(config)# conduit permit tcp host 61.144.23.50 eq ssh any
```

1.8. ACL

```
1、配置内网到VPN不做NAT
   access-list 107 permit ip 192.168.0.0 255.255.255.0 172.16.1.0 255.255.255.0
   (建立内网-->VPN的访问列表)
   nat (inside) 0 access-list 107 （内网-->VPN不做NAT，引用上一步access-list 107）

2、配置内网到DMZ 做NAT
   access-list 102 permit tcp 192.168.0.0 255.255.255.0 host 172.16.0.103 eq 1433
   access-list 102 permit tcp 192.168.0.0 255.255.255.0 host 172.16.0.103 eq 3125
   nat (inside) 2 access-list 102（内网-->DMZ做NAT，引用上一步access-list 102）

3、配置内网到Internet 做NAT
   access-list 101 permit ip 192.168.0.0 255.255.255.0 any
   nat (inside) 1 access-list 101 0 0

4、配置DMZ到VPN不做NAT
   access-list 107 permit ip 172.16.0.0 255.255.255.0 172.16.1.0 255.255.255.0
   (建立内网-->VPN的访问列表)
   nat (DMZ) 0 access-list 107

4、配置VPN到DMZ不做NAT
   access-list 150 permit ip 172.16.1.0 255.255.255.0 172.16.0.0 255.255.255.0
   (建立内网-->VPN的访问列表)
   nat (e3) 0 access-list 150
```

1.9. 配置远程telnet访问

```
password chen （把telnet的密码修改为chen）
telnet 192.168.0.1 255.255.255.255 inside（开启内网口的telnet服务）
telnet 192.168.0.0 255.255.255.0 inside（允许所有内网用户访问telnet服务）
telnet 0.0.0.0 0.0.0.0 e3
telnet 61.144.203.41 255.255.255.255 e3
```

1.10. 配置DHCP

```
pix515(config)#ip address dhcp
pix515(config)#dhcpd enable inside
pix515(config)#dhcpd auto_config outside（自动配置外网DHCP服务参数）
pix515(config)#dhcpd address 172.16.0.20-172.16.0.200 inside （内网DHCP分配的IP地址范围）
pix515(config)#dhcpd dns 208.67.222.222 208.67.220.220
pix515(config)#dhcpd domain example.com
```

1.11. VPN

PPTP

```
1、命令行方式直接在PIX上配置PPTP的VPN，即PIX作为PPTP方式VPDN的服务器
    ip local pool pptp 10.0.0.1-10.0.0.50
    //定义一个pptp 方式的vpdn拨入后获得的IP地址池，名字叫做pptp。此处地址段的定义范围不要和拨入后内网其他计算机的IP冲突，并且要根据拨入用户的数量来定义地址池的大小
    vpdn group PPTP-VPDN-GROUP accept dialin pptp
    vpdn group PPTP-VPDN-GROUP ppp authentication pap
    vpdn group PPTP-VPDN-GROUP ppp authentication chap
    vpdn group PPTP-VPDN-GROUP ppp authentication mschap
    vpdn group PPTP-VPDN-GROUP ppp encryption mppe auto
    //以上为配置pptp的vpdn组的相关属性
    vpdn group PPTP-VPDN-GROUP client configuration address local pptp
    //上面定义pptp的vpnd组使用本地地址池组pptp，为一开始定义的
    vpdn group PPTP-VPDN-GROUP pptp echo 60
    vpdn group PPTP-VPDN-GROUP client authentication local
    //此处配置pptp的vpdn拨入用户口令认证为本地认证，当然也可以选择AAA服务器认证，本地认证属于比
```

```
较方便的一种实现
    vpdn username test1 password *********
    vpdn username test2 password *********
    //上面为定义本地用户认证的用户帐号和密码，可以定义多个
    vpdn enable outside
    //在pix防火墙的outside口起用vpdn功能，也可以在其他接口上应用
  2、使用pix防火墙内部的某个pptp的VPDN服务器作为专门的VPN服务器，只是在pix上开放相应的服务端口
  pptp使用1723端口，而通常pix里面的服务器对外都是做的静态NAT转换，但是光双向开放1723端口仍旧无法建立pptp的vpn连接，那么对于pix 6.3以上版本的pptp穿透可以用一条命令fixup protocol pptp 1723 来解决这个问题。
```

Ipsec VPN 配置

```
ip local pool pigpool 172.16.1.50-172.16.1.240   (建立VPN的地址空间)
sysopt connection permit-ipsec (开启系统ipsec端口)
sysopt connection permit-pptp (开启系统pptp端口)
sysopt connection permit-l2tp (开启系统l2tp端口)

isakmp enable e3  (e3接口启用isakmp)
isakmp policy 8 encryption des (定义phase 1协商用DES加密算法)
isakmp policy 8 hash md5 (定义phase 1协商用MD5散列算法)
isakmp policy 8 authentication pre-share (定义phase 1使用pre-shared key进行认证)
isakmp key pix address 0.0.0.0 netmask 0.0.0.0 (定义使用共享密匙pix)
isakmp client configuration address-pool local pigpool e3 (将VPN client地址池绑定到isakmp)
isakmp policy 8 group 2 (isakmp policy 10 group 2)
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac (定义一个变换集strong-des)
crypto dynamic-map cisco 4 set transform-set strong-des (把strong-des添加到动态加密策略cisco)
crypto map partner-map 20 ipsec-isakmp dynamic cisco (把动态加密策略绑定到partner-map加密图)
crypto map partner-map client configuration address initiate (定义给每个客户端分配IP地址)
crypto map partner-map client configuration address respond (定义PIX防火墙接受来自任何IP的请求)
crypto map partner-map interface e3 (把动态加密图vpnpeer绑定到e3口)
vpdn group 2 accept dialin l2tp
vpdn group 2 ppp authentication pap
vpdn group 2 client configuration address local pigpool
vpdn group 2 client authentication local
vpdn group 2 l2tp tunnel hello 80
vpdn username pix password pix (设置vpn密码，密码必须与共享密匙一样)
vpdn enable e3
```

vpn本地身份验证

```
crypto map vpnpeer client authentication LOCAL
username whr password whr
no username whr
```

修改VPN拨入密码

```
no isakmp key ******** address 0.0.0.0 netmask 0.0.0.0 (删除共享密匙)
isakmp key whr address 0.0.0.0 netmask 0.0.0.0      (设置共享密匙)
vpdn username chase  (删除chase用户)
vpdn username chase password whr   (设置用户名为chase；密码为whr；密码要与共享密匙相同)
```

1.12. 防止DDOS攻击

网上找到的，我不确认是否可以起到效果：）

```
步骤1：开启日志功能，并确定系统日志级别
logging on
logging trap 7 (7为最高级别了)
步骤2：确定一台日志服务器(192.168.1.10)，并把系统日志输出导系统日志服务器上
logging host inside 192.168.1.10
步骤3：配置入侵检测（IDS）为攻击类特征码和信息类特征码创建策略
ip audit name attackpolicy attack action alarm reset
ip audit name infopolicy info action alarm reset
步骤4：在接口上启用策略
ip audit interface outside attackpolicy
ip audit interface outside infopolicy
```

```
步骤5：在日志服务器上安装日志软件（如果是LINUX可免了）
Kiwi_Syslogd2.exe
步骤6：大功告成了。
```

1.13. SNMP

```
firewall(config)# sh snmp
snmp-server host inside 172.16.0.5              "安装了MRTG和Cacti服务器地址
snmp-server location 172.16.0.1                 "位置描述，可以写内网端口地址，或者更直
观的描述如：gateway firewall
snmp-server contact netkiller@example.com
snmp-server community cisco                     "public
snmp-server enable traps                                "允许管理信息发送
```

PIX 515 仅支持snmp v1

```
neo@monitor:~$ snmpwalk -v1 -c public 172.16.1.254
interfaces.ifTable.ifEntry.ifDescr
IF-MIB::ifDescr.1 = STRING: PIX Firewall 'outside' interface
IF-MIB::ifDescr.2 = STRING: PIX Firewall 'inside' interface


neo@monitor:~$ snmpwalk -v1 -c public 172.16.1.254
SNMPv2-MIB::sysDescr.0 = STRING: Cisco PIX Firewall Version 6.3(5)

