学 习 笔 记

蓝狐网络技术

Bluefox-T24-XiaoGe

2008-09-01

QQ：844978372

目　　录

学习笔记

Lesson 1　IP寻址

一、　为什么需要 IP 地址？

IP 地址唯一区分和标识资源所属的主机

Windows 下查看：ipconfig /all

IP 地址由网络号和主机号组成

网关用于解决主机和外网的通信

二、　IP 地址的分配原则

1. 唯一性
2. 按块划分
3. 可扩展性
4. 私有性
5. 业务对应性

三、　IP 地址的分类

一般分成五类：

A 类：0.0.0.0~127.255.255.255

B 类：128.0.0.0~191.255.255.255

C 类：192.0.0.0~223.255.255.255

D 类：224.0.0.0~239.255.255.255

E 类：240.0.0.0~255.255.255.255

保留：127.0.0.1　　0.0.0.0

私有地址：10.0.0.0/8　　172.16.0.0/12　　192.168.0.0/16

可用地址：能够在设备上和主机上配置的地址

不可用地址：主机位全 0 的表示网络本身；主机位全 1 表示该网络内的所有主机

网关地址：需要提取一个地址用来作网关，实现不同网段的主机通信

四、　子网划分

根据企业的需求，把一个大的网络划分成若干个小的网络就叫子网划分

通过改变子网掩码来表达划分子网的意图

划分子网的目的：隔离广播；实现受控访问

五、　IP 子网的快速划分

模：256

魔术数：2n　n 代表主机位和网络位分界的字节中的剩余主机位

子网掩码：模 - 魔术数

子网号：前一个子网 + 魔术数

可用主机：$2^m - 2$　　m 代表剩余主机位

六、　VLSM；变长子网掩码

普通用户：/24

特殊用户：/29

网络设备：/30

七、 私有地址的 NAT

为了保证地址唯一性，只允许公有地址上 Internet

而启用内网往往都是使用私有地址，这时需要 NAT 把私有地址转换成公有地址上 Internet。

【返回目录】

Lesson 2 TCP、IP基础

一、 协议，Protocol

通信双方事先约定并共同遵守的标准或准则

数据通信是由实现了相同协议的软硬件相互配合完成的

若干相互交联的协议组成了协议族

二、 通讯模型

OSI 七层模型

应用层、表示层、会话层、传输层、网络层、数据链路层、物理层

功能由协议完成

对等通讯

下层为上层服务

三、 应用层服务

应用程序与网络的接口解决通信的可用性问题

应用层的常见协议

HTTP 、FTP 、TFTP、 TELNET、 SNMP 、POP3、 SMTP 、DNS 、DHCP

四、 传输层

作用：为应用层提供端到端的传输服务

常见协议：TCP UDP

TCP 的数据结构：

源端口			目标端口
序列号			
确认号			
报头长度	保留	标记	窗口
校验和			紧急
选项			
Data			

UDP 的数据结构：

源端口	目标端口
报文长度	校验和
Data	

工作原理：TCP

Tcp：面向连接的、可靠的、有序的、流量控制的

Tcp 的数据结构：

Tcp 的协议包叫段：segment

Tcp 的端口号：源端口号由发送方的系统进程随机产生大于等于 1024 的一个端口号，目标端口一般都为知名端口号。

常见协议的端口号：

FTP：20、21

SSH：22

Telnet：23

SMTP：25

TACACS：49

DNS：53

DHCP：67、68

TFTP：69

HTTP：80

POP3：110

NTP：123

NETBIOS：137、138、139

HTTPS：443

参考书《TCP IP 协议族》《TCP IP 详解》

工作原理：UDP

- ✧ 无连接的，不可靠的，无序的，无流量控制的
- ✧ UDP 的数据结构：
- ✧ TCP 只支持目标 IP 是单播的上层应用
- ✧ UDP 支持目标 IP 是单播和多播以及广播的上层应用

端口号分为：

1.熟知端口号：0-1023 由 IANA 指派和控制

2.注册端口号：1024-4951 IANA 不指派也不控制，可在 IANA 注册，防止出现重复。

3.动态端口：4952-65535 不用指派、注册，可由任何进程来使用，是短暂端口。

五、 网络层

作用：提供主机的传输服务，通过 IP 地址标识不同主机

常见协议：IP、IPX

IP 报文结构：

版本	首部长度	服务类型	总长	
标识			标志	偏移量
TTL	协议	首部校验和		
源 IP				
目标 IP				
选项				填充
数据				

- **版本：**目前基本取值 4，因为 Ipv6 有自己的报文结构
- **首部长度：**4bit，取值 0~15，一个单位代表 4 个字节，首部最大 60 字节
- **服务类型：**8bit，前三个比特表示优先级，
- **总长：**16bit，表示数据包最大长度 65535 字节
- **标识：**16bit，为了使分段后的各个数据包能够准确重组
- **标志：**3bit，第一个比特保留，第二个比特表示 Don’t Fragment ，第三个比特表示 More Fragment
- **偏移量：**13bit，用在分片中
- **TTL：**8bit，防止 IP 包循环。每经过一个路由器 TTL 减一
- **协议：**8bit，标识传输层的协议；TCP 为 6；UDP 为 17 等等
- **校验和：**16bit，检查 IP 首部的完整性
- **源 IP：**32bit，发送 IP 包的主机地址
- **目标 IP：**32bit，接收 IP 包的主机地址
- **选项：**用于网络测试和排错，最大 40 个字节

ICMP 报文结构：

类型	代码	校验和
首部的其余部分		
数据部分		

常见的 ICMP Echo Request 包：类型 8、代码 0

常见的 ICMP Echo Response 包：类型 0、代码 0

路由协议：辅助建立路由表并指导 IP 包如何转发

特性：无连接的、不可靠的、无序的、无流量控制的、尽力而为的

六、 测试工具

PING：测试网络的基本连通性，模拟用户发送小的，少量的 IP 包测试双向连通性

原理：发送方产生 ICMP 的 echo request

中间的路由器传输这个 IP 包到目的地

接收方产生 ICMP 的 echo reply

PING 不通的原因：

TRACERT：探测 IP 包所经过的路径

发送方产生三个 IP 包

收到 IP 包后把 TTL 减 1，如果 TTL 为 0 路由器则丢弃，ICMP 报告超时错误

收到 ICMP 的超时错误，把 TTL 加 1

TELNET：一个明文的登陆管理工具，也可以用来做探测测试

如telnet www.xiaoge.cn 80

七、 数据链路层

作用：解决在各种介质上传输数据；为了屏蔽差异性，使用数据链路层协议

LAN：以太网，令牌环，FDDI，ATM

WAN：PPP，HDLC，

以太网帧结构：

目标 Mac	源 Mac	TYPE	Data	CRC

ARP（Address Resolution Protocol）：地址解析协议，是一种将 IP 地址转化成物理地址的协议。

ARP 原理：某机器 A 要向主机 B 发送报文，会查询本地的 ARP 缓存表，找到 B 的 IP 地址对应的 MAC 地址后，就会进行数据封装和传输。如果未找到，则广播 A 一个 ARP 请求报文（携带主机 A 的 IP 地址 Ia——物理地址 Pa），请求 IP 地址为 Ib 的主机 B 回答物理地址 Pb。网上所有主机包括 B 都收到 ARP 请求，但只有主机 B 识别自己的 IP 地址，于是向 A 主机发回一个 ARP 响应报文。其中就包含有 B 的 MAC 地址，A 接收到 B 的应答后，就会更新本地的 ARP 缓存。接着使用这个 MAC 地址发送数据（由网卡附加 MAC 地址）。因此，本地高速缓存的这个 ARP 表是本地网络流通的基础，而且这个缓存是动态的。

ARP 协议并不只在发送了 ARP 请求才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。因此，当局域网中的某台机器 B 向 A 发送一个自己伪造的 ARP 应答，而如果这个应答是 B 冒充 C 伪造来的，即 IP 地址为 C 的 IP，而 MAC 地址是伪造的，则当 A 接收到 B 伪造的 ARP 应答后，就会更新本地的 ARP 缓存，这样在 A 看来 C 的 IP 地址没有变，而它的 MAC 地址已经不是原来那个了。由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输。所以，那个伪造出来的 MAC 地址在 A 上被改变成一个不存在的 MAC 地址，这样就会造成网络不通，导致 A 不能 Ping 通 C！这就是一个简单的 ARP 欺骗。

ARP 欺骗的种类:

对路由器 ARP 表的欺骗

对内网 PC 的欺骗

局域网 ARP 欺骗的解决方法：

PC 安装 ARP 防火墙，防止 ARP 欺骗

思科交换机的 DAI

交换机的 Port-ACL

链路层设备：交换机，网桥

八、 物理层

解决信号如何在介质上传输

物理层设备：Hub

【返回目录】

Lesson 3 IOS基础

一、 路由器的基本组件

- ROM：相当于 PC 的 BIOS，用来引导 IOS 映像
- Flash：相当于 PC 的硬盘，用来存储 IOS 映像和其他文件
- DRAM：相当于 PC 的内存，用来运行 IOS 系统
- NVRAM：非易失性随机存储器，存储初始或启动配置文件
- 接口：相当与 PC 的网卡，用来连接不同的设备
- 访问端口：console

  Vty

路由器的启动顺序：

思科路由器启动顺序	加电自检	
ROM	Bootstrap	Load Bootstrap
FLASH 1	Cisco	Locate and Load Operating System
TFTP SERVER 2	Internetwork	
ROM 3	Operating System	
NVRAM 1	Configuration file	Locate and configuration File or Enter Setup Mode
TFTF SERVER 2		
CONSOLE 3		
ROM 里有最小维护版本的 IOS~		

二、 IOS 的基本配置

具体的基本配置：

基本路由器的检验命令：

show version

show processes

show protocols

show mem

show ip route

show startup-config

show running-config

show flash

show interfaces

基本路由配置命令

进入：config terminal/memory/network 配置网络时常采用的命令：copy

1. 标识：hostname 标识名
2. 启动标识：banner 启动标识
3. 接口：interface 端口号
4. 密码：line 0 6

login

passwd 口令

enable password/secret 口令

5. 接口：

1）配置端口

interface 端口号

clock rate 时钟速率（64000）/* 在串口中配置 */

bandwidth 带宽（缺省 56） /* 在串口中配置 */

media-type 介质类型 /* 在以太网口上 */

early-token release /* 在令牌环网口上 */

ring-speed 16 /* 在令牌环网口上 */

no shutdown

write memory

2）检验端口

show interfaces

show controllers

6． 配置环境

1） 引导方式

boot system flash IOS-filename

boot system tftp IOS-filename tftp-address

boot system rom

2） 配置 Register 值

config-register 0x2102

7． 查看邻居路由

show cdp interface

show cdp neighbors [detail]

show cdp entry routerA

8． IP Address 配置

Ip address 网络地址 掩码

Ip host 主机名 address

Ip name-server 服务器地址 1 服务器地址 2 。。。

Ip domain-lookup nsap

Show hosts

Ping 主机名/IP 地址

Trace 主机名/IP 地址

IP 路由

1． 静态路由

ip routing

ip route 目标网络号 掩码 端口号 [permanent]