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.451
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1899600400) 219 days,
20:40:04.00
SNMPv2-MIB::sysContact.0 = STRING: neo.chen@xiu.com
SNMPv2-MIB::sysName.0 = STRING: firewall.xiu.com
SNMPv2-MIB::sysLocation.0 = STRING: gw
SNMPv2-MIB::sysServices.0 = INTEGER: 4
IF-MIB::ifNumber.0 = INTEGER: 2
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifDescr.1 = STRING: PIX Firewall 'outside' interface
IF-MIB::ifDescr.2 = STRING: PIX Firewall 'inside' interface
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 1500
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 100000000
IF-MIB::ifSpeed.2 = Gauge32: 100000000
IF-MIB::ifPhysAddress.1 = STRING: 0:1c:58:b5:6e:80
IF-MIB::ifPhysAddress.2 = STRING: 0:1c:58:b5:6e:81
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: up(1)
IF-MIB::ifLastChange.1 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.2 = Timeticks: (0) 0:00:00.00
IF-MIB::ifInOctets.1 = Counter32: 4008321683
IF-MIB::ifInOctets.2 = Counter32: 4051905092
IF-MIB::ifInUcastPkts.1 = Counter32: 2797544526
IF-MIB::ifInUcastPkts.2 = Counter32: 2017238766
IF-MIB::ifInNUcastPkts.1 = Counter32: 38465473
IF-MIB::ifInNUcastPkts.2 = Counter32: 27783306
IF-MIB::ifInDiscards.1 = Counter32: 0
IF-MIB::ifInDiscards.2 = Counter32: 0
IF-MIB::ifInErrors.1 = Counter32: 16601
IF-MIB::ifInErrors.2 = Counter32: 32841
IF-MIB::ifInUnknownProtos.1 = Counter32: 0
IF-MIB::ifInUnknownProtos.2 = Counter32: 0
IF-MIB::ifOutOctets.1 = Counter32: 2947292253
IF-MIB::ifOutOctets.2 = Counter32: 3544827218
IF-MIB::ifOutUcastPkts.1 = Counter32: 1968227296
IF-MIB::ifOutUcastPkts.2 = Counter32: 2414528344
IF-MIB::ifOutNUcastPkts.1 = Counter32: 0
IF-MIB::ifOutNUcastPkts.2 = Counter32: 0
IF-MIB::ifOutDiscards.1 = Counter32: 0
IF-MIB::ifOutDiscards.2 = Counter32: 0
IF-MIB::ifOutErrors.1 = Counter32: 0
IF-MIB::ifOutErrors.2 = Counter32: 0
IF-MIB::ifOutQLen.1 = Gauge32: 0
IF-MIB::ifOutQLen.2 = Gauge32: 0
IF-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.2 = OID: SNMPv2-SMI::zeroDotZero
IP-MIB::ipAdEntAddr.120.13.14.30 = IpAddress: 120.13.14.30
```

```
IP-MIB::ipAdEntAddr.172.16.1.254 = IpAddress: 172.16.1.254
IP-MIB::ipAdEntIfIndex.120.13.14.30 = INTEGER: 1
IP-MIB::ipAdEntIfIndex.172.16.1.254 = INTEGER: 2
IP-MIB::ipAdEntNetMask.120.13.14.30 = IpAddress: 255.255.255.192
IP-MIB::ipAdEntNetMask.172.16.1.254 = IpAddress: 255.255.255.0
IP-MIB::ipAdEntBcastAddr.120.13.14.30 = INTEGER: 0
IP-MIB::ipAdEntBcastAddr.172.16.1.254 = INTEGER: 0
IP-MIB::ipAdEntReasmMaxSize.120.13.14.30 = INTEGER: 65535
IP-MIB::ipAdEntReasmMaxSize.172.16.1.254 = INTEGER: 65535
```

如果你使用snmp v2版本尝试连接pix防火墙将会提示

```
neo@monitor:~$ snmpwalk -v2c -c public 172.16.1.254
Timeout: No Response from 172.16.1.254
```

1.14. 开启WEB管理

```
http server enable
http 172.16.0.1 255.255.255.255 inside
```

172.16.0.1 是from ip,或者允许一个IP段

```
http 172.16.0.0 255.255.255.0 inside
```

http 登录密码

```
username admin password ysCf4HUXoqIPDu1 privilege 15
```

https://172.16.0.254

1.15. 保存

write memory

```
pix515(config)# write mem
Building configuration...
Cryptochecksum: 5641ca9c 2ef4c53c 0dc8a8f9 75d47f09
[OK]
pix515(config)#
```

1.15.1. 备份及恢复

备份

```
pix515(config)# write net 192.168.2.111:pix515.rtf
Building configuration...
TFTP write 'pix515.rtf' at 192.168.2.111 on interface 1
[OK]
```

恢复

```
pix515(config)# clear config all  是清除所有配置
如何想要通过tftp恢复，得要先配置一下inside接口地址:
pixfirewall(config)# ip add inside 192.168.2.1 255.255.255.0
pixfirewall(config)# ping 192.168.2.111  测试一下到TFTP服务器是否通
        192.168.2.111 response received -- 0ms
        192.168.2.111 response received -- 0ms
        192.168.2.111 response received -- 0ms
pix515(config)# configure net 192.168.2.111:pix515.rtf
Global 10.6.6.151 will be Port Address Translated
Global 10.6.6.150 will be Port Address Translated
Global 10.6.6.211 will be Port Address Translated
.
Cryptochecksum(unchanged): ead0c833 1ed19938 b863ace2 4902f21b
```

```
Config OK
```

1.16. clear

```
clear xlate
clear arp
clear local-host
```

1.16.1. NAT映射更改后仍然指向之前的IP

```
clear xlate
```

1.16.2. reload

```
fix515(config)# reload
```

---

2. Cisco ASA Firewall

2.1. Console 登录

```
ciscoasa> en
Password:
ciscoasa# show run
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
interface GigabitEthernet1/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/3
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
ftp mode passive
pager lines 24
logging asdm informational
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2ca307ae725244ecf965030aa8ee6a2b
: end
ciscoasa#
```

2.2. Management0/0

使用静态IP地址

```
ciscoasa(config-if)# no dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# no dhcpd enable management
ciscoasa(config)# interface Management0/0
ciscoasa(config-if)# ip address 192.168.3.254 255.255.255.0
Waiting for the earlier webvpn instance to terminate...
Previous instance shut down. Starting a new one.
```

使用DHCP分配IP地址

```
```

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
Waiting for the earlier webvpn instance to terminate...
Previous instance shut down. Starting a new one.
ciscoasa(config-if)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
ciscoasa(config)#
```

2.3. 接口配置

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# ip address 172.16.0.2 255.255.255.0
ciscoasa(config-if)# no shutdown


ciscoasa(config-if)# interface GigabitEthernet1/0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip address 192.168.3.254 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# show ip
System IP Addresses:
Interface                Name                   IP address      Subnet mask
Method
GigabitEthernet0/0       outside                172.16.0.2      255.255.255.0
manual
Management0/0            management             192.168.1.1     255.255.255.0
manual
GigabitEthernet1/0       inside                 192.168.3.254   255.255.255.0
manual
Current IP Addresses:
Interface                Name                   IP address      Subnet mask
Method
GigabitEthernet0/0       outside                172.16.0.2      255.255.255.0
manual
Management0/0            management             192.168.1.1     255.255.255.0
manual
GigabitEthernet1/0       inside                 192.168.3.254   255.255.255.0
manual
```

2.3.1. 子接口

```
interface GigabitEthernet1/0.1
 no vlan
 no nameif
 no security-level
 ip address 172.16.7.254 255.255.255.0
```

2.4. route

```
ciscoasa(config)# route outside 0 0 172.16.0.1
show route
```

2.5. ACL

2.5.1. Blacklist

黑名单规则

```
access-list outside extended permit icmp any any
access-list outside deny ip any any
access-list outside extended permit tcp any any eq www
access-list outside extended permit tcp any any eq https
access-list outside extended permit tcp any host 28.6.7.23 eq ftp
access-list outside permit tcp any host 202.96.134.133 eq www
access-list outside permit ip any host 133.11.20.21 eq ftp
access-group outside in interface outside
```

2.5.2. Whitelist

白名单规则

```
access-list outside extended permit ip any any
access-list outside extended permit icmp any any
access-list outside extended permit tcp any any
access-list outside extended permit udp any any
access-list outside deny ip any host 192.168.0.1
access-list outside deny ip any host 192.168.0.2 eq www
access-group outside in interface outside
```

2.5.3. Example

```
access-list outside extended permit icmp any any
access-list outside extended permit tcp any any eq www
access-list outside extended permit tcp any any eq ssh
access-list outside extended permit udp any host 120.112.13.20 eq domain
access-list outside extended permit udp any host 120.112.13.23 eq domain
access-list outside extended permit tcp any host 120.112.13.18 eq ssh
access-list outside extended permit tcp any host 120.112.13.7 eq ftp
access-list outside extended permit tcp any host 120.112.13.21 eq www
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.27 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.28 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.11 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.12 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.8 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.9 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.15 eq
ssh
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.29 eq
ftp
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.10 eq
ftp
access-list outside extended permit tcp host 113.106.63.1 host 120.112.13.10 eq
ssh
access-list outside deny ip 192.168.0.0 0.255.255.255 any
access-list outside deny ip 127.0.0.0 0.255.255.255 any
access-list outside extended permit tcp any host 120.112.13.33
access-list outside permit ip any any

access-list inside extended permit icmp any any
access-list inside extended permit ip any any
```

```
ciscoasa(config)# access-list outside permit icmp any any
ciscoasa(config)# access-group outside in interface outside
ciscoasa(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp any any (hitcnt=0) 0x390a154c
```

extended关键字可能省略 access-list outside permit ip any any，另外我比较喜欢用nameif做acl名称，这样比较直观如： outside，你也可以使用传统100，101什么的

2.6. 配置NAT映射

把inside区域的所有地址进行映射，映射为outside端口的那个公网IP地址。

```
globle (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
```

指定其他IP

```
asa(config)#nat(inside) 1 192.168.1.1 255.255.255.0
```

```
asa(config)#global(outside) 1 222.240.254.193 255.255.255.248
```

定义的地址池

```
asa(config)#nat (inside) 0 192.168.1.1 255.255.255.255      //表示192.168.1.1这个地址
不需要转换。直接转发出去。
asa(config)#global (outside) 1 133.1.0.1-133.1.0.14       //定义的地址池
asa(config)#nat (inside) 1 0 0                              //0 0表示转换网段中的所有地
址。定义内部网络地址将要翻译成的全局地址或地址范围
```

我的配置

```
global (outside) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0 0 0
```

2.6.1. IP 映射

```
static (inside,outside) 222.24.24.2 192.168.1.2
static (inside,outside) 222.24.24.2 192.168.1.2 4096 32
```

后面的4096为限制连接数，32为限制的半开连接数。

```
asa(config)#static (dmz,outside) 13.1.0.2 10.65.1.102         ;静态NAT
asa(config)#static (inside,dmz) 10.66.1.20 10.66.1.20         ;静态NAT
```

2.6.2. 端口映射

```
static (inside,outside) tcp 61.144.203.40 80 192.168.0.116 80 netmask
255.255.255.255 0 0
static (inside,outside) tcp 61.144.203.40 20 192.168.0.116 20 netmask
255.255.255.255 0 0
static (inside,outside) 221.221.147.195 192.168.0.10 netmask 255.255.255.255 tcp
8089 0
```

2.7. timeout

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
```

2.8. DHCP

2.8.1. management

```
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

2.8.2. inside

```
dhcpd address 192.168.1.100-192.168.1.199 inside
设置DHCP服务器地址池
dhcpd dns 208.67.222.222 208.67.220.220 interface inside                        设
置DNS服务器到内网端口
dhcpd enable inside
设置DHCP应用到内网端口
```

2.9. SNMP

```
snmp-server host inside 172.16.1.2
snmp-server location GuangDong
snmp-server contact neo.chen@xiu.com
snmp-server community public
```

2.10. 用户登录

创建用户

```
username cisco password cisco
#明文密码
username cisco password 3USUcOPFUiMCO4Jk encrypted
#加密密码
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15 #不需要enable密码
```

匹配地址 172.16.0.1 255.255.255.255

匹配网段 172.16.0.0 255.255.255.0

所有地址 0.0.0.0 0.0.0.0

2.10.1. Telnet

```
username cisco password cisco
aaa authentication telnet console LOCAL
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
```

2.10.2. SSH

```
1) username xxxx password xxxx
2) passwd xxxxx
3) ssh x.x.x.x x.x.x.x {inside/outside}
4) crypto key generate rsa modulus {512/768/1024/2048}
5) aaa authentication ssh console LOCAL
```

```
username cisco password cisco
passwd cisco
ssh 172.16.0.1 255.255.255.255 outside
crypto key generate rsa modulus 2048
aaa authentication ssh console LOCAL
```

2.11. VPN

2.11.1. site to site

2.11.2. webvpn

2.12. service-policy

```
ciscoasa(config)# access-list TEST200K permit ip host x.x.x.x any
ciscoasa(config)# class-map internet
ciscoasa(config-cmap)# match access-list TEST200K

ciscoasa(config)# policy-map out-police
ciscoasa(config-pmap)# class internet

ciscoasa(config-pmap-c)# police output 200000 1000 conform-action transmit exceed-
action drop

ciscoasa(config)# service-policy out-police interface outside
```

使用NAT映射后应该配置到inside接口上

```
access-list 200k extended permit ip any host x.x.x.x
access-list 500k extended permit ip any host x.x.x.x

class-map 200k
    match access-list 200k
policy-map limit200k
    class 200k
        police input 2096000 1048
        police output 2096000 1048
service-policy limit200k interface inside

class-map 500k
    match access-list 500k
policy-map limit500k
    class 500k
        police input 2096000 1048
        police output 2096000 1048
service-policy limit500k interface inside
```

2.13. failover

```
interface GigabitEthernet1/1
!
interface GigabitEthernet1/1.1
 description STATE Failover Interface
 vlan 2
!
interface GigabitEthernet1/1.2
 description LAN Failover Interface
 vlan 3
!

failover
failover lan unit primary
failover lan interface failover GigabitEthernet1/1.2
failover link state GigabitEthernet1/1.1
failover interface ip failover 172.16.10.1 255.255.255.248 standby 172.16.10.2
failover interface ip state 172.16.10.9 255.255.255.248 standby 172.16.10.10
```

```
ciscoasa# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         Ifc Failure              14:49:44 UTC Oct 26 2011
                              outside: No Link
Other host -   Secondary
               Standby Ready  Comm Failure             16:27:18 UTC Oct 26 2011

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

2.14. 备份配置文件

我建议你放弃tftp,目前主流设备都支持很多协议。我比较喜欢使用ftp

```
ciscoasa# copy running-config ftp://test:your_pasword@172.16.0.2

Source filename [running-config]?

Address or name of remote host [172.16.1.2]?

Destination username [test]?

Destination password [******]?

Destination filename [running-config]?
Cryptochecksum: e5bb0305 02196b08 59efc7e5 9b4e1132
!!!!!!
19447 bytes copied in 3.900 secs (6482 bytes/sec)
```

---

3. 查看命令

```
show ver（查看系统信息）
show run（查看防火墙运行配置）
show ip address（查看防火墙IP地址）
show nameif
show conduit
show config
show run
show static
show global
show dhcpd
show nat

Since it shows connection by host
show local-host
show conn
show xlate detail

# show cpu usage
CPU utilization for 5 seconds = 6%; 1 minute: 6%; 5 minutes: 7%

# sh traffic
outside:
        received (in 1806806.980 secs):
                3051312134 packets      3372506524 bytes
                1001 pkts/sec   1001 bytes/sec
        transmitted (in 1806806.980 secs):
                3680162240 packets      3426881395 bytes
                2001 pkts/sec   1000 bytes/sec
inside:
        received (in 1806806.980 secs):
                3633230948 packets      1921928934 bytes
                2001 pkts/sec   1001 bytes/sec
        transmitted (in 1806806.980 secs):
                2935232007 packets      2574723752 bytes
                1001 pkts/sec   1001 bytes/sec
```

3.1. show interface

```
firewall(config)# show interface
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 001c.58b5.6e80
  IP address 120.13.14.30, subnet mask 255.255.255.192
  MTU 1500 bytes, BW 100000 Kbit full duplex
        2813730585 packets input, 322384351 bytes, 0 no buffer
        Received 38464886 broadcasts, 0 runts, 0 giants
        16601 input errors, 0 CRC, 0 frame, 16601 overrun, 0 ignored, 0 abort
        1938316742 packets output, 958234027 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (3/144)
        output queue (curr/max blocks): hardware (0/128) software (0/278)
interface ethernet1 "inside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 001c.58b5.6e81
  IP address 172.16.0.254, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 100000 Kbit full duplex
        2015029888 packets input, 2028029332 bytes, 0 no buffer
        Received 27779782 broadcasts, 0 runts, 0 giants
        32841 input errors, 0 CRC, 0 frame, 32841 overrun, 0 ignored, 0 abort
        2392423441 packets output, 4158892725 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/154)
        output queue (curr/max blocks): hardware (2/128) software (0/353)
```

```
```

3.2. show static

```
firewall(config)# show static
static (inside,outside) 120.12.14.6 172.16.0.6 netmask 255.255.255.255 0 0
static (inside,outside) 120.12.14.7 172.16.0.7 netmask 255.255.255.255 0 0
static (inside,outside) 120.12.14.8 172.16.0.8 netmask 255.255.255.255 0 0
static (inside,outside) 120.12.14.10 172.16.0.10 netmask 255.255.255.255 0 0
```

3.3. show ip

```
firewall(config)# show ip
System IP Addresses:
        ip address outside 120.12.14.3 255.255.255.192
        ip address inside 172.16.0.254 255.255.255.0
Current IP Addresses:
        ip address outside 120.12.14.3 255.255.255.192
        ip address inside 172.16.0.254 255.255.255.0
```

3.4. show cpu usage

```
firewall(config)# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 20%; 5 minutes: 20%
```

3.5. show conn count

```
firewall(config)# show conn count
5661 in use, 117879 most used
```

3.6. show blocks

```
firewall(config)# show blocks
  SIZE    MAX    LOW    CNT
     4   1600   1424   1600
    80    400    394    398
   256    500    442    500
  1550    933      0    618
```