2． 缺省路由

ip default-network 网络号

3． 动态路由

1） RIP 配置

Router rip

Network 网络号

Show ip route

Show ip protocol

Debug ip

2） OSPF 配置

Router ospf 进程号

Redistribute 其它路由协议

Network 端口网络 反掩码 area 区域号

Area 区域号 range 网络号 掩码

Area 区域号 default-cost 花销值

Ip ospf priority number

Ip ospf cost 花销值

Show ip ospf database

3） BGP 配置

Router bgp 自治域号

Redistribute 其它路由协议

Network 网络号 /* 自治域内 */

Aggregate-address 网络号 掩码 summary-only 汇总网络

Neighbor 相邻网络号 remote-as 自治域号 /* 自治域间的网络 */

流量控制

1） 被动端口

passive interface 端口号

2） 缺省路由

ip default 网络号/端口网络

3） 静态路由

ip route 目标网络号 掩码 端口号

4）ACL 过滤表

(全局上) access-list 访问号 1 {permit|deny} 反掩码号 [established]

access-list 访问号 2 {permit|deny} IP/TCP 协议 源网络 目的网络

操作符 参数

(端口上)access-group 访问号 in|out

distribute-list 访问号 in|out 端口号

5） Null 0 interface

Ip route address mask null 0

广域网配置

1） PPP

Ppp pap sent-usename 封装

Ppp chap hostname

Ppp chap password

2）X.25

encapsulation x25 [dce]

x25 address

x25 map 协议地址 /*SVC */

x25 pvc pvc 号 ip 地址 x25 地址 /*PVC */

ip switching

x25 route x.121 地址 接口 x.121 映射地址

3） FrameRelay

Frame-relay local-dlci IP 网络号

Frame-relay map 协议地址

Frame-relay lmi-type ansi

三、 IOS 恢复

第一种方法：系统还可以启动到配置模式时

使用 copy tftp flash 即可升级还原以前的 IOS

第二种方法：IOS 被删除后的恢复

如果因为误操作将 FLASH 中的 IOS 删除了，原 IOS 中的大部分命令都无法具体的过程如下，那么 ROUTER 将进入 ROM 使用。此时，可以通过 TFTP 服务器向中存储的基本 IOS 模式，在这种模式下 ROUTER 传输 IOS，使系统得已恢复。其在一台机器上安装 TFTP 服务器软件，将 IOS 文件放置在 TFTP 服务器的默认根目录下，打开 TFTP 服务器，用控制线将这台机器与 ROUTER 连接起来，另外用交叉网线连接机器的网卡和 ROUTER 的以太口。（也可以用普通的网线将 ROUTER 和交换机相连再连接机器）做好以上工作后，打开机器的超级终端工具，连接上 ROUTER，此时窗口中出现的命令行提示符为: ROMMON 1 > （其中“1”代表命令行的行数）。在提示符后输入命令：

（可以使用 ctrl+break 组合键进入 ROMMON 模式）

ROMMON 1 >IP_ADDRESS= ROUTER 的 IP 地址（要和 TFTP 服务器在同一网段内）

ROMMON 2 >IP_SUBNET_MASK= ROUTER 的子网掩码

ROMMON 3 >DEFAUT_GATEWAY= 默认网关地址 （可以没有，也可以是 TFTP 服务器）

ROMMON 4 >TFTP_SERVER= TFTP 服务器 IP 地址

ROMMON 5 >TFTP_FILE= IOS 文件名（只给出文件名，不需要路径）

ROMMON 6 >tftpdnld 回车

注意：前面的几条命令必须使用大写，而最后的 tftpdnld 则要用小写。

在 tftpdnld 命令执行后，只行下，输入 reset 重启 ROUTER，要根据提示选，就可完成文件的传重启后就又回到了熟悉的 IOS 模式下输。当文件传输完后，将自动回到命令甚至连以前配置的信息都不会丢失。

第三种方法：通过 Xmodem 升级 2610 的 IOS 实例

如果你不小心使用了命令 erase flash 那么发生什么就可想而知了。因此，建议在你拿到路由器等网络设备时 最好先将它的 IOS 等操作系统备份出来，以备万一！

本篇主要介绍通过 Xmodem 上传 IOS 的过程（以 2610 为例，不过这个方法用在其他设备上没什么太大区别）

准备工作，只要有 Cisco 原配的线缆就可以（注：Xmodem 与实际的 modem 没有任何联系 只是一个传输协议 数据是通过终端的串口和路由器的 Console 口灌进去的）

在没有 IOS 的情况下 系统只能进入 Rommon 状态，在这个状态下只能见到如下命令：

rommon 8 > ?

alias set and display aliases command

boot boot up an external process

break set/show/clear the breakpoint

confreg configuration register utility

cont continue executing a downloaded image

context display the context of a loaded image

cookie display contents of cookie PROM in hex

dev list the device table

dir list files in file system

dis display instruction stream

dnld serial download a program module

frame print out a selected stack frame

help monitor builtin command help

history monitor command history

meminfo main memory information

repeat repeat a monitor command

reset system reset

set display the monitor variables

stack produce a stack trace

sync write monitor environment to NVRAM

sysret print out info from last system return

tftpdnld tftp image download

unalias unset an alias

unset unset a monitor variable

xmodem x/ymodem image download

在这个模式下，输入 Xmodem

rommon 9 > xmodem -r

会提示如下警告：

WARNING: All existing data in bootflash will be lost!

Invoke this application only for disaster recovery.

Do you wish to continue? y/n [n]: y

Ready to receive file ? ...

然后在超级终端的传送栏目=> 选择发送选项 => 再选择 Xmodem 并指明 IOS 所在的路径即开始上传 IOS,等待时间很长，视 IOS 的大小和传输速度。对于初次做 IOS 上传，建议不要去修改什么传输速率。传完以后对整个系统初始化 界面如下：

Erasing flash at 0x603c0000

program flash location 0x602f0000

Download Complete!

program load complete, entry point: 0x80008000, size: 0x2f0074

Self decompressing the image :

##

[OK]

四、 IOS 升级

首先启动 Cisco TFTP Server，准备好升级的 IOS 放到 TFTP 根目录下。

当然也可以使用 FTP。

Router#copy tftp flash

Source filename []? c2500-d-1.121-8a.bin

Address or name of remote host []? 172.16.162.58

Destination filename [c2500-d-1.121-8a.bin]? (按回车键确认)

系统提示是否在拷贝之前将 Flash 中的文件系统删除，按回车键确认后系统再次提示删除操作将把 Flash 中的所有文件清除，问是否继续，再次按回车键确 认删除操作。一系列的"e"表示正在进行删除 Flash 上文件系统的操作。接下来是文件复制的进程，同样以一系列的"!"来表示，"!"的数目越多表示文件越大。

最后系统对 IOS 文件进行了校验，并确认传输没有错误，IOS 软件升级操作即告完成。

IOS 软件升级完成后，需要重新启动路由器，使得新软件进入运行状态。

IOS 软件的升级对存放在 NVRAM 中的启动配置文件并不产生任何影响，路由器的启动配置文件还是原来的文件。

五、 IOS 密码恢复

2500 及以前

将一台终端或装有超级终端软件的 PC 接到设备的 console 口上

在启动的 60 秒内按下中断键，使设备进入 rommon 状态.

>o/r 0x2142 #修改寄存值，使之路由器启动不加载配置文件

>i #重启

重启后，就进去了没有运行配置文件的系统，可以使用 Show startup-config 查看密码，如果密码被加密了，则需要复制 startup-config 文件到 Running-config 文件中，先删除原有密码，然后设置新密码，再保存配置文件。

把寄存值改回去：(router-config)#config-register 0x2102

重启路由器即可~

3600 以其以后的路由器：

开机 30 秒内按住 Ctrl+break 使之进入 Rommon 模式

修改寄存值：>confreg 0x2142

重启路由器：>reset

路由器运行后查看配置文档或删除密码，同上！

交换机密码恢复：

用 Console 线把 PC 和交换机相连，打开终端

断电，重启交换机

接上电源后，按住 Mode 键，待终端出现 Switch：的提示即可放下

在 switch：flash_init #使之初始化

Cat flash:config.text #查看 flash 下的 config.text 配置文件，可以看到密码（加密的继续下一步）

Rename flash:config.text flash:t24.text　　#重命名启动文件

重启交换机 boot 命令，copy flash:t24.text running-config

删除密码：no enable password/secret

保存配置文件

六、　PIX 密码恢复

本方法只是针对没有 floppy 的 PIX，采用 TFTP 进行文件传输。

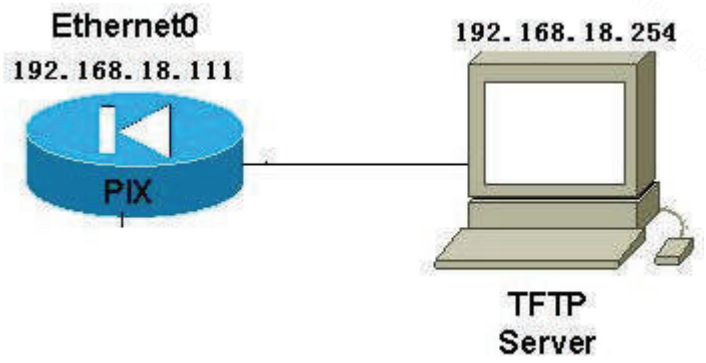
1、准备：

1）PC 一台，其上安装 TFTP 服务器

2）交叉线一条，连接 PIX 以太网口和 PC 网卡

3）下载密码恢复软件（根据 PIXOS 的版本选择不同的恢复软件），放到 TFTP 服务器的目录下

2、网络拓扑示意图



3、详细恢复过程：

启动 PIX，ctrl+breack，进入到 monitor>模式下，执行下面的操作：

monitor> interface 0

0: i8255X @ PCI(bus:0 dev:13 irq:10)

1: i8255X @ PCI(bus:0 dev:14 irq:7)

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9

monitor> address 192.168.18.111

address 192.168.18.111

monitor> server 192.168.18.254

server 192.168.18.111

monitor> file np63.bin

file np63.bin

monitor> gateway 192.168.18.254

gateway 192.168.18.254

monitor> ping 192.168.18.254

Sending 5, 100-byte 0xf8d3 ICMP Echoes to 192.168.18.254, timeout is 4 seconds:

!!!!!

Success rate is 100 percent (5/5)

monitor> **tftp**

tftp np63.bin@192.168.18.254 via 192.168.18.254.....

Received 92160 bytes

Cisco Secure PIX Firewall password tool (3.0) #0: Tue Aug 22 23:22:19 PDT 2000

Flash=i28F640J5 @ 0x300

BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] **y**

Passwords have been erased.

Rebooting....重新启动后就可以了！

4、相关软件：根据 PIX 的不同 OS 版本进行选择。

np70.bin　　#适合 PIXOS 版本为 7.0 以后的~

np50.bin

np51.bin

np52.bin

np53.bin

np60.bin

np61.bin

np62.bin

np63.bin　　#适合 PIXOS 版本为 6.3 的~

七、　ASA 密码恢复

普通的恢复类似 IOS 路由器：
进入 CONSOLE 的物理连接，重启设备

```
You can press the Esc (Escape) key after "Use BREAK or ESC to interrupt boot" is shown. This will take you into ROMMON mode, as follows:
rommon #0>
rommon #0> confreg
Current Configuration Register: 0x00000011
Configuration Summary: boot TFTP image, boot default image from Flash on netboot failure
Do you wish to change this configuration? y/n [n]: y

disable system configuration? y/n [n]: y
```

红色部分是需要键入的命令

设备接着执行，将提示：

```
Current Configuration Register: 0x00000040
Configuration Summary: boot ROMMON ignore system configuration
Update Config Register (0x40) in NVRAM...
```

这里将 0X11 启动模式转变到 0X40 模式——类似 IOS 的 0X2102 到 0X2142

```
rommon #1> boot
```

重新启动，将进入以下模式：

```
ciscoasa>
ciscoasa> enable
Password:<cr>
ciscoasa#
```

现在

```
ciscoasa# copy startup-config running-config 完成密码重设
Chicago# config terminal
Chicago(config)# passwd cisco123
Chicago(config)# enable password cisco123
```

改回启动方式

```
Chicago(config)# config-register 0x11
```

最后需要保存

```
Chicago(config)# copy running-config startup-config
```

【返回目录】

Lesson4 LAN技术基础

一、 局域网技术

1. Lan 的定义：是在同一个管理组织机构下的通信系统，使得计算机等设备通过互连介质在一个较小的范围内互连形成的可以实现资源共享以及数据通讯网络
2. Lan 的实现技术：

二、 以太网技术

传统以太网技术：（共享式以太网）

HUB：工作在物理层，没有地址的概念，洪泛数据包，造成广播过大

逻辑拓扑为总线结构，采用 CSMA/CD 机制解决冲突问题

碎片：小于 64 字节的数据包就叫碎片

现代以太网技术：（交换式以太网）

Switch：工作在数据链路层，基于 Mac 地址进行数据转发

交换机采用交叉交换矩阵总线结构，建立多条点对点的并发连接

交换机能减小冲突域，但还是没有解决广播域的问题

交换机一个端口一个冲突域，采用全双工（缓存）解决冲突

Mac 表：由 Mac 地址、端口号、Vlan 号组成。默认失效时间 Win 下

三、 交换机技术

交换机基本功能：

Mac 地址的学习功能

转发、过滤、洪泛数据帧

转发 Mac 表能够匹配的单播帧

过滤源 Mac 和目标 Mac 在同一端口上的数据

洪泛未知目标 Mac 的单播帧

交换机的基本配置：

删除相关文件

Config.text //交换机默认保存启动的文件

Vlan.dat //交换机中创建了的 Vlan 信息

查看文件 dir

删除文件 delete *.*

主机命名：hostname bluefox

口令设置：enable password bluefox

配置端口：int f0/1.....

配置管理地址： int vlan 1 ip address 192.168.1.253 255.255.255.0

配置线路密码： line vty 0 4 password bluefox login

配置网关： ip default-gateway 192.168.1.254

Vlan 技术：

Vlan 的定义：Vlan 是指交换机上创建的能将代表一个大的广播域的物理 Lan 分隔成若干个小的广播域的逻辑 Lan，这个逻辑 Lan 就是 Vlan。

Vlan 的特性：

一个 Vlan 一个广播域

一个 Vlan 一个独立的 IP 网段

一个 Vlan 可以跨越多个交换机，一个交换机上可以创建多个 Vlan

Vlan 之间所以数据（单播、多播、广播）均被隔离

一个 Vlan 内可以包含一组接口，也可以不包含任何接口

同一 Vlan 不同 IP 网段不能通信；同一 IP 网段不同 Vlan 不能通信

Vlan 的作用：

隔离广播域

组网的安全性

组网的灵活性

四、 Vlan 的类型

以太网 Vlan

令牌环 Vlan

FDDI Vlan

ATM Vlan

五、 Vlan 的创建、实施

基于端口

基于 Mac

基于用户名

基于 IP

创建 Vlan

全局配置模式：configuration terminal vlan 2 name v2 exit

特权配置模式：vlan database vlan 2 name v2 vlan3 name v3 exit

Vlan 与接口的绑定：int f0/1switch mode access switch access vlan 2

Int range f0/1 – 10 switch mode access sw ac vl 2

查看 Vlan 与接口的绑定：show vlan

Vlan 的保存：

正常情况下，Catalyst 交换机自动保存创建 Vlan 的信息于 Vlan.dat 文件；但 Vlan 与接口的绑定信息以及其他交换机的配置均保存在 config.text 内。

Vlan 的删除：

Conf t　　no vlan 2

注：被删除的 Vlan 中的接口会处于挂起状态的，不能接受和发送任何数据。并且在 show vlan 时也不会显示出来，需要人工把它放到其他 Vlan 中去。

Vlan 的支持：

不同的交换机或者不同的 IOS 版本所支持的 Vlan 数量也不同

【返回目录】

Lesson 5　　Trunk

一、　Trunk 的作用

Access：承载正常的以太网帧，仅仅属于某个特定的 Vlan

Trunk：承载被打标识的以太网帧，Cisco 设备缺省能够承载所有 Vlan 的流量

二、　Trunk 的封装

ISL：Cisco 私有的用来标记 Vlan 信息的协议，该协议通过对原始的以太网帧进行头部和尾部的重新封装。

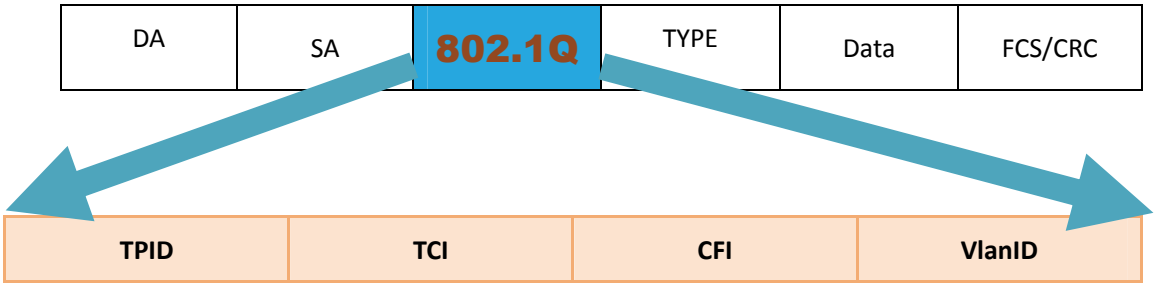
802.1Q：802.1Q 是 IEEE 标准的 Vlan 标签格式。它允许 Vlan 标记帧可以在不同厂家的交换机之间传递。它只使用了额外的四个字节插入原有的以太网帧中。

标记协议标识符（TPID）：16bit

标记控制信息（TCI）：3bit

规范格式指示器（CFI）：1bit

VlanID：12bit



三、 Trunk 的配置

静态配置：

Int f0/1

Switchport trunk encapsulation isl/dot1q/negotion

Switchport mode trunk

动态配置

DTP（Dynamic Trunk Protocol）

目前只有 Cisco 交换机缺省支持自动协商 Trunk 的功能，该功能依赖于 Cisco 的私有协议。该协议主要用于协商两台交换机之间的链路能否成为中继链路。

通过 DTP 协议交互的参数有 VTP 域名，Trunk 的封装以及 Trunk 的模式。

VTP 域名默认为空

DTP 的工作模式：

On

Off

Desirable

Auto

Nonegotiable

能自动协商的 DTP 模式：

On-on on-auto on-desirable

Trunk 中添加、删除 Vlan

Switchport trunk allowed vlan {add|remove|except|all} vlan-list

【返回目录】

Lesson 6 VTP

一、 VTP 的基本概念：

是在二层交换网络中用来动态配置与管理 Vlan 信息，使得交换机上 Vlan 的数据库保持一致的一种 Cisco 私有二层协议。

二、 VTP 的基本原理：

基本操作思路：

在交换机 Trunk 上交互 VTP 信息，使得位与同一个 VTP 域名内的交换机自动进行 Vlan 的添加、删除和修改。

VTP 域：

具有相同 VTP 域名且通过 Trunk 互连的交换机集合

VTP 域名默认为空，为空时交换机只能接受和处理 DTP 数据包，不能发送

VTP 消息同步，只对交换机产生影响，不对用户数据产生影响

VTP 消息：

VTP 汇总通告：交换机每 5 分钟发送一次汇总通告，通告邻居目前的 VTP 域名和配

置修订号。

VTP 通告请求：在交换机重启后或 VTP 参数改变的时候发送通告请求。

VTP 子网通告：VTP 服务器上删除或创建、修改了 Vlan 就发送子网通告。

VTP 加入消息：

VTP 的同步原则：

VTP 域名、版本、口令都必须相同（域名默认为空，版本默认为 1，口令为空）

VTP 配置修订号高的同步配置修订号低的

VTP 只在 Trunk 链路上承载

VTP 只同步 Vlan 信息，不同步 Vlan 与接口的绑定信息

VTP 模式：

Sever：能在本地删除、创建、修改 Vlan 信息；可以产生、发送、接收、处理、转发 VTP 消息

Client：不能在本地删除、创建、修改 Vlan 信息；可以产生、发送 VTP 消息

Transparent：能在本地删除、创建、修改 Vlan 信息；只能转发 VTP 消息；不能发送自身的 Vlan 消息；修订号始终为 0

VTP 配置：

VTP 域名：vtp domain bluefox

VTP 版本：vtp version 1

VTP 口令：vtp password xiaoge

VTP 模式：vtp mode {client | server | transparent}

VTP 修剪：vtp pruning

【返回目录】

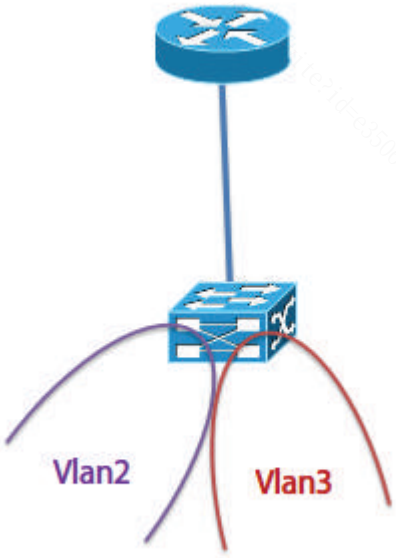
Lesson 7　Vlan间路由

一、　Vlan 间路由的基本概念

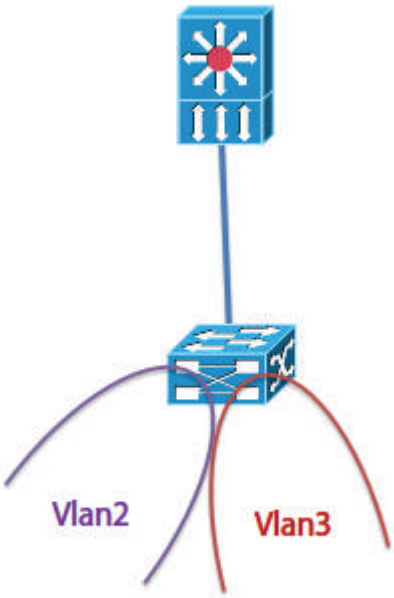
1. 本质：解决不同网段之间的通信问题
2. 关键：找网关

二、　Vlan 间路由的解决方案

1. 路由器：旁挂路由器解决方案



2. 交换机：采用三层交换机解决方案



单臂路由器 Vlan 间路由：

1. 配置二层交换机

   部署 Vlan

   部署 Trunk

2. 配置路由器

   Int e0

   No sh

   Ip add 192.168.1.254 255.255.255.0

   Int e0.2

   Encapsulation dot1q 2

   Ip add 192.168.2.254 255.255.255.0

   Int e0.3

   Encapsulation dot1q 3

   Ip add 192.168.3.254 255.255.255.0

子接口的 Mac 都采用物理接口的 Mac 地址

802.1Q 协议有 Native Vlan 的概念：

默认的 Native Vlan 是 Vlan 1，用来承载管理数据如：VTP、DTP、BPDU 以及用户数据

三层交换机的 Vlan 间路由

定义：具有三层路由转发功能的交换机，基于硬件实现路由转发功能的交换机

应用：采用 SVI 接口作为各个 Vlan 的网关

配置：

```
int vlan 1
ip add 192.168.1.254 255.255.255.0
int vlan 2
ip add 192.168.2.254 255.255.255.0
int vlan 3
ip add 192.168.3.254 255.255.255.0
```

【返回目录】

Lesson 8 STP

一、 基本定义

是交换机通过某种特定的算法来逻辑地阻塞某些端口以达到避免数据转发循环，从而生成一个无环路的数据转发路径的一种二层协议。

二、 操作原理

基本工作思想：

通过比较交换机之间彼此交互的 BPDU 中的相关参数，选出根网桥、根端口、指定端口、剩下的则为阻塞端口。

相关术语：

根网桥：在所有交换机中具有最小网桥 ID 的交换机。

网桥 ID 的组成：网桥优先级+背板 Mac+VlanID

根端口：位于根网桥上的具有到根网桥最小路径开销的端口

开销参考： 10M 100

100M 19

1000M 4

10000M 2

指定端口：每个交换网段中具有最小根路径开销的接口

BPDU：网桥协议数据单元

目标 Mac：0x01-80-c2-00-00-00

0x01-80-0c-cc-cc-cd

源 Mac：发送 BPDU 的交换机背板 Mac 地址

```
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Spanning Tree (0)
BPDU Type: Configuration (0x00)
BPDU flags: 0x00
  0... .... = Topology Change Acknowledgment: No
  .... ...0 = Topology Change: No
Root Identifier: 32768 / cc:01:03:54:00:00
Root Path Cost: 0
Bridge Identifier: 32768 / cc:01:03:54:00:00
Port identifier: 0x8006
Message Age: 0
Max Age: 20
Hello Time: 2
Forward Delay: 15
```