3.7. show mem

```
firewall(config)# show mem
Free memory:        75529176 bytes
Used memory:        58688552 bytes
------------     ----------------
Total memory:      134217728 bytes
```

3.8. show traffic

```
firewall(config)# show traffic
outside:
        received (in 1812494.446 secs):
                2813262888 packets      253141259 bytes
                1000 pkts/sec   2 bytes/sec
        transmitted (in 1812494.446 secs):
                1937679278 packets      288527512 bytes
                1000 pkts/sec   0 bytes/sec
inside:
        received (in 1812494.446 secs):
                2014390684 packets      1357597340 bytes
                1000 pkts/sec   0 bytes/sec
        transmitted (in 1812494.446 secs):
                2391958734 packets      4089671095 bytes
                1002 pkts/sec   2000 bytes/sec
```

3.9. show xlate

```
firewall(config)# show xlate
64 in use, 1051 most used
Global 120.13.14.10 Local 172.16.0.10
Global 120.13.14.18 Local 172.16.0.48
Global 120.13.14.28 Local 172.16.0.28
Global 120.13.14.35 Local 172.16.0.35
Global 120.13.14.24 Local 172.16.0.41
Global 120.13.14.13 Local 172.16.0.33
Global 120.13.14.7 Local 172.16.0.7
Global 120.13.14.6 Local 172.16.0.6
PAT Global 120.13.14.30(23951) Local 172.16.0.42(61748)
Global 120.13.14.21 Local 172.16.0.24
Global 120.13.14.23 Local 172.16.0.23
Global 120.13.14.25 Local 172.16.0.54
Global 120.13.14.14 Local 172.16.0.34
Global 120.13.14.27 Local 172.16.0.27
Global 120.13.14.22 Local 172.16.0.22
Global 120.13.14.5 Local 172.16.0.13
Global 120.13.14.15 Local 172.16.0.15
Global 120.13.14.4 Local 172.16.0.4
Global 120.13.14.26 Local 172.16.0.26
PAT Global 120.13.14.30(31707) Local 172.16.0.101(63573)
PAT Global 120.13.14.30(31705) Local 172.16.0.51(46332)
PAT Global 120.13.14.30(31709) Local 172.16.0.101(63587)
PAT Global 120.13.14.30(31708) Local 172.16.0.101(51612)
Global 120.13.14.16 Local 172.16.0.56
Global 120.13.14.20 Local 172.16.0.20
Global 120.13.14.12 Local 172.16.0.12
Global 120.13.14.8 Local 172.16.0.8
Global 120.13.14.38 Local 172.16.0.38
Global 120.13.14.29 Local 172.16.0.2
PAT Global 120.13.14.30(61715) Local 172.16.0.47(35662)
PAT Global 120.13.14.30(61714) Local 172.16.0.37(5809)
PAT Global 120.13.14.30(61713) Local 172.16.0.141(55314)
PAT Global 120.13.14.30(61712) Local 172.16.0.141(55313)
PAT Global 120.13.14.30(61699) Local 172.16.0.47(46235)
PAT Global 120.13.14.30(61698) Local 172.16.0.47(52197)
PAT Global 120.13.14.30(61696) Local 172.16.0.37(43727)
PAT Global 120.13.14.30(61703) Local 172.16.0.47(49113)
PAT Global 120.13.14.30(61702) Local 172.16.0.141(55309)
PAT Global 120.13.14.30(61700) Local 172.16.0.47(44744)
PAT Global 120.13.14.30(61707) Local 172.16.0.47(56175)
PAT Global 120.13.14.30(61706) Local 172.16.0.47(50588)
PAT Global 120.13.14.30(61705) Local 172.16.0.47(58676)
PAT Global 120.13.14.30(61704) Local 172.16.0.141(55310)
PAT Global 120.13.14.30(61711) Local 172.16.0.47(39698)
PAT Global 120.13.14.30(61710) Local 172.16.0.141(55312)
PAT Global 120.13.14.30(61709) Local 172.16.0.141(55311)
PAT Global 120.13.14.30(61708) Local 172.16.0.47(54897)
PAT Global 120.13.14.30(391) Local 172.16.0.49(123)
PAT Global 120.13.14.30(389) Local 172.16.0.161(137)
PAT Global 120.13.14.30(393) Local 172.16.0.37(123)
PAT Global 120.13.14.30(392) Local 172.16.0.5(123)
Global 120.13.14.19 Local 172.16.0.19
Global 120.13.14.9 Local 172.16.0.9
Global 120.13.14.11 Local 172.16.0.11
PAT Global 120.13.14.30(61682) Local 172.16.0.37(44507)
PAT Global 120.13.14.30(61681) Local 172.16.0.37(1561)
PAT Global 120.13.14.30(61684) Local 172.16.0.141(55307)
PAT Global 120.13.14.30(61694) Local 172.16.0.141(55308)
PAT Global 120.13.14.30(61693) Local 172.16.0.47(49428)
PAT Global 120.13.14.30(61692) Local 172.16.0.37(46051)
PAT Global 120.13.14.30(61667) Local 172.16.0.141(55306)
PAT Global 120.13.14.30(61666) Local 172.16.0.47(39924)
PAT Global 120.13.14.30(61670) Local 172.16.0.37(62964)
```

4. FAQ

4.1. inside 不能到达 outside

inside 下面PC可以ping 通网关，但不能ping通WAN上的服务器

```
nat (inside) 1 172.16.3.0 255.255.255.0
```