TCN-BPDU：感知网络拓扑变化的交换机产生，由根端口发出去，发往根网桥，用来加快 Mac 表的收敛，时间为 15s，比 Mac 表自身的更新时间 300s 快。

配置 BPDU：只要根网桥才能发送配置 BPDU

STP 核心算法：

确定最小的根网桥 ID：选举根网桥

确定最小的根路径开销：选举根端口、指定端口

确定最小的发送网桥 ID

确定最小的端口 ID

三、 STP 选举过程

根网桥：初始化时每个交换机都认为自己是根网桥，都向外发送配置 BPDU

根端口：

收到的 BPDU 中的根路径开销+本地接口速率的开销之和

收到的 BPDU 中的发送网桥 ID

收到的 BPDU 中的端口 ID

知道端口：

发送出去的 BPDU 中的根路径开销

根网桥上的所有活动端口都为指定端口

四、 STP 的配置

配置目的：

使得所形成的无环路转发路径是最优的

在实现主备备份的同时实现业务的分离

工作模式：

CST

PVST

PVST+

具体配置：

STP 在思科的交换机上默认已经开启

指定根网桥：spanning-tree vlan 2 root primary

端口开销：spanning-tree vlan 2 cost 23

端口优先级：spanning-tree vlan 2 port-priority 112 //16 的倍数

五、 STP 的收敛

交换网络从不稳定状态进入稳定状态的过程与时间。接口从不接收转发数据到接收转发数据的过程。

接口状态：

Blocking：不接收转发用户数据

Listening：能接收 BPDU 但不转发用户数据

Learning：接收用户数据但不转发用户数据，能接收转发 BPDU

Forwarding：接收转发用户数据

Disable：不接收转发任何数据

时间参数：

Hello Time：

Forwarding Time：

Max Age：

对于传统的 STP 收敛：

直接链路故障 30S

间接链路故障 50S

六、 STP 的高级特性

加快 STP 收敛

调整 STP 的时间参数：

Spanning-tree vlan # {hello time | max age | forwarding-delay} ~

采用思科的专有特性：

Portfast：用来接 PC 终端的接口，使之快速转发

Uplink-fast：

Backbone-fast：检测非直连链路故障

协议的升级：

STP------RSTP-----MSTP

STP 的稳定与安全

BPDU-Guard：应用于 Portfast 接口，如果在一个接口启用后，收到 BPDU 则自动进入 Errdisable 状态！

Root-Guard：根保护，配置该特性的端口不能成为根端口。收到更好的 BPDU 也不理睬！

BPDU-Filter：过滤 BPDU，此端口将不发送任何的 BPDU 并忽略所有接收到的 BPDU！

Loop-Guard：防止一个阻断的端口由于链路不正常（不能双向通信等）接不到 BPDU 后变成转发，配了此项后，即使接不到 BPDU 也是阻断的 loop-inconsistent blocking state（启用 loop guard 时自动关闭 root guard）

UDLD：单向链路检测

【返回目录】

Lesson 9　HSRP

一、　HSRP 的基本概念

思科私有的一种热备份路由器冗余协议；一种解决主备网关备份冗余的协议。

HSRP 选举：选出主网关，备份网关

虚拟 IP：与真实网关在同一网段但不能是相同的 IP 地址；只与主网关形成映射关系。

目标 IP：224.0.0.2；被 UDP 封装，端口号 1985

源 IP：自己的接口 IP

目标 Mac：00-00-0c-07-ac-xx　　//xx 代表所属组号

源 Mac：自己的接口 Mac 地址

参考 RFC：rfc2281

二、 HSRP 的组件

- 主网关（活动路由器）：

  HSRP 选举具有最高的优先级的路由器，主要用来接收发送终端 PC 去外网的数据

- 备份网关：

  HSRP 选举具有次高优先级的路由器，主要用来监控主网关，不能接收 PC 的数据

- 虚拟 IP（PC 使用的网关）：

  通过 HSRP 虚拟出来的地址，作为终端 PC 的网关，与主网关形成映射关系

HSRP 报文结构

版本	Code	状态	Hello
Hold	优先级	组	保留
鉴权			
虚拟 IP			

版本：

Code：

状态：主网关发送的就为活动状态，备份网关发送的为备份状态

Hello：默认为

Hold：一般为 3 倍的 Hello 时间

优先级：取值 0~255，默认 100，取值 0 则代表不参加选举

组：每个组对应一条转发路径

保留：

鉴权：配置的口令

虚拟 IP：自带放在 Hello 报文里，与其他路由器的报文比较。

比较顺序：先比优先级，如果相同则比发送报文的接口 IP 地址。

三、 HSRP 的配置

接口模式下：

Int e0

Ip add 192.168.0.252 255.255.255.0

Standby 1 priority 200

Standby 1 ip 192.168.0.254

上游接口跟踪：

Standby 1 track s0 110

Standby 1 preempt

【返回目录】

Lesson 10 WAN

一、 WAN 链路的基本类型

专线技术

由 ISP 为企业远程节点之间互联提供点-点的专有连接

特性：

- ✧ 逻辑连接持久有效
- ✧ 安全性高
- ✧ 支持多种传输速率 64Kbps---40Gbps

- ✧ 支持多种传输介质和接口标准
- ✧ 配置与维护简单，运营稳定
- ✧ 运营成本较高

专线典型代表：

DDN 专线：数字数据网，早期的一张业务网~

能提供的带宽：64X KBps　1≤X≤32

从 ISP 的 DDN 业务网中为企业远程节点间互联提供专线连接

E1 专线：从 ISP 的 SDH/PDH 传输网中为企业远程节点间互联提供标准速率为 2.048Mbps 的专线技术。也是中小型企业用的最多最流行的专线连接。

SDH：“同步数字系列”（Synchronous Digital Hierarchy）

PDH：“准同步数字系列”（Plesiochronous Digital Hierarchy）

E3 专线：从 ISP 中的 SDH/PDH 传输网中为企业远程节点间互联提供标准速率为 34Mbps 的专线技术。

POS：从 ISP 中的 SDH/PDH 传输网中为企业远程节点间互联提供标高速的专线技术

速率\标准	中国	美国
155Mbps	STM-1	OC-3
622Mbps	STM-4	OC-12
2.5Gbps	STM-16	OC-48
10Gbps	STM-64	OC-192