5. Example

5.1. ASA Firewall

例 6.1. ASA 5550

```
: Saved
:
ASA Version 8.2(1)
!
hostname asa5550
enable password Yi7fhXUH4X/ZMh encrypted
passwd 2KFQnNId2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 110.112.133.60 255.255.255.192
!
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
interface GigabitEthernet1/0
 nameif inside
 security-level 100
 ip address 172.16.0.254 255.255.255.0
!
interface GigabitEthernet1/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/3
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
```

```
access-list outside extended permit icmp any any
access-list outside extended permit udp any host 110.112.133.20 eq domain
access-list outside extended permit udp any host 110.112.133.23 eq domain
access-list outside extended permit udp any host 110.112.133.18 eq domain
access-list outside extended permit tcp any host 110.112.133.18 eq ssh
access-list outside extended permit tcp any host 110.112.133.7 eq ftp
access-list outside extended permit tcp any host 110.112.133.21 eq www
access-list outside extended permit tcp any host 110.112.133.22 eq www
access-list outside extended permit tcp any host 110.112.133.13 eq 3389
access-list outside extended permit tcp any host 110.112.133.24 eq 3389
access-list outside extended permit tcp any host 110.112.133.9 eq www
access-list outside extended permit tcp any host 110.112.133.29 eq ssh
access-list outside extended permit tcp any host 110.112.133.29 eq www
access-list outside extended permit udp any host 110.112.133.29 eq 1194
access-list outside extended permit tcp any host 110.112.133.6 eq www
access-list outside extended permit tcp any host 110.112.133.7 eq www
access-list outside extended permit tcp any host 110.112.133.8 eq www
access-list outside extended permit tcp any host 110.112.133.10 eq www
access-list outside extended permit tcp any host 110.112.133.11 eq www
access-list outside extended permit tcp any host 110.112.133.12 eq www
access-list outside extended permit tcp any host 110.112.133.27 eq www
access-list outside extended permit tcp any host 110.112.133.28 eq www
access-list outside extended permit tcp any host 110.112.133.25 eq www
access-list outside extended permit tcp any host 110.112.133.25 eq 3389
access-list outside extended permit tcp any host 110.112.133.18 eq 3306
access-list outside extended permit tcp any host 110.112.133.13 eq ftp
access-list outside extended permit tcp any host 110.112.133.13 eq 8000
access-list outside extended permit tcp any host 110.112.133.26 eq ssh
access-list outside extended permit tcp any host 110.112.133.5 eq www
access-list outside extended permit tcp any host 110.112.133.26 eq ftp
access-list outside extended permit tcp any host 110.112.133.14 eq 8080
access-list outside extended permit tcp any host 110.112.133.19 eq www
access-list outside extended permit tcp any host 110.112.133.17 eq www
access-list outside extended permit tcp any host 110.112.133.16 eq www
access-list outside extended permit tcp any host 110.112.133.4 eq www
access-list outside extended permit tcp any host 110.112.133.4 eq ftp
access-list outside extended permit tcp any host 110.112.133.4 eq ssh
access-list outside extended deny udp any host 110.112.133.7
access-list outside extended permit tcp any host 110.112.133.62 eq www
access-list outside extended permit tcp any host 110.112.133.62 eq ssh
access-list outside extended permit tcp any host 110.112.133.24 eq 5900
access-list outside extended permit tcp any host 110.112.133.35 eq www
access-list outside extended permit tcp any host 110.112.133.35 eq 3389
access-list outside extended permit tcp any host 110.112.133.38 eq www
access-list outside extended deny udp any host 110.112.133.38
access-list outside extended permit tcp any host 110.112.133.44 eq www
access-list outside extended permit tcp any host 110.112.133.44 eq 5900
access-list outside extended permit tcp any host 110.112.133.8 eq https
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.27 eq
ssh
access-list outside extended permit tcp any any eq www
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.28 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.11 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.12 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.8 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.9 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.15 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.29 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.10 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.10 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.9 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.8 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.11 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.12 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.5 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.25 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.16 eq
3306
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.18 eq
```

```
3306
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.5 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.17 eq
1526
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.7 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.21 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.21 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.54 eq
sqlnet
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.35 eq
ftp
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.25 eq
sqlnet
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.25 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.38 eq
ssh
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.33
access-list outside extended permit tcp host 110.102.60.1 host 110.112.133.42 eq
3389
access-list outside extended permit tcp any host 110.112.133.44
access-list inside extended permit icmp any any
access-list inside extended permit ip any any
pager lines 24
logging asdm informational
mtu outside 1500
mtu management 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-621.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 172.16.0.0 255.255.255.0
static (inside,outside) 110.112.133.61 172.16.0.51 netmask 255.255.255.255
static (inside,outside) 110.112.133.6 172.16.0.6 netmask 255.255.255.255
static (inside,outside) 110.112.133.7 172.16.0.7 netmask 255.255.255.255
static (inside,outside) 110.112.133.8 172.16.0.8 netmask 255.255.255.255
static (inside,outside) 110.112.133.10 172.16.0.10 netmask 255.255.255.255
static (inside,outside) 110.112.133.11 172.16.0.11 netmask 255.255.255.255
static (inside,outside) 110.112.133.12 172.16.0.12 netmask 255.255.255.255
static (inside,outside) 110.112.133.15 172.16.0.15 netmask 255.255.255.255
static (inside,outside) 110.112.133.28 172.16.0.28 netmask 255.255.255.255
static (inside,outside) 110.112.133.20 172.16.0.20 netmask 255.255.255.255
static (inside,outside) 110.112.133.23 172.16.0.23 netmask 255.255.255.255
static (inside,outside) 110.112.133.22 172.16.0.22 netmask 255.255.255.255
static (inside,outside) 110.112.133.13 172.16.0.33 netmask 255.255.255.255
static (inside,outside) 110.112.133.14 172.16.0.34 netmask 255.255.255.255
static (inside,outside) 110.112.133.24 172.16.0.41 netmask 255.255.255.255
static (inside,outside) 110.112.133.29 172.16.0.2 netmask 255.255.255.255
static (inside,outside) 110.112.133.9 172.16.0.9 netmask 255.255.255.255
static (inside,outside) 110.112.133.27 172.16.0.27 netmask 255.255.255.255
static (inside,outside) 110.112.133.26 172.16.0.26 netmask 255.255.255.255
static (inside,outside) 110.112.133.5 172.16.0.13 netmask 255.255.255.255
static (inside,outside) 110.112.133.19 172.16.0.19 netmask 255.255.255.255
static (inside,outside) 110.112.133.4 172.16.0.4 netmask 255.255.255.255
static (inside,outside) 110.112.133.16 172.16.0.56 netmask 255.255.255.255
static (inside,outside) 110.112.133.21 172.16.0.24 netmask 255.255.255.255
static (inside,outside) 110.112.133.35 172.16.0.35 netmask 255.255.255.255
static (inside,outside) 110.112.133.25 172.16.0.54 netmask 255.255.255.255
static (inside,outside) 110.112.133.38 172.16.0.38 netmask 255.255.255.255
static (inside,outside) 110.112.133.33 172.16.0.3 netmask 255.255.255.255
static (inside,outside) 110.112.133.42 172.16.0.42 netmask 255.255.255.255
static (inside,outside) 110.112.133.18 172.16.0.216 netmask 255.255.255.255
static (inside,outside) 110.112.133.44 172.16.0.44 netmask 255.255.255.255
access-group outside in interface outside
route outside 0.0.0.0 0.0.0.0 110.112.133.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management
```

```
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet 0.0.0.0 0.0.0.0 management
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh 172.16.0.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
dhcpd address 172.16.0.210-172.16.0.220 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username root password 5UR7s8NU670UrLPQ encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect http
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3d468f00f692b6364b2485bc8a3fa65c
: end
```

第 7 章 Netflow

目录

1. Firewall

```
ASA (config)# flow-export destination inside 192.168.100.1 2055
ASA (config)# flow template timeout-rate 1
ASA (config)# access-list flow_export_acl permit ip host 10.1.1.1 host 10.2.2.2
ASA (config)# class-map flow_export_class
ASA (config-cmap)# match access-list flow_export_acl
ASA (config)# policy-map flow_export_policy
ASA (config-pmap)# class flow_export_class
ASA (config-pmap-c)# flow-export event-type flow-creation destination
192.168.100.1
```

```
flow-export destination inside 172.16.1.2 2055
flow template timeout-rate 1
access-list flow_export_acl permit ip host 172.16.1.254 host 172.16.1.2
class-map flow_export_class
match access-list flow_export_acl
policy-map flow_export_policy
class flow_export_class
flow-export event-type flow-creation destination 172.16.1.2


flow-export destination inside 172.16.1.2 2055
access-list flow_export_acl permit ip any any
class-map flow_export_class
match access-list flow_export_acl
policy-map flow_export_policy
class flow_export_class
flow-export event-type all destination 172.16.1.2
```

2. Route

```
router#enable
Password:*****
router#configure terminal
router(config)#interface FastEthernet 0/1
router(config-if)#ip route-cache flow
router(config-if)#exit
router(config)#ip flow-export destination 192.168.9.101 9996
router(config)#ip flow-export source FastEthernet 0/1
router(config)#ip flow-export version 5
router(config)#ip flow-cache timeout active 1
router(config)#ip flow-cache timeout inactive 15
router(config)#snmp-server ifindex persist
router(config)#^Z
router#write
router#show ip flow export
router#show ip cache flow
```

3. Switch

```
A Sample Device Configuration
The following is a set of commands issued on a router to enable NetFlow version 5 on the
FastEthernet 0/1 interface and export to the machine 192.168.9.101 on port 9996.

switch>(enable)ip flow-export destination 192.168.9.101 9996
switch>(enable)ip flow-export version 7
switch>(enable)ip flow-export source FastEthernet 0/1
switch>(enable)ip flow-cache timeout active 1
switch>(enable)ip route-cache flow infer-fields
```

NetFlow Statistics Collection Configuration Example

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/20ew/configuration/guide/nfswitch.html#wp1014951

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip route-cache flow
Switch(config)# ip flow-export destination 40.0.0.2 9991
Switch(config)# ip flow-export version 5
Switch(config)# end
Switch# show ip flow export
Flow export is enabled
  Exporting flows to 40.0.0.2 (9991)
  Exporting using source IP address 40.0.0.1
  Version 5 flow records
  2 flows exported in 1 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Switch#
Switch# show ip cache flow

IP Flow Switching Cache, 17826816 bytes
  0 active, 262144 inactive, 4 added
  14 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 10 seconds
  last clearing of statistics 15:48:37
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other            1      0.0         3    46      0.0       0.0      10.3
IP-other             1      0.0       100    38      0.0       0.0      10.2
Total:               2      0.0        51    38      0.0       0.0      10.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Switch#
```

```
show ip flow export              显示当前Netflow的配置。
show ip cache verbose flow       显示当前活动的流的概要，还显示设备输出了多少Netflow数据。
```

第 8 章 network experiment

目录

1. SNMP

```
enable
config terminal
snmp-server community public RO
snmp-server trap-source FastEthernet0/0
snmp-server contact [你的联系人EMAIL地址]
snmp-server enable traps
```

2. VLan Router

2.1. VLAN间DHCP

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vlan 2 name development
VLAN 2 modified:
    Name: development
Switch(vlan)#vlan 3 name market
VLAN 3 modified:
    Name: market
Switch(vlan)#exit
APPLY completed.
Exiting....

Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#int vlan 2
Switch(config-if)#ip address 192.168.8.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 3
Switch(config-if)#ip address 192.168.9.1 255.255.255.0
Switch(config-if)#exit

Switch(config)#ip dhcp pool vlan2
Switch(dhcp-config)#network 192.168.8.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.8.254
Switch(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Switch(dhcp-config)#lease 7
Switch(dhcp-config)#exit

Switch(config)#ip dhcp pool vlan3
Switch(dhcp-config)#network 192.168.9.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.9.254
Switch(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Switch(dhcp-config)#lease 7
Switch(dhcp-config)#exit

Switch(config)#ip dhcp excluded 192.168.8.1 192.168.8.254
Switch(config)#ip dhcp excluded 192.168.9.1 192.168.9.254

Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 2-3

Switch(config)#interface  range f0/1 - 10
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
Switch(config-if-range)#ip dhcp snooping trust
Switch(config-if-range)#exit
Switch(config)#interface  range f0/11 - 20
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
Switch(config-if-range)#ip dhcp snooping trust
Switch(config-if-range)#exit

Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#end
```