电路交换技术：

由 ISP 为企业远程节点间互联提供临时的逻辑连接

特性：

- ✧ 速率较低
- ✧ 实现技术比较复杂
- ✧ 文档性差
- ✧ 组网成本低

典型代表：

ISDN：

BRI	2B+D	B 代表用户数据 B=64K	D 代表控制信息 D=16K
PRI	30B+D	B=64K	D=64K

带外管理机制：控制管理信息和用户数据分开

带内管理机制：控制管理信息和用户数据在一起

PSTN： Public Switched Telephone Network

分组交换技术：

由 ISP 为企业多个远程节点之间互联提供的一种共享物理链路的 WAN 技术。

网络设备根据分组中的地址来决定分组的转发。

典型代表：FR、ATM、X.25

特性：共享式、适合分支节点多的网络环境

PPPoE+IPSec/VPN

特性：低成本、安全性高、灵活性高

二、 广域网链路的连接

WAN 链路的基本功能组件

- DTE：Data Terminal Equipment；数据终端设备

  为广域网链路提供数据发送与接收的设备

  典型代表：路由器、PC 终端、NAS

- DCE：Data Communication Equipment；数据通信设备

  为同步串行接口提供时钟、数据格式转换功能

  典型代表：调制解调器、基带猫、光端机、光纤收发器、协议转发器

- CPE：客户前端设备

用于用户机房的设备，包括 DTE、DCE 设备

- 分界线：

  用户责任区与 ISP 责任区的分界

- 本地回环链路：最后一英里

  从电信 ISP 的 Co Switch 到用户机房

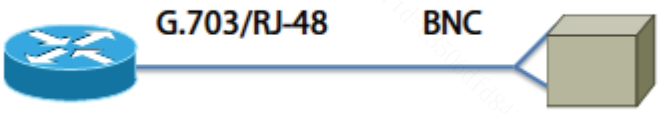
- Co Switch：中心局交换机

  提供本地回环链路的交换机

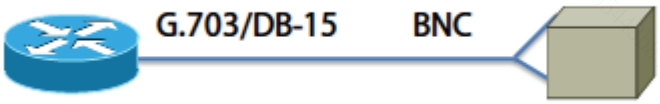
三、 WAN 链路的具体连接

E1 的四种连接

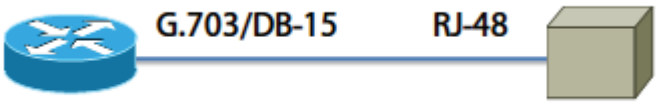
✧ 思科主流：RJ-48 转 BNC 连接线缆、光端机，光纤接口，FC 型



✧ 国内主流：75 欧姆非平衡同轴电缆、光端机，FC 光纤连接器



✧ 其他 1：120 欧姆平衡双绞线缆、光端机



✧ 其他 2：V.35 线缆、协转、光端机

RJ-45 和 RJ-48 的区别：线序不同

E3 的连接：

POS 的连接：

ADSL 共享上网破解：

PC 双网卡做代理

用路由器拨号

四、 WAN 链路的封装

HDLC：

高级数据链路控制协议

是数据链路层最基础的协议

主要用于点-点的串行链路中，也支持点-多点

版本：ISO-HDLC、CISCO-HDLC

ISO-HDLC

标志	地址	控制	Data	标志

标志：开始或结束，用来区分帧

地址：11111111

控制：

CISCO-HDLC

标志	地址	控制	Proprietary	Data	标志

Proprietary：标识多种上层协议

Keepalive 报文：每 10 秒发送一次，用来检测对端的状态。

PPP：Point-2-Point

以 HDLC 为基础，支持多种上层协议的一种开放式标准协议，支持多种物理接口标准

支持多种功能特性：

- ✧ IP 地址自动分配
- ✧ 支持身份认证
- ✧ 支持多链路绑定
- ✧ 支持数据压缩
- ✧ 支持回拨功能

PPP 的组件结构

标志	地址	控制	协议域	信息域	校验	标志
1B	1B	1B	2B	1500B	2B	1B

NCP：网络控制协议

提供多网络协议的支持

负责协商基于逻辑连接的上层分组信息的数据结构

可以相互把自己的接口 IP 带出去

LCP：链路控制协议

负责建立、测试、维护基于物理层的逻辑连接

PPP、FR 能检测到本地环路

HDLC 不能检测本地环路，适合打环测试~

PPP 的身份认证

PAP：密码验证协议；验证简单；安全性低

特性：明文认证、认证频率由被认证方控制、不具备再次认证机制

CHAP：竞争握手验证协议；验证复杂；安全性高

特性：密文认证、认证频率有认证方控制、具备再次认证机制

PPP 多链路绑定：

将路由器之间多条 PPP 链路逻辑绑定形成一条高带宽、高可靠性的逻辑 PPP 链路！

Frame-Relay：

FR 的基本功能特性：

是分组交换技术的典型代表

是面向连接的数据链路层技术

有 ISP 为客户分配 PVC 来实现远程节点之间点-点的逻辑连接

一条物理链路上可以存在多条 PVC

FR 的相关术语：

AR/CIR：

AR：本地接入速率

CIR：承诺平均速率（与 PVC 有关）

VC：虚电路

由 ISP 为 FR 通信双方提供的点-多点逻辑连接！

PVC：永久虚电路

类似专线

SVC：交换式虚电路

类似拨号，临时建立的虚电路

DLCI：数据链路控制标识符

用来标识 PVC；由 FR 交换机产生并分配给 FR 客户端。

DLCI 具有本地意义，一条完整的 PVC 至少由一对 DLCI 映射而成

DLCI 也是 FR 帧中的二层地址

LMI：本地管理接口

实际上是工作在 FR 客户端与 FR 交换机之间的一种协议。主要负责 DLCI(PVC)的获取以及 PVC 的状态感知。

PVC 状态：

- ✧ Active
- ✧ Inactive
- ✧ Deleted

IARP：逆向 ARP

动态实现本地 DLCI 与远端 IP 地址之间的映射！

FR 的配置：

FR 的拓扑结构：

NBMA：非广播型多路访问

子接口：

点-点：一个子接口对应一条 PVC

点-多点：一个子接口对应多条 PVC

FR 的配置：

FR_Switch：

(config)#frame-relay switching

Int s0

No sh

Encapsulation frame-relay {ietf | cisco}

Frame-relay lmi-type {cisco | ansi}

Frame-relay intf-type dce

Clock rate 64000

Frame-relay route 102 int s1 201

Frame-relay route 103 int s2 301

FR_NBMA_Client：

Int s0

No sh

Encapsulation frame-relay {ietf | cisco}

Frame-relay lmi-type {ansi | cisco}

Ip add 192.168.1.1 255.255.255.0

FR_P2PSubInt_Client：

Int s0

No sh

Encapsulation frame-relay {ietf | cisco}

Frame-relay lmi-type {ansi | cisco}

Int s0.1 point-to-point

Frame-relay interface-dlci 102

Ip add 192.168.1.1 255.255.255.0

Int s0.2 point-to-point

Frame-relay interface-dlci 103

Ip add 192.168.2.1 255.255.255.0

【返回目录】

Lesson 11 E1

E1 的帧结构：

PCM 机制；脉冲编码；数模转换

抽样：8000 次/S

量化：8000 次脉冲/S

编码：8bit/脉冲；64000bits/S

复用技术：

时分复用：数字信号

T1：24 路数字信号（北美、日本）

E1：32 路数字信号（欧洲、中国）

频分复用：广播、电视、无线

波分复用：DWM、光网络

一个标准的 E1 帧：256bit

一路 E1 的时隙：32 个

根据 E1 帧中所有时隙所承载的数据类型的不同以及数据到达的目的地的不同，分为：

成帧：time slots 0 承载同步信息，1~31 可以随机绑定在一起用来承载到达同一目的地或不同目的地的数据。

非成帧：所有 32 路时隙全部用来承载到达同一目的地的用户数据。

成复帧：ts0 承载同步信息，ts16 承载控制信息，ts1~15　ts17~32 承载用户数据。

非信道化 E1：非成帧

信道化 E1：成帧

成复帧：应用于拨号网络，拨号信息可以通过 ts16 传输。

E1 的配置：

配置步骤：

- 配置 E1 控制器
- 定义帧的类型与线路编码（可选）
- 定义时隙逻辑逻辑绑定组
- 配置逻辑绑定组虚接口

配置命令：

- controller e1 0/0
- framing {crc4 | no-crc4}
- line code {hdb3 | ami}
- channel-group 0 timeslots 1-2
- channel-group 1 timeslots 3-10
- interface s0/0:0

  Encapsulation ppp

  Ip add 192.168.1.2 255.255.255.0
- interface s0/0:1

  Encapsulation ppp

Ip add 192.168.3.2 255.255.255.0

- controller e1 0/0
- channel-group 0 ts1-31
- int s0/0:0
- encapsulation ppp
- ip add 192.168.3.2 255.255.255.0

- channel-group 0 unframe

【返回目录】

Lesson 12 路由器

一、 路由器的使用场景

路由器是具有路由功能的网络设备，工作在网络层，基于路由表转发 IP 数据包

应用场景：

LAN：隔绝二层广播、做 Vlan 间路由

WAN： 提供不同子网间的路由

提供 WAN 接口

提供丰富的业务特性

隔离二层环境及广播包

二、 路由器的工作原理

网络设备帮助用户正确转发数据包，转发的依据是路由表

路由表由若干条目组成：

代码：标识路由条目的来源

目标网络：

下一跳：往往是直连接口的 IP，到目标网络应该把数据交给谁

本地出口：

到一个目标可能有多条路径，在路由表中的是最佳的！

选择最佳路径的依据是 AD & Metric

先比较 AD，如果相同则再比 Metric，值越小越好！

只有网络号和子网掩码都相同的才具有比较的条件！

AD 是衡量路由来源的可信度标准的，可以人工修改。

Metric 是特定的路由协议衡量路径优劣的重要参数。

基于目标 IP 查找路由表

用目标 IP 和子网掩码进行与运算

路由条目匹配成功-----转发

路由条目匹配不成功---丢弃并 ICMP 报错

找到出口后，并针对出口解决二层封装

如果有多个相同的子网掩码，则按照最长匹配原则进行计算，细化的优先

三、 创建路由表

直连网络通过接口感知并自动进入路由表

非直连网络无法通过接口感知，必须创建（手动、自动）

静态路由：ip route 目标网络 子网掩码 下一跳/本地出口 [AD]

动态路由：配置路由协议，略

Cisco 路由器路由协议的默认管理距离：

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
External Enhanced IGRP	170
Internal BGP	200
Unknown;Discard Route	255

【返回目录】

Lesson 13 静态路由

保证源到目标沿路径每个路由器都有到达目标的路由（双向）

路由汇总：使用一条较为粗略的汇总路由代替一些细化路由，通过改变目标网络的网络号和子网掩码来实现。

使用条件：有共同的网络号、有共同的出口。

优点：减少路由条目，提高查找速度

缺点：可能导致次佳路径，甚至出现循环

地址规划：起始是偶数、结束是奇数、最好分配 2^n 个子网并且连续分配

缺省路由：0.0.0.0 0.0.0.0

浮动静态路由：

维持路由的条件：

下一跳必须可达或本地出口有用！

主链路 down 掉，主路由消失，备份路由自动起来！

关于同一个目标网络号相同，子网掩码相同，有多条路径则比较 AD 和 Metric，选择最佳路径。

负载均衡：

单个设备单个链路无法承载流量压力。

负载均衡：　二层：以太网通道、PPP MultiLink

三层：路由

四层：

关于同一个目标有多条路径进入路由表，就可能利用这些路径来转发数据。

负载均衡实现方法：

路由器的转发方式决定了负载均衡的方法：按包、按目标、按源+目标

进程交换：按包负载

快速交换：按目标负载

CEF：按目标负载

替代路由：

利用最长匹配原则，做细化路由

静态路由缺点：

无法感知拓扑变化

拓扑结构简单，不需要感知拓扑变化---静态路由

拓扑结构复杂，需要感知拓扑变化------动态路由

【返回目录】

Lesson 14 RIP

一、 简介

Routing Information Protocol

路由信息协议：辅助路由器建立路由表，以便转发数据信息

辅助性协议：RIP OSPF EIGRP IS-IS BGP

版本：

Version 1：应用于 ipv4

Version 2：应用于 ipv4，是 version1 的升级版本，支持 CIDR，VLSM

Version ng：应用于 Ipv6

应用场景：一般用于早期中小型企业网

算法：

Distance Vector：RIP EIGRP BGP

Link State：OSPF IS-IS

二、 工作流程

Rip 是基于特定的软硬件实现

协议包：

Request：请求包，向邻居通告自己的身份，请求特定的路由信息

Response：应答包，向邻居通告路由信息

封装：Rip 被 UDP 封装，端口号 520，目标 IP：255.255.255.255，源 IP：接口 IP

工作流程：

启动 Rip 进程，从属于该进程的所有活动接口向外发送请求包

每隔 30S 定期向外发送应答包，通告路由信息（邻居维持机制，可靠性机制）

收到应答包后，安装路由信息

从应答包中获得目标网络，AD=120

使用路由器个数作为 Metric

直连网络为 0Hops，通告之前+1Hops，进来时不添加，使用源 IP 作为下一跳

安装成功后，启动失效计时器，默认 60S

在 60S 内仍没有收到则清除

为加快收敛使用触发更新

为防止循环，使用水平分隔和无穷大计数

水平分隔：从一个接口收到的路由不能再从这个接口通告出去

三、 基本配置

启动 Rip 进程：

Router rip

Network a.b.c.d

四、 RIP-V2

Router rip

Version 2

Network a.b.c.d

V2 的改进：

带子网掩码，支持 VLSM

目标 IP 使用组播地址：224.0.0.9

支持路由认证

支持路由标记和下一跳属性

为了兼容 V1，在主网边界自动汇总，需要手工关闭

Router rip

Version 2

No auto-summary

Network a.b.c.d

Offset-list [acl] [in/out] [0~16] [interface]

先检查从某个接口接收或发送的 RIP 通告是否存在和 ACL 指定的地址相匹配，如果匹配则就把匹配的路由条目的 Metric/Hops 加大或减小

被动接口：该接口只作用于特定的协议

在 Rip 中的行为：只接收路由更新，不发送路由更新

应用场景：不需要发送协议的接口

*一些小厂商的被动接口做的不好！慎用！

单播更新：通过单播的形式发送路由信息

Router rip

Neighbor *ip

GRE 携带路由

广播、组播简单，但在特殊链路上封装有问题

FR ATM VPN

路由重发布与缺省路由

两种路由协议之间不会自动通告路由信息，必须通过重发布才能相互通告！

Router rip

Redistribute static metric 1

Redistribute connected metric 1

路由认证：

路由协议缺省不带认证，为了保证路由协议自身的安全，可以在接口下使用路由认证！

Key chain bluefoxkey

Key 1

Key-string bluefox

Ip rip authentication key chain bluefoxkey

Ip rip authentication mode md5/text

应用场景：连接不安全的区域的路由器

接口汇总：

Int s0/0

Ip summary-address rip ip_address mask

RIP 协议包的数据结构：

Command	Version	Routing domain
Address family		Route tag
Ip address		
Net mask		
Next hop		
metric		

【返回目录】

Lesson 15 OSPF

一、OSPF 简介

1. Open Shortest Path First。
2. 它是一种动态路由协议，国际标准，参考资料为 RFC2328。
3. Link-State，基于链路状态的一种协议。
4. 收敛快，带宽占用少，支持 VLSM & CIDR。
5. 三个版本：版本 1 在实验室；版本 2 是为 IPv4 服务；版本 3 为 IPv6 服务。
6. Link-State：链路状态；对网络的认识来自于始发路由器，具有全局拓扑，
   在邻居间可靠传输（洪泛）LSA。
7. Distance-Vector：距离矢量；对网络的认识来自于直连邻居。简单但不可避免循环。
8. 划分区域---减轻协议压力：通过区域限制 LSA 的不必要洪泛。

二、OSPF 的工作机制

1. 协议包类型：

HELLO：用来建立和维持邻居关系

DBD：用来检验路由器之间数据库并进行同步

LSR：链路状态请求，向邻居请求特定的 LSA

LSU：链路状态更新，携带 LSA 向邻居通告路由

LSAck：确认，对收到的 LSA 进行确认

2. 封装：

被 IP 直接封装，IP 协议号 89，源 IP 使用出口 IP

目标 IP ：224.0.0.5（ALL OSPF ROUTERS），

224.0.0.6（ALL OSPF DR & BDR ROUTERS）

3. 工作流程：

三个阶段：交换阶段；路由发现阶段；路由选择阶段。

(一)、交换阶段：

通过 Hello 形成正确的邻居，邻接关系

1) 启动 OSPF 进程，从所有属于该进程的活动接口向外发送 Hello 包
2) 对端路由器收到 Hello 包后检查其中的参数，决定能否形成邻居

检查的参数有：

- 区域号：相邻接口必须在同一个区域
- 认证：相邻接口的认证必须相同
- Hello 间隔、失效时间：相邻接口的 Hello 和失效时间必须一样
- 存根标志：相邻接口的存根标志必须一致

3) 如果参数匹配，则放入邻居表，标志为 Init 状态
4) 如果在邻居的 Hello 里看到自己的 RID，则标志为 two-ways 状态
5) Two-ways 状态标志着邻居形成，邻接关系如何形成受制于网络类型

Point-2-point：邻居中自动形成邻接关系

Multi-access：必须先在邻居中选举 DR 和 BDR，其他的为 DROther，再决定形成邻接关系

6) 定期发送 Hello 包，维持邻居关系，默认为 10S，失效时间 40S

（二）、路由发现阶段：

形成完全相同的 LSDB

1) 只有形成邻接关系才能进入路由发现阶段
2) 首先处于 Exchange_start 状态，通过选举主从路由器解决 DBD 可靠的问题，RID 高的成为主路由器，主路由器控制 DBD 的序号
3) 一旦选举出主从路由器，则进入 Exchange 状态，通过 DBD 向邻接描述自己的 LSDB 中的 LSA
4) 之后进入 Loading 状态，通过 LSR 向邻接请求，用 LSU 携带 LSA 用 LSAck 对收到的 LSA 进行确认。
5) 最后 LSDB 完全相同-----达到 Full 状态！

（三）、路由选择阶段

生成用户所需的路由表

1) 只有 LSDB 完全相同才会进入路由选择阶段
2) 每个路由器以 LSDB 中的 LSA 为原材料独立进行 SPF 运算
3) 然后针对特定的目标网络把沿途路径 Cost 相加，比较总和，总 Cost 最小的就是最佳路径
4) 拓扑发生变化，感知拓扑变化的 router 产生新的 LSA 洪泛到全网！收到新的 LSA 重新计算
5) LSA 年龄：3600S；每隔 1800S 始发路由器重新生成新的 LSA

4. OSPF 术语：

RID：在 OSPF 网络中唯一区分一台路由器，如果有 Loopback 接口并配有 IP 则使用最大的 IP 作为 RID，没有则选择最大的物理接口 IP。可以人为指定。

Neighbors：物理相连，相互可能交换 Hello 且参数相同的路由器。

Adjanceny：邻接，OSPF 路由器只有形成邻接关系后才能交换 LSA

LSA：链路状态通告，向邻居通告的拓扑信息

DR：指定路由器，在广播类型中为减少压力而产生的

BDR：备份指定路由器

Area：区域，若干个路由器的接口组成区域

Stub：存根，OSPF 中的一个特殊的区域

NSSA：不那么的存根，OSPF 中的一个特殊区域

Virtual-Link：虚连接，如果一个区域没有直接和 A0 相连，则须用虚连接。

Cost：OSPF 的 Metric 值计算的原材料

三、基本配置

1. 启动 OSPF 进程：

   Router ospf 23

2. 指定 RID：

   Router-id *.*.*.*

3. 把相关接口放入 OSPF 进程：

   Network a.b.c.d *.*.*.* area #

4. 所有配置完成后：clear ip ospf process

5. 验证配置

   Show ip route

   Show ip ospf

   Show ip ospf interface *

   Show ip ospf neighbors

   Show ip protocols

   Show ip ospf database

6. OSPF 认证

   ✧ 基于接口的明文认证：

   Ip ospf authentication

   Ip ospf authentication-key ~

   ✧ 基于接口的 MD5 认证：

   Ip ospf authentication message-digest

   Ip ospf message-digest 1~255 md5 ~

7. 发布 0/0

   Default-information originate metric # metric-type 1/2

四、不同接口类型上的 OSPF

（一）、专线上的 OSPF

协议：PPP、HDLC

类型：point-2-point

OSPF 邻居自动形成

OSPF 邻接自动形成

（二）、以太网上的 OSPF

协议：Ethernet

类型：broadcast

以太网自动封装广播与组播，邻居自动形成

邻居形成邻接，在 two-ways 之后要在邻居中选举 DR 和 BDR，再决定如何形成邻接！

为什么选举 DR、BDR？

因为以太网链路导致过多的邻居、邻接关系！n(n-1)/2！，过多的邻接关系会导致协议压力过大，所以在该链路上选举一个 LSDB 的同步中心，就是所谓的 DR，BDR 只作为 DR 的备份。默认选举时间 40S。

关系图：

	DR	BDR	DROther
DR	---	邻居、邻接	邻居、邻接
BDR	---	---	邻居、邻接
DROther	---	---	邻居

怎样选举 DR、BDR？

使用 Hello 包进行选举，比较接口优先级；

接口优先级默认为 1，取值范围【0~255】，0 表示不参与选举

取值越大越好，最大优先级的为 DR，次高的为 BDR

如果优先级相同，则比较 RID，最大的为 DR，次高的为 BDR

新加入的路由器必须服从之前的选举结果

选举是由网络类型所决定的

为了加快收敛，可以人为改变接口的网络类型，抑制选举

Int f0/0;　ip ospf network point-to-point

（三）、FR、ATM 上的 OSPF

协议：Frame-Relay、ATM

类型：NBMA（Non-broadcast Multicast Access）

封装可能会出现问题：

MA 网络会导致 DR、BDR 的选举

非全互联的 PVC，DR 选举有问题，需手工指定 DR

- ✧ 手工修改分部的接口优先级为 0

  Int s0/0; ip ospf priority 0

- ✧ 或者修改网络类型

  Ip ospf network point-to-multipoint

  Ip ospf network point-to-point

（四）、接口的带宽

OSPF 把到目标沿途所经过的出口 Cost 相加，选择总 Cost 最小的作为最佳路径。

参考带宽：100Mbps

Cost=参考带宽/出口带宽

修改参考带宽：

修改接口 Cost，控制出口

Int f0/0

Ip ospf cost 100

五、多区域 OSPF

1. 为什么要多区域？

每个（OSPF）路由器要求都有完全相同的 LSDB，这样导致 LSA 的洪泛造成设备、协议压力过大。

整个 OSPF 也在同一个动荡域中，每个小变化就带来风吹草动。

把一个大的 OSPF 网络划分成若干个小的相互独立的 OSPF 网络就叫区域。

不同的区域通过 AreaID 来区分。

每个区域是一个单独的动荡域，LSA 的洪泛在区域内不受阻碍，但通过区域的划分可以控制 LSA 的不必要洪泛。

2. 多区域的问题及解决方案

区域间的通讯由 A0（骨干区域）来完成

要求所有区域都和 A0 相连

每个区域把区域内拓扑通告给 A0，再由 A0 分发给其他区域

每个 OSPF 进程只能有一个 A0，保证其健壮性

3. 路由器的类型

区域和接口绑定

根据接口与区域的关系把路由器分类：

- ✧ 内部路由器：

  一个 Router 的所有接口都在同一区域内

  一个区域内所有内部 Router 的 LSDB 完全相同

- ✧ 区域边界路由器：

  Area Border Router（ABR）

  接口分属于两个或两个以上的区域，并且至少有一个接口属于 A0

  作用：控制区域内 LSA 的洪泛；区域间拓扑信息的可控洪泛

  ABR 针对每个区域单独维护 LSDB

- ✧ 骨干路由器：

  至少有一个接口属于 A0

- ✧ 自治系统边界路由器：

  Autonomous System Border Router（ASBR）

  通过重发布引入外界路由的路由器

  负责沟通 OSPF 网络与非 OSPF 网络之间的路由传递

4. LSA 的类型

为了控制 LSA，由不同的路由器产生不同的 LSA

(一) 区域内路由

目标网络在同一个区域内（“O”）

- ➢ **路由器 LSA（LSA1）**

每个 OSPF Router 都会针对自己所在的区域内生成一个 LSA1

用来描述接口状态，邻接关系，身份信息

LSA1 只能在区域内洪泛

➢ **网络类型 LSA（LSA2）**

由 DR 产生，描述所在的多路访问网络及所属的路由器

LSA1、LSA2 只在区域内洪泛，被 ABR 阻止

(二) 区域间路由

目标网络在另一个区域（“OIA”）

ABR 针对自己所在的区域产生描述其他区域的拓扑

➢ **网络汇总 LSA（LSA3）**

由 ABR 针对自己所在的区域产生描述其他区域的拓扑

缺省每个子网生成一个 LSA3

在 ABR 上针对 LSA3 做控制

以区域为单位分配地址块，方便路由汇总

Router ospf 23

Area 1 range 172.16.0.0 255.255.252.0

➢ **ASBR 汇总 LSA（LSA4）**

由 ABR 生成，向本区域描述其他区域 ASBR 的可达性

(三) 外部路由

目标网络在非 OSPF 进程内的、通过 ASBR 重发布引入的路由（“OE2”）

➢ **自治系统 LSA（LSA5）**

由 ASBR 通过重发布引入，缺省每个子网生成一个 LSA5

LSA5 在区域间洪泛，不能进入特殊区域

5. 路由汇总

划分区域的目的就是为了通过路由汇总压制动荡

ABR 针对 LSA3

(config-router)#area # range 子网 掩码

(config-router)#area # range 子网 掩码 【cost | not-advertise | ...】

Cost：改变默认的通告 Cost

Not-advertise：不发布汇总路由

(config-router)#area # filter-list # in/out

(config)#ip prefix-list bluefox seq 10 permit/deny 172.16.0.0/21 [ge/le value]

Ge：minimum prefix length to be matched

Le：maximum prefix length to be matched

Length < ge < le

ASBR 针对 LSA5

(config-router)#summary-address 子网 掩码

(config-router)#summary-address 子网 掩码 【cost | not-advertise | ...】

缺省生成 OE2

OE2：总 Cost=外部 Cost //如果外部 Cost 相等，则比较内部 Cost

OE1：总 Cost=外部 Cost+内部 Cost

6. 特殊区域

通过 ABR 抑制不必要的其他区域的协议压力

✧ 存根区域

不想接受其他区域的外部路由信息

LSA5 不再洪泛进入 Stub 区域；生成（0/0）LSA3

骨干区域不能配置 Stub 或其他特殊区域

虚链路不能穿越特殊区域

存根区域不能作重发布

在 Stub 区域内的接口都须配置

ABR(config-router)#area # stub

Other(config-router)#area # stub

✧ 完全存根区域

不想接收其他区域的外部路由和区域间路由

LSA5 和 LSA3 不再洪泛进入 Totally Stub 区域

相关配置：

ABR(config-router)#area # stub no-summary

Other(config-router)#area # stub

✧ NSSA；Not-so-stub-Area

既想阻止其他区域的 LSA5，本区域又想作重发布

LSA5 不再洪泛进入 Stub 区域

重发布的路由以 LSA7 的形式进入 NSSA 区域；（“ON2”）；再由 ABR 以 LSA5 通告出

去

在 Stub 区域内的接口都须配置

ABR(config-router)#area # nssa

Other(config-router)#area # nssa

✧ Totally NSSA

不想接收其他区域的外部路由和区域间路由

LSA5 和 LSA3 不再洪泛进入 Totally NSSA 区域

相关配置：

ABR(config-router)#area # nssa no-summary

Other(config-router)#area # nssa

特殊区域 LSA 分布图：

	1	2	3	4	5	7	0/0
Stub	有	有	有				3
Totally Stub	有	有					3
NSSA	有	有	有			有	7
Totally NSSA	有	有				有	3