例 8.1. VLAN间DHCP实例

Cisco Catalyst 2960 Series Switches

```
Switch#show running-config
Building configuration...

Current configuration : 4716 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.
enable password 123456
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
ip dhcp pool vlan2
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 192.168.9.0 255.255.255.0
   default-router 192.168.9.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp snooping vlan 2-3
no ip dhcp snooping information option
ip dhcp snooping
!
!
crypto pki trustpoint TP-self-signed-2135278336
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2135278336
 revocation-check none
 rsakeypair TP-self-signed-2135278336
!
!
crypto pki certificate chain TP-self-signed-2135278336
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32313335 32373833 3336301E 170D3933 30333031 30303030
  35315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 31333532
  37383333 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100B628 478437A6 397971B0 B3A62590 C505A465 D7D1E604 DC5F92E2 68868536
  286DA2A2 3C782BCC 47625B33 5CC22974 04B26BDF F353FEFB DE2A2F27 2964BC40
  5CDEE5DE 7D9EB86F A32118E6 9345B5C4 8632832E 397D2F58 41F70394 EB49DCE9
  633DABDF 140E6ECD BA8927B4 8EF18AAB 700C9063 2C571D79 04341253 08507FA4
  5FB30203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
  551D1104 0B300982 07537769 7463682E 301F0603 551D2304 18301680 1419F564
  86C05FAB 617613B5 943AF70D 6754DF2C A3301D06 03551D0E 04160414 19F56486
  C05FAB61 7613B594 3AF70D67 54DF2CA3 300D0609 2A864886 F70D0101 04050003
  818100A2 3658FCD0 2E373F72 05DB683D 9EDD2244 0439DB83 AA6A65BE 14309A5C
  9B317329 2E5B4275 0FA7A78C 7681F7EC 8DAD3CC8 85B315F1 DA43BFB4 B4D92F6F
  0C983A7A 0C8030EE F0AE34DB 81C18F45 A2F2B98A 232430D5 EF2C3667 E9C2C1EF
  C6457E0A 1EA81332 E7691037 6A2AFF97 DBCAFECB CB673797 7D2D0547 C1D742F0 F99208
  quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
```

```
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/5
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/6
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/7
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
```

```
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan2
 ip address 192.168.8.1 255.255.255.0
 no ip route-cache
!
interface Vlan3
 ip address 192.168.9.1 255.255.255.0
 no ip route-cache
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 password 123456
 login
line vty 5 15
 password 123456
 login
!
end

Switch#
```

Cisco 2811 Router

```
Router#show running-config
Building configuration...

Current configuration : 1103 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$d51C$qZVGfyDQJHQZ/W4muxjo4/
enable password chen
!
no aaa new-model
!
resource policy
!
no network-clock-participate wic 0
ip subnet-zero
```

```
!
!
ip cef
!
!
!
!
!
controller E1 0/0/0
!
!
interface FastEthernet0/0
 ip address 192.168.3.39 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.8.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
 ip address 192.168.9.254 255.255.255.0
 no snmp trap link-status
!
router rip
 network 192.168.3.0
 network 192.168.8.0
 network 192.168.9.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
no ip http server
!
snmp-server community public RO
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password 3655927
 login
!
scheduler allocate 20000 1000
!
end

Router#
```

2.2. 多vlan与vlan间路由，并且每个vlan配合一个DHCP池，所有vlan均能访问internet

Cisco 2811 Router + 2960 Switch

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded 192.168.8.1
Router(config)#ip dhcp excluded 192.168.8.254
Router(config)#ip dhcp excluded 192.168.9.1
Router(config)#ip dhcp excluded 192.168.9.254

Router(config)#ip dhcp pool vlan2
Router(dhcp-config)#network 192.168.8.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.8.254
Router(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Router(dhcp-config)#lease 7
Router(dhcp-config)#exit
```

```
Router(config)#ip dhcp pool vlan3
Router(dhcp-config)#network 192.168.9.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.9.254
Router(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Router(dhcp-config)#lease 7
Router(dhcp-config)#exit

Router(config)#interface f0/0
Router(config-if)#ip address 172.16.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit

Router(config)#interface f0/1
Router(config-if)#description Connect to 2960_f0/24
Router(config-if)#no shut
Router(config-if)#exit

Router(config)#interface f0/1.1
Router(config-subif)#ip address 192.168.8.254 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#no shut
Router(config-subif)#exit


Router(config)#interface f0/1.2
Router(config-subif)#ip address 192.168.9.254 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#no shut
Router(config-subif)#exit

Router(config)#ip routing
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.254
Router(config)#router rip
Router(config-router)#network 172.16.0.0
Router(config-router)#network 192.168.8.0
Router(config-router)#network 192.168.9.0
Router(config-router)#exit
Router(config)#exit
Router#wr
Building configuration...
[OK]
```

```
Switch(config)#interface  range f0/1 - 10
Switch(config-if-range)#switchport access vlan 1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
Switch(config-if-range)#no shut
Switch(config-if-range)#exit

Switch(config)#interface  range f0/11 - 20
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
Switch(config-if-range)#no shut
Switch(config-if-range)#exit

Switch(config)#interface f0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#no shut
Switch(config-if)#exit

Switch(config)#interface vlan 2
Switch(config-if)#ip add 192.168.8.1 255.255.255.0
192.168.8.0 overlaps with Vlan2
Switch(config-if)#ip helper-address 192.168.8.254
```

```
Switch(config-if)#no shut
Switch(config-if)#exit

Switch(config)#interface vlan 3
Switch(config-if)#ip add 192.168.9.1 255.255.255.0
Switch(config-if)#ip helper-address 192.168.9.254
Switch(config-if)#no shut
Switch(config-if)#exit

Switch(config)#end
Switch#wr
Building configuration...
[OK]
```

例 8.2. 配置实例参考

Router: Cisco 2811 Series Routers

```
Router#show running-config
Building configuration...

Current configuration : 1592 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$d51C$qZVGfyDQJHQZ/W4muxjo4/
enable password chen
!
no aaa new-model
!
resource policy
!
no network-clock-participate wic 0
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.8.254
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.9.254
ip dhcp excluded-address 192.168.8.253
!
ip dhcp pool vlan2
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 192.168.9.0 255.255.255.0
   default-router 192.168.9.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
!
!
!
!
controller E1 0/0/0
!
!
interface FastEthernet0/0
 ip address 192.168.3.39 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
```

```
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.8.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
 ip address 192.168.9.254 255.255.255.0
 no snmp trap link-status
!
router rip
 network 192.168.3.0
 network 192.168.8.0
 network 192.168.9.0
!

Router#
```

Switch: Cisco Catalyst 2960 Series Switches

```
Switch#show running-config
Building configuration...

Current configuration : 3502 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.
enable password 123456
!
username neo password 0 chen
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip dhcp snooping information option
!
!
crypto pki trustpoint TP-self-signed-2135278336
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2135278336
 revocation-check none
 rsakeypair TP-self-signed-2135278336
!
!
crypto pki certificate chain TP-self-signed-2135278336
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32313335 32373833 3336301E 170D3933 30333031 30303030
  35315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 31333532
  37383333 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100B628 478437A6 397971B0 B3A62590 C505A465 D7D1E604 DC5F92E2 68868536
  286DA2A2 3C782BCC 47625B33 5CC22974 04B26BDF F353FEFB DE2A2F27 2964BC40
  5CDEE5DE 7D9EB86F A32118E6 9345B5C4 8632832E 397D2F58 41F70394 EB49DCE9
  633DABDF 140E6ECD BA8927B4 8EF18AAB 700C9063 2C571D79 04341253 08507FA4
  5FB30203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
  551D1104 0B300982 07537769 7463682E 301F0603 551D2304 18301680 1419F564
  86C05FAB 617613B5 943AF70D 6754DF2C A3301D06 03551D0E 04160414 19F56486
  C05FAB61 7613B594 3AF70D67 54DF2CA3 300D0609 2A864886 F70D0101 04050003
  818100A2 3658FCD0 2E373F72 05DB683D 9EDD2244 0439DB83 AA6A65BE 14309A5C
  9B317329 2E5B4275 0FA7A78C 7681F7EC 8DAD3CC8 85B315F1 DA43BFB4 B4D92F6F
  0C983A7A 0C8030EE F0AE34DB 81C18F45 A2F2B98A 232430D5 EF2C3667 E9C2C1EF
  C6457E0A 1EA81332 E7691037 6A2AFF97 DBCAFECB CB673797 7D2D0547 C1D742F0 F99208
  quit
```

```
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan2
 ip address 192.168.8.1 255.255.255.0
 ip helper-address 192.168.8.254
 no ip route-cache
!
interface Vlan3
 ip address 192.168.9.1 255.255.255.0
 ip helper-address 192.168.9.254
```

```
 no ip route-cache
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 password 123456
 login
line vty 5 15
 password 123456
 login
!
end

Switch#
```

3. VLAN下联Switch

f0/21 与 f0/22 下个链接一个交换机并用vlan2,vlan3管理下联交换机

```
Switch#show running-config
Building configuration...