六、OSPF 注意的问题

1. 怎样防止路由协议的安全

   配置认证

   使用重分布

   在不需要发送 OSPF 信息的地方使用被动接口

2. 邻居形成不了的原因

   外因：物理层；链路层；ACL；OSPF 配置等

   内因：区域号、存根标志、认证、Hello 间隔是否一致。

3. 如果长时间卡在 Exstart 或 Exchange 状态

   则应检查 MTU 是否抑制

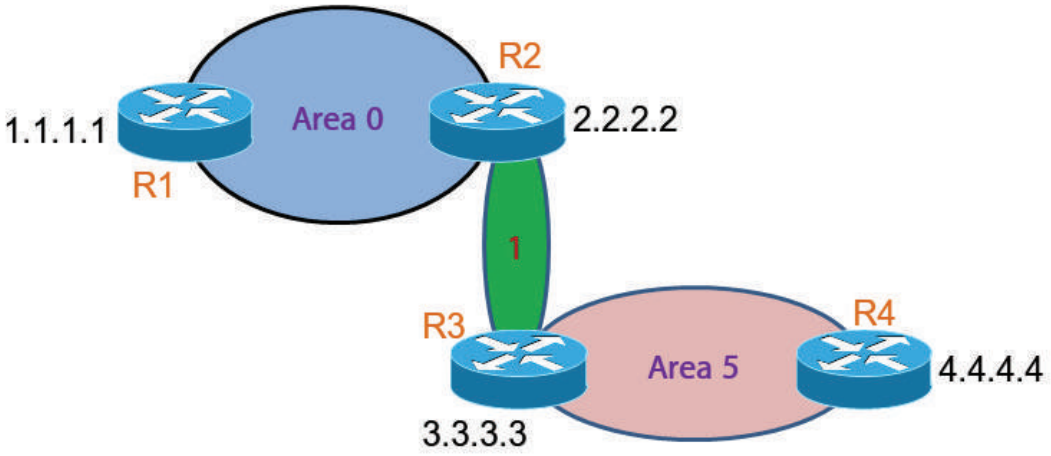
4. NSSA 区域存在的问题

   LSA7 重发布出去，在 ABR 上阻止并转换 LSA5 通告出去，同时 forwarding-address 置位并填上发布者的接口 IP！这样会导致下一跳不可达（因为接口 IP 可能不会被通告出去）

   解决方法：

   - ✧ LSA5 再汇总一次，使 forwarding-address 不置位。
   - ✧ Cisco：area # nssa translate type7 suppress-fa　//压制 fa 置位！

5. OSPF 区域不分离问题



OSPF Virtual-Link

只需在 R3、R2 上配置 Virtual-Link 就可解决

R3.(config-router)#area 1 virtual-link 2.2.2.2

R2.(config-router)#area 1 virtual-link 3.3.3.3

Area 1 作为传输区域

七、OSPF 在 FR 中的解决方法

1. PVC 全互连，且支持广播

   Ip ospf network broadcast

2. PVC 全互连，不支持广播

   配置单播：neighbor a.b.c.d priority ~

3. PVC 非全互连，支持广播

   导致 DR 选举混乱，需手工指定 DR，让其他的路由器不参与选举，把非 DR 的优先级改为 0

   Ip ospf priority 0

4. PVC 非全互连，支持广播

   划分子接口，使路由器相互形成点-点链路，两端都要改

   Int s1/0.2

   Ip ospf network point-to-point

   Frame-relay interface-dlci ~

5. PVC 非全互连，支持广播

   配置成非广播

   Ip ospf network non-broadcast

   Neighbor a.b.c.d

6. PVC 非全互连，支持广播

   配置成点-多点且指定邻居

   Ip ospf network point-to-multipoint

   Neighbor a.b.c.d

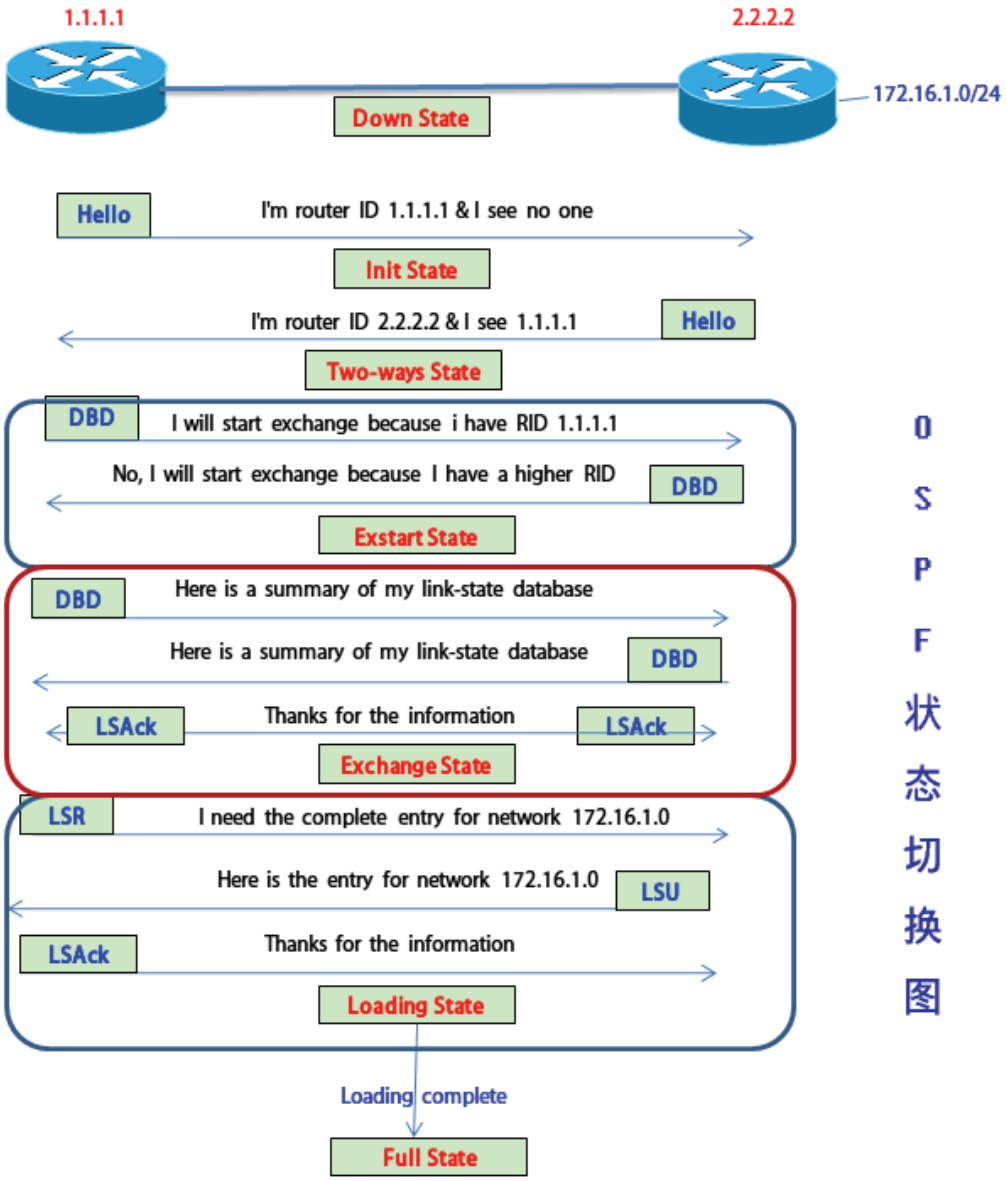
7. PVC 非全互连，不支持广播

   配置成点-多点非广播

   Ip ospf network point-to-point non-broadcast

   Neighbor a.b.c.d

八、OSPF 状态切换图



【返回目录】

Lesson 16 EIGRP

一、 EIGRP 功能简介

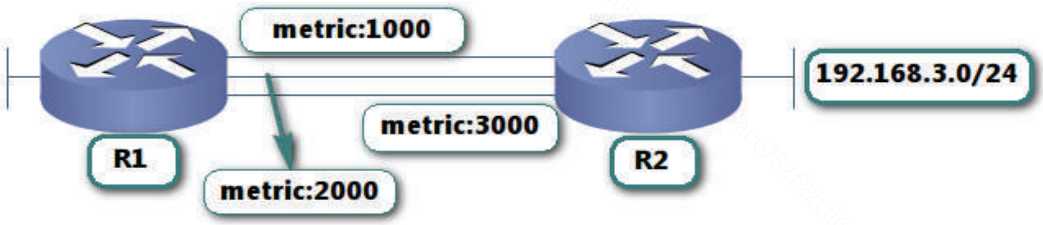
Enhanced Interior Gateway Routing Protocol

Cisco 私有协议

（一）EIGRP 的优点：

1. 收敛迅速
2. 无环路的无类路由
3. 增量型路由更新
4. 支持等价与非等价的负载均衡
5. 支持 VLSM 和 CIDR
6. 支持多种网络层协议，如 IP; IPX; AppleTalk

（二）相关术语介绍：



1. Feasible Distance；可行距离

   到达每个目标网络的最小 Metric 将作为那个目标网络的 FD。

2. Feasiable Condition；可行条件

   邻居宣告到达目标网络的距离小于本地路由器到达目标网络的 FD。

3. Feasible Successor；可行后继器

如果一个邻居宣告到达目标网络的距离满足 FC，那么这个邻居就成为 FS。

4. Advertise Distance；通告距离

邻居通告自己到达目标网络的最小 Metric。

5. Successor；后继器

直接连接的一个邻居路由器，通过它到达目标网络具有最短的路由。

二、 EIGRP 的工作机制

（一）协议包的类型：

1. Hello 包：用来发现和恢复邻居。
2. Ack 包：是不包含数据的 Hello 包，单播
3. Update 包：传播路由更新，不定期、通过可靠的方式传送，比较灵活，当一台路由器需要更新时就单播发送，当多台路由器需要更新时就采用组播。
4. Query 包：当拓扑发生变化时就主动向邻居查找。
5. Reply 包：收到查询后给予应答。

Hello 包的参数：K1 K2 K3 K4 K5 AS

Metric 值计算的参考参数：带宽、延迟、负载、可靠性、最大传输单元

这些参数必须匹配才能形成邻居

（二）封装

EIGRP 被 IP 封装，协议号为 88；目标 IP：224.0.0.10

（三）工作流程

1. 启动 EIGRP 进程，从属于该进程的接口向外发 Hello 包，以便建立邻居关系。
2. 收到 Hello 包后，检查其中的参数，如果匹配则形成邻居关系。
3. 只有形成邻居关系后才会向邻居发送 Update 包通告路由，收到 Update 包使用 Ack

包进行确认。

4. 把 Update 包里面的信息放入拓扑表中，经过路由计算，选出最佳路径的路由放入路由表中，并向邻居通告，选择备份路境以便加快收敛

5. 定期发送 Hello，维持邻居关系

默认的时间参数

	Hello Time	Hold Time
NBMA （>T11.544）	60s	180s
OTHER（>T11.544）	5s	15s

默认的 Metric 值的计算

Metric = 【10^7/最小带宽+总延时】* 256

带宽：到目标网络所经的出口中最小带宽值

延迟：到目标网络沿途的总和

三、EIGRP 的基本配置

1. 启动 EIGRP

(config)#router eigrp {AS}

2. 把相关接口放入进程

(config-router)#network {*network-number*} *[wildcards]*

IOS-12.0(4)T 以后引入通配符

3. 关闭自动汇总

(config-router)#no auto-summary

4. 手工精确汇总

(config-if)#ip summary-address eigrp # *ip-address mask [AD]*

5. 重发布其他路由协议

(config-router)#redistribute * metric #

6. 开启不等值负载

(config-router)#variance *

7. 认证

(config)#Key chain bluefoxx ; key 1 ; key-string cisco ;