Current configuration : 3800 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.
enable password 123456
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
ip dhcp pool vlan2
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 192.168.9.0 255.255.255.0
   default-router 192.168.9.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp snooping vlan 2-3
no ip dhcp snooping information option
ip dhcp snooping
!
mls qos
!
crypto pki trustpoint TP-self-signed-2135278336
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2135278336
 revocation-check none
 rsakeypair TP-self-signed-2135278336
!
!
crypto pki certificate chain TP-self-signed-2135278336
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32313335 32373833 3336301E 170D3933 30333031 30303030
  35315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 31333532
  37383333 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100B628 478437A6 397971B0 B3A62590 C505A465 D7D1E604 DC5F92E2 68868536
  286DA2A2 3C782BCC 47625B33 5CC22974 04B26BDF F353FEFB DE2A2F27 2964BC40
  5CDEE5DE 7D9EB86F A32118E6 9345B5C4 8632832E 397D2F58 41F70394 EB49DCE9
  633DABDF 140E6ECD BA8927B4 8EF18AAB 700C9063 2C571D79 04341253 08507FA4
  5FB30203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
  551D1104 0B300982 07537769 7463682E 301F0603 551D2304 18301680 1419F564
  86C05FAB 617613B5 943AF70D 6754DF2C A3301D06 03551D0E 04160414 19F56486
  C05FAB61 7613B594 3AF70D67 54DF2CA3 300D0609 2A864886 F70D0101 04050003
  818100A2 3658FCD0 2E373F72 05DB683D 9EDD2244 0439DB83 AA6A65BE 14309A5C
```

```
  9B317329 2E5B4275 0FA7A78C 7681F7EC 8DAD3CC8 85B315F1 DA43BFB4 B4D92F6F
  0C983A7A 0C8030EE F0AE34DB 81C18F45 A2F2B98A 232430D5 EF2C3667 E9C2C1EF
  C6457E0A 1EA81332 E7691037 6A2AFF97 DBCAFECB CB673797 7D2D0547 C1D742F0 F99208
  quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/22
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan2
 ip address 192.168.8.1 255.255.255.0
```

```
 no ip route-cache
!
interface Vlan3
 ip address 192.168.9.1 255.255.255.0
 no ip route-cache
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 password 123456
 login
line vty 5 15
 password 123456
 login
!
end
```

4. LAN to LAN

LAN -> Route <- LAN

```
Router#sh run
Building configuration...

*Dec 18 09:36:02.775: %SYS-5-CONFIG_I: Configured from console by console
Current configuration : 700 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
no network-clock-participate wic 0
ip subnet-zero
!
!
ip cef
!
!
!
!
!
controller E1 0/0/0
!
!
interface FastEthernet0/0
 ip address 192.168.3.39 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.6.1 255.255.255.0
 duplex auto
 speed auto
!
ip default-gateway 192.168.3.1
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
no ip http server
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end

Router#
```

5. vlan example

例 8.3. Cisco 2811 Router + 2960 Switch

```
enable
configure terminal
!
ip dhcp excluded-address 192.168.6.1
ip dhcp excluded-address 192.168.6.254
ip dhcp excluded-address 192.168.7.1
ip dhcp excluded-address 192.168.7.254
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.8.254
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.9.254

!
ip dhcp pool vlan2
   network 192.168.6.0 255.255.255.0
   default-router 192.168.6.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 192.168.7.0 255.255.255.0
   default-router 192.168.7.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan4
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan5
   network 192.168.9.0 255.255.255.0
   default-router 192.168.9.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp snooping
ip dhcp snooping vlan 2-5
!
interface FastEthernet0/13
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/15
 switchport access vlan 4
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/16
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
```

```
interface Vlan2
 ip address 192.168.6.1 255.255.255.0
 no ip route-cache
!
interface Vlan3
 ip address 192.168.7.1 255.255.255.0
 no ip route-cache
!
interface Vlan4
 ip address 192.168.8.1 255.255.255.0
 no ip route-cache
!
interface Vlan5
 ip address 192.168.9.1 255.255.255.0
 no ip route-cache
!
```

Router

```
interface FastEthernet0/0
 ip address 192.168.3.39 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.6.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
 ip address 192.168.7.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.3
 encapsulation dot1Q 4
 ip address 192.168.8.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.4
 encapsulation dot1Q 5
 ip address 192.168.9.254 255.255.255.0
 no snmp trap link-status
!
router rip
 network 192.168.3.0
 network 192.168.8.0
 network 192.168.9.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
```

例 8.4. example 2

Switch

```
interface FastEthernet0/13
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 4
```

```
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
!

interface Vlan2
 ip address 192.168.6.1 255.255.255.0
 ip helper-address 192.168.6.254
 no ip route-cache
!
interface Vlan3
 ip address 192.168.7.1 255.255.255.0
 ip helper-address 192.168.7.254
 no ip route-cache
!
interface Vlan4
 ip address 192.168.8.1 255.255.255.0
 ip helper-address 192.168.8.254
 no ip route-cache
!
interface Vlan5
 ip address 192.168.9.1 255.255.255.0
 ip helper-address 192.168.9.254
 no ip route-cache
!
```

Router

```

ip dhcp excluded-address 192.168.6.1
ip dhcp excluded-address 192.168.6.254
ip dhcp excluded-address 192.168.7.1
ip dhcp excluded-address 192.168.7.254
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.8.254
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.9.254

!
ip dhcp pool vlan2
   network 192.168.6.0 255.255.255.0
   default-router 192.168.6.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 192.168.7.0 255.255.255.0
   default-router 192.168.7.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan4
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan5
   network 192.168.9.0 255.255.255.0
   default-router 192.168.9.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
interface FastEthernet0/0
 ip address 192.168.3.39 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.6.254 255.255.255.0
```

```
 no snmp trap link-status
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
 ip address 192.168.7.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.3
 encapsulation dot1Q 4
 ip address 192.168.8.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.4
 encapsulation dot1Q 5
 ip address 192.168.9.254 255.255.255.0
 no snmp trap link-status
!
router rip
 network 192.168.3.0
 network 192.168.6.0
 network 192.168.7.0
 network 192.168.8.0
 network 192.168.9.0
 network 172.16.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
```

5.1. running-config

例 8.5. Router running-config

```
Router#show running-config
Building configuration...

Current configuration : 2333 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$d51C$qZVGfyDQJHQZ/W4muxjo4/
enable password chen
!
no aaa new-model
!
resource policy
!
no network-clock-participate wic 0
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.8.254
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.9.254
ip dhcp excluded-address 192.168.6.254
ip dhcp excluded-address 192.168.7.1
ip dhcp excluded-address 192.168.7.254
ip dhcp excluded-address 192.168.6.1
!
ip dhcp pool vlan2
   network 192.168.6.0 255.255.255.0
   default-router 192.168.6.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
```

```
!
ip dhcp pool vlan3
   network 192.168.7.0 255.255.255.0
   default-router 192.168.7.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan4
   network 192.168.8.0 255.255.255.0
   default-router 192.168.8.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan5
   network 192.168.9.0 255.255.255.0
   default-router 192.168.9.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
!
!
!
!
controller E1 0/0/0
!
!
interface FastEthernet0/0
 ip address 192.168.3.39 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.6.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
 ip address 192.168.7.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.3
 encapsulation dot1Q 4
 ip address 192.168.8.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.4
 encapsulation dot1Q 5
 ip address 192.168.9.254 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.5
!
router rip
 network 192.168.3.0
 network 192.168.6.0
 network 192.168.7.0
 network 192.168.8.0
 network 192.168.9.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
no ip http server
!
snmp-server community public RO
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password 3655927
 login
!
scheduler allocate 20000 1000
!
end
```

```
Router#
```

例 8.6. Switch running-config

```
Switch#show running-config
Building configuration...

Current configuration : 3941 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zQct$RlZjEVk3PV//OrS4KYm46.
enable password 123456
!
username neo password 0 chen
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip dhcp snooping information option
!
!
crypto pki trustpoint TP-self-signed-2135278336
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2135278336
 revocation-check none
 rsakeypair TP-self-signed-2135278336
!
!
crypto pki certificate chain TP-self-signed-2135278336
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32313335 32373833 3336301E 170D3933 30333031 30303030
  35315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 31333532
  37383333 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100B628 478437A6 397971B0 B3A62590 C505A465 D7D1E604 DC5F92E2 68868536
  286DA2A2 3C782BCC 47625B33 5CC22974 04B26BDF F353FEFB DE2A2F27 2964BC40
  5CDEE5DE 7D9EB86F A32118E6 9345B5C4 8632832E 397D2F58 41F70394 EB49DCE9
  633DABDF 140E6ECD BA8927B4 8EF18AAB 700C9063 2C571D79 04341253 08507FA4
  5FB30203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
  551D1104 0B300982 07537769 7463682E 301F0603 551D2304 18301680 1419F564
  86C05FAB 617613B5 943AF70D 6754DF2C A3301D06 03551D0E 04160414 19F56486
  C05FAB61 7613B594 3AF70D67 54DF2CA3 300D0609 2A864886 F70D0101 04050003
  818100A2 3658FCD0 2E373F72 05DB683D 9EDD2244 0439DB83 AA6A65BE 14309A5C
  9B317329 2E5B4275 0FA7A78C 7681F7EC 8DAD3CC8 85B315F1 DA43BFB4 B4D92F6F
  0C983A7A 0C8030EE F0AE34DB 81C18F45 A2F2B98A 232430D5 EF2C3667 E9C2C1EF
  C6457E0A 1EA81332 E7691037 6A2AFF97 DBCAFECB CB673797 7D2D0547 C1D742F0 F99208
  quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

```
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 4
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan2
 ip address 192.168.6.1 255.255.255.0
 ip helper-address 192.168.6.254
 no ip route-cache
!
interface Vlan3
 ip address 192.168.7.1 255.255.255.0
 ip helper-address 192.168.7.254
 no ip route-cache
!
interface Vlan4
 ip address 192.168.8.1 255.255.255.0
 ip helper-address 192.168.8.254
 no ip route-cache
!
interface Vlan5
```

```
 ip address 192.168.9.1 255.255.255.0
 ip helper-address 192.168.9.254
 no ip route-cache
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 password 123456
 login
line vty 5 15
 password 123456
 login
!
end

Switch#
```

6. Cisco Catalyst 3750 series DHCP + VLAN + Routing Example

过程 8.1. Cisco Catalyst 3750 series Example

1. 进入交换机

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

2. 划分VLAN.

```
Switch#VLAN database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.


Switch(vlan)#vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)#vlan 3
VLAN 3 added:
    Name: VLAN0003
Switch(vlan)#
```

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 172.16.0.100 255.255.255.0
Switch(config)#exit

Switch(config)#interface vlan 2
Switch(config-if)#ip address 10.10.0.1 255.255.255.0

Switch(config)#interface vlan 3
Switch(config-if)#ip address 10.10.1.254 255.255.255.0
```

3. DHCP

```
Switch(config)#ip dhcp pool vlan2
Switch(dhcp-config)#network 10.10.0.0 255.255.255.0
Switch(dhcp-config)#default-router 10.10.0.1
Switch(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Switch(dhcp-config)#lease 7
Switch(dhcp-config)#exit

Switch(config)#ip dhcp pool vlan3
Switch(dhcp-config)#network 10.10.1.0 255.255.255.0
Switch(dhcp-config)#default-router 10.10.1.254
Switch(dhcp-config)#dns-server 208.67.222.222 208.67.220.220
Switch(dhcp-config)#lease 7
Switch(dhcp-config)#exit
```

启用路由 vlan 路由

```
Switch(config)#ip routing
Switch(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.254
```

4. 配置接口

```
Switch(config)#interface GigabitEthernet1/0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)# switchport mode access
Switch(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet1/0/2 but will only
 have effect when the interface is in a non-trunking mode.
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#exit


Switch(config)#interface GigabitEthernet1/0/3
Switch(config-if)#switchport access vlan 3
Switch(config-if)#switchport mode access
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet1/0/3 but will only
 have effect when the interface is in a non-trunking mode.
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
```

5. 配置访问控制列表

```
  Switch(config)access-list 103 permit ip 192.168.2.0 0.0.0.255 192.168.3.0
0.0.0.255
  Switch(config)access-list 103 permit ip 192.168.3.0 0.0.0.255 192.168.2.0
0.0.0.255
  Switch(config)access-list 103 permit udp any any eq bootpc
  Switch(config)access-list 103 permit udp any any eq tftp
  Switch(config)access-list 103 permit udp any eq bootpc any
  Switch(config)access-list 103 permit udp any eq tftp any
  Switch(config)access-list 104 permit ip 192.168.2.0 0.0.0.255 192.168.4.0
0.0.0.255
  Switch(config)access-list 104 permit ip 192.168.4.0 0.0.0.255 192.168.2.0
0.0.0.255
  Switch(config)access-list 104 permit udp any eq tftp any
  Switch(config)access-list 104 permit udp any eq bootpc any
  Switch(config)access-list 104 permit udp any eq bootpc any
  Switch(config)access-list 104 permit udp any eq tftp any
```

应用访问控制列表

/*将访问控制列表应用到VLAN 3和VLAN 4,VLAN 2不需要*/

```
Switch(config)Int Vlan 3
  Switch(config-vlan)ip access-group 103 out
  Switch(config-vlan)Int Vlan 4
  Switch(config-vlan)ip access-group 104 out
```

6. 结束并保存配置

```
Switch(config)#end
Switch#write memory
Building configuration...
[OK]
Switch#
00:43:52: %SYS-5-CONFIG_I: Configured from console by console
```

例 8.7. Cisco Catalyst 3750 series Example

```
Switch#show running-config
Building configuration...
```

```
Current configuration : 2085 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
no aaa new-model
switch 1 provision ws-c3750g-24ts
system mtu routing 1500
ip subnet-zero
ip routing
!
ip dhcp pool vlan2
   network 10.10.0.0 255.255.255.0
   default-router 10.10.0.1
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 10.10.1.0 255.255.255.0
   default-router 10.10.1.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/3
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
```

```
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
 ip address 172.16.0.100 255.255.255.0
!
interface Vlan2
 ip address 10.10.0.1 255.255.255.0
!
interface Vlan3
 ip address 10.10.1.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.0.254
ip http server
!
!
control-plane
!
!
line con 0
line vty 5 15
!
end
```

7. Cisco Catalyst 3750 + Cisco Catalyst 2960 VTP Example

7.1. VTP Server

```
config terminal

vlan database
vtp mode server
vtp domain cisco
vtp password cisco

ip routing
!
ip dhcp pool vlan2
   network 10.10.0.0 255.255.255.0
   default-router 10.10.0.1
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 10.10.1.0 255.255.255.0
   default-router 10.10.1.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7


interface GigabitEthernet1/0/2
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/3
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!

interface Vlan1
 ip address 172.16.0.100 255.255.255.0
!
interface Vlan2
 ip address 10.10.0.1 255.255.255.0
!
interface Vlan3
 ip address 10.10.1.254 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.16.0.254


end
```

7.2. VTP Client

```
conf t
int GigabitEthernet0/2
switchport mode trunk
end

vlan database
vtp client
vtp domain cisco
vtp password cisco

interface FastEthernet0/23
 switchport access vlan 3
```

```
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!


interface FastEthernet0/24
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!

exit
```

7.3. Cisco Config File

例 8.8. 3750

```
Switch#show running-config
Building configuration...

Current configuration : 1427 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
```

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/24
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
ip http server
!
control-plane
!
!
line con 0
line vty 5 15
!
end

Switch#
Switch>
Switch>
Switch>
Switch>en
Switch#show run
Switch#show running-config
Building configuration...

Current configuration : 2085 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
no aaa new-model
switch 1 provision ws-c3750g-24ts
system mtu routing 1500
ip subnet-zero
ip routing
!
ip dhcp pool vlan2
   network 10.10.0.0 255.255.255.0
   default-router 10.10.0.1
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
ip dhcp pool vlan3
   network 10.10.1.0 255.255.255.0
   default-router 10.10.1.254
   dns-server 208.67.222.222 208.67.220.220
   lease 7
!
!
!
!
no file verify auto
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/3
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
 ip address 172.16.0.100 255.255.255.0
!
interface Vlan2
 ip address 10.10.0.1 255.255.255.0
!
interface Vlan3
 ip address 10.10.1.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.0.254
ip http server
!
!
control-plane
```

```
!
!
line con 0
line vty 5 15
!
end
```

例 8.9. 2960

```
Switch#show running-config
Building configuration...

Current configuration : 1427 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
```

```
!
interface FastEthernet0/23
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface FastEthernet0/24
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping trust
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
ip http server
!
control-plane
!
!
line con 0
line vty 5 15
!
end
```

第 9 章 FAQ

目录

1. switchport trunk encapsulation dot1q 提示 invaild input at^marker.

switchport trunk encapsulation dot1q它提示无效的输入 invaild input at^marker.^就是指向encapsulation的位置

对于switchport trunk encapsulation dot1q中的错误是因为encapsulation dot1q 是不用配置的，也就是说它只支持dot1q协议。不用配置。如果你遇到一个支持sli 和dot1q两个协议的交换机时才用。

第 10 章 Reference

目录

1. Cisco IOS IP Configuration Guide, Release 12.2

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html

2. Cisco IOS Firewall

http://www.cisco.com/en/US/products/sw/secursw/ps1018/tsd_products_support_series_home.html

3. Network Command

http://networkcommand.org/cisco/