(Config-if)#ip authentication mode eigrp 23 md5

(Config-if)# ip authentication key-chain eigrp 23 bluefoxx

8. 被动接口

(config-router)#passive-interface #

不发送 EIGRP 的的相关信息

9. 验证配置

Show/debug ip route

Show/debug ip protocols

Show/debug ip eigrp topology

Show/debug ip eigrp neighbors

【返回目录】

Lesson 17 IS-IS

一、 简介：

1. Intermediate System To Intermediate System

   作为一种路由协议就是帮助用户生成所需要的路由表。Is-is 是一种链路状态路由协议，被定义在 RFC1195。

2. 与 OSPF 的区别：

   都是链路状态协议，都使用 SPF 算法。

   ISIS 的扩展性比 OSPF 强，适用大型 ISP 网络；而 OSPF 简单，适用中大型网络。

   都有区域的概念，但 OSPF 必须使用区域获得性能；ISIS 可以只有一个区域。

   OSPF 路由协议中 LSA 的数量较多；而 ISIS 每个路由器在区域内只发一份 LSP。

   OSPF 只支持 IP 路由，而 ISIS 即支持 IP 路由又支持 OSI-CLNP 路由

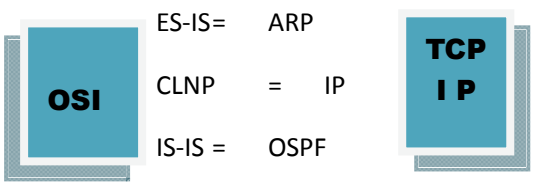
3. 常见术语：

   ES：（End System）就是指没有路由能力的网络节点。类似与 TCP/IP 中的主机。

   IS：（Intermediate System）指有数据包转发的网络节点，即路由器。

   CLNP：（Connectionless Network Protocol）无连接网络协议，类似 TCP/IP 中的 IP 协议。

   Level：ISIS 缺省属于 level-1 和 level-2



   NSAP：（Network Service Access Point）网络服务访问点

   NET：（Network Entity Titles）网络实体名称。在 IP 环境一般是 00

System ID：通常由 Mac 地址构成或由 IP 地址转换而成

Area ID：通常在全网内唯一指定

Net 86.0731.2020.1002.1030.00

86.0731　　#区域号

2020.1002.1030　　#System-ID

00　　#NET

二、 工作原理：

1. 协议包的种类：

Hello：建立并维持同层邻居

SNP：（Sequence Number Protocol）辅助同层邻居之间 LSDB 的同步

LSP：（Link State Protocol）向同层邻居通告拓扑

Level-1 只能在同一个区域内形成邻居

Level-2 形成邻居不受区域的影响

2. 协议包的封装：

目标 Mac	源 Mac	长度	DSAP	SSAP	Control	ISIS-Data

3. 工作流程：

- ✧ 启动 ISIS 进程，从属于该进程的活动接口向外发送 Hello 包。
- ✧ 收到 Hello 包后检查其中的参数，如果匹配，则放入邻居表。
- ✧ 通过发送 CSNP 描述各自的 LSDB；通过 PSNP 向邻居请求特定的 LSP 并解决可靠性，SNP 辅助 LSP 的可靠传输。
- ✧ 最终通过洪泛 LSP，同一个区域内所有 Level-1 的 LSDB 完全相同。
- ✧ 每个 ISIS 路由器以 LSDB 中的 L1-LSP 为材料独自进行 SPF 计算生成区域内的路

由。

✧ 区域间通信借助于区域边界的 Level-1-2 及 Level-2 组成的骨干区域。

三、 简单配置

Config#router isis [tag]//启动 ISIS 路由进程

Net 49.0731.1985.0523.1314.00 //为路由进程配置 NET 地址

Is-type {level-1 | level-1-2 | level-2-only } //配置路由器的角色

Config-if#ip router isis [tag]//在相应的接口下启用 ISIS 路由

Config-if# Isis metric ~ //指定改接口的某层 Metric 值

Passive-interface ~

Config-router#No hello-padding //确保 MTU 一致的话可以关闭 Hello 填充

Config-router#Metric-style wide //修改 Metric 为宽度量

Show ip route //查看该路由器学到的最佳路由表

Show isis route //查看 ISIS 路由协议学到的路由表

Show isis database //查看 ISIS 拓扑数据库的内容

Show ip protocol //查看该路由器运行了哪些具体的路由协议

Show isis neighbors//查看 ISIS 路由邻居的情况

Show clns interface * //查看运行 ISIS 路由的接口信息

无法形成邻居或邻接的原因？

如果没有明显的配置错误或互操作错误则可能是软件或硬件的故障

✧ 检查接口物理层、数据链路层

✧ 检查是否在接口上启动了相应的 IS-IS 进程

✧ 检查是否错误地配置了被动接口

✧ 检查是否有不匹配的 Level 与 Area 的关系

- 检查是否有不匹配的子网
- 检查是否存在相同的 System-ID
- 检查是否存在 MTU 不一致的问题
- 检查认证是否一致
- 检查是否有损坏的 Hello 数据包

以太网上的 IS-IS：

- OSPF 为减轻协议开销，选举 DR、BDR
- 而 IS-IS 为减轻协议开销，选举 DIS，而没有 BDIS
- DIS 作为链路的 LSDB 的同步中心
- DIS 允许其他路由器形成邻居、邻接
- DIS 定期发送 CSNP；描述自己的 LSDB
- DIS 以 1/3 的 hello 间隔发送 Hello 包
- DIS 的选举是抢占式的，选举时比较优先级，如果优先级相同则比较 System-ID

修改网络类型：isis network point-to-point

四、 IS-IS 多区域：

为什么要多区域？

- 减轻协议压力，压制动荡
- OSPF 通过引入 A0 骨干区域解决区域间循环
- IS-IS 通过所有 Level-1-2 和 Level-2 组成骨干区域
- 骨干区域必须连续
- 区域通过 NET 地址决定，一个设备一个区域
- 区域的边界在链路上
- 区域只影响 Level-1 的邻居关系的形成

- ✧ 一个设备缺省属于 Level-1-2
- ✧ 连接其他区域的 Level-1-2 自动生成 L1-LSP 把 ATT 置位
- ✧ 内部路由器根据此 ATT 置位生成 0/0 指向 Level-1-2
- ✧ 只有 Level-2 设备才能做重发布！
- ✧ Cisco 允许 Level-1 设备做重发布！

修改特定的接口所属的 Level

Int f0/0

Isis circuit-type level-*

重发布（缺省重发布到 Level-2）

Router isis [tag]

Redistribute connect ip* level-1 lsp

LSP OL：LSP Over Load

解决内存不足的问题（监视自己的内存）

如果发现内存不足会把 Metric 放大！

用来等待 BGP：

Router isis [tag]

Set-overload-bit on-startup wait-for-BGP

路由泄露：

Router isis [tag]

Redistribute isis [tag] ip* into level-1 destribute-list #(acl)

路由汇总：

Summary-address 子网号 子网掩码 level-2(默认)/level-1/level-1-2

路由认证：

Config-if#isis password ~~~

Config-if#isis authentication mode md5/text

修改 Hello 间隔：

Isis hello-interval …

【返回目录】

Lesson 18 BGP

一、 BGP 简介：

1. **BGP：** Border Gateway Protocol
2. **Version：** 1/2 4/4+ ；目前使用的为 4+
3. **AS：** Autonomous System；在同一个组织管理下使用相同策略的设备的集合。

   公有 AS：1~64511 私有 AS：64512~65535
4. **为什么使用 BGP？**

   需要承载大量的路由；它的策略能力非常强大；对新特性（MPLS VPN）支持良好。
5. **IGP 与 BGP 的区别：**

   IGP 收敛快而 BGP 收敛慢；资源消耗也大。IGP 为 BGP 提供 Peer 和 Next-hop 的可达性。BGP 又分为 eBGP 和 iBGP。

二、 BGP 工作原理：

1. **协议包：**

   - ✧ **OPEN：** 携带参数建立 Peer
   - ✧ **Keepalive：**（默认 60s）定期发送并维持 Peer
   - ✧ **Update：** 向 Peer 通告 NLRI（路由）
   - ✧ **Notification：** 发送详细的出错信息并拆除 BGP 的连接
   - ✧ **Route-refresh：** 在做了 BGP 策略以后，可以向 Peer 重新请求或发送 NLRI 以便完成路由决策（clear ip bgp * soft in/out）

2. **封装：**

   - ✧ BGP 协议包被 TCP 封装；
   - ✧ 目标端口 179；
   - ✧ 源 IP 缺省为出口 IP；
   - ✧ 目标 IP 为 Peer 的 IP。

3. **工作原理：**

   BGP 是 TCP 之上的一种应用，在 BGP Peer 建立之前必须完成 TCP 的三次握手；

   BGP 没有建立成功的因素：

   IP 因素：IGP 有没有解决目标的可达性

   TCP 因素：端口号有没有放通

   设备因素：是否具有运行 BGP 的资源

4. **工作状态：**

   启动进程>>>>>资源预留>>>>>TCP 连接>>>>>建立 BGP Peer>>>>>通告维持路由

   - ✧ **Idle：** 标志正在启动 BGP 进程 和准备相关资源
   - ✧ **Connect：** 标志正在进行 TCP 连接
   - ✧ **Active：** 标志 TCP 连接失败；重新尝试新的连接
   - ✧ **Open sent：** 标志 TCP 连接成功；发送 Open 报文建立 BGP Peer
   - ✧ **Open confirm：** 标志 Open 参数协商成功；发送 Keepalive 报文维持 BGP Peer
   - ✧ **Estabilised：** 收到 Keepalive 后就可以发送 Update 报文通告路由了

三、 BGP 的基本配置：

1. 建立 BGP Peer：

eBGP：router bgp 64512

neighbor 10.0.0.2 remote-as 64513

router bgp 64512

neighbor 2.2.2.2 remote-as 64513

neighbor 2.2.2.2 update-source loopback 0

neighbor 2.2.2.2 ebgp-multihop 2 //因为 eBGP 的跳数默认为 1

iBGP：router bgp 64512

neighbor 10.0.0.6 remote-as 64512

neighbor 10.0.0.6 next-hop-self //解决下一跳的可达性

router bgp 64512

neighbor 2.2.2.2 remote-as 64512

neighbor 2.2.2.2 update-source loopback 0

neighbor 2.2.2.2 next-hop-self

为什么使用 Loopback 做为 Peer 的地址？

- ✧ 因为考虑到链路可能不止一条
- ✧ 可以保证 BGP Peer 的稳定
- ✧ 和新业务的融合

2. 发现路由：

IGP 发现路由，而 BGP 通过重发布获取路由。BGP 重发布的路由必须和 IGP（路由表）的路由一致。

- **静态获取：**通过 Network 命令

  Network 子网号 mask 子网掩码 [可选参数]

  Network 语句最大支持 200 条；起源属性为 i

- **动态获取：**通过 Redistribut 命令

  Redistribute *protocol* [可选参数]

3. 通告路由：

eBGP 缺省使用 Peer 作为下一跳

iBGP 缺省不改变下一跳；必须由管理员解决下一跳的可达性

D-V 算法的循环避免：

- 水平分割；
- eBGP 使用 AS-Path 属性防止循环；
- iBGP 为防止循环属性不把从 iBGP Peer 收到的路由再通告给任何 iBGP Peer。

向 eBGP Peer 通告路由时，会把自己的 AS 号附加在 as-path 属性的最左边

从 eBGP Peer 收到路由时，先检查 as-path 属性，如果发现有自己的 AS 号的路由则丢弃

iBGP 同步：

从 iBGP Peer 收到的路由，在成为最佳路径并向其他 eBGP Peer 通告之前必须被 IGP 所知道。

目的：防止可能出现的路由黑洞

解决：

- 把 BGP 的路由重发布到 IGP 中
- iBGP Peer 之间如果是 Full Mesh 则可以关闭同步
- 使用 MPLS VPN 也可以关闭同步

四、 BGP 路由进程模型：

BGP 如何获取路由：

- ✧ 自己发现
- ✧ Peer 通告

五、 路由决策顺序：

路由决策依赖于路由属性的取值

要参与路由决策之前必须解决下一跳可达及同步问题

- ✧ 优先选择具有最大权重属性的路由；本地发现的路由默认为 32768；Peer 通告的为 0
- ✧ 优先选择具有最大 Local-pref 属性的路由；默认都为 100
- ✧ 优先选择本地发现的而不是 Peer 通告的（下一跳为 0.0.0.0 的路由）
- ✧ 优先选择具有最短 AS-Path 属性的路由
- ✧ 优先选择具有最小起源属性的路由；i<e<?
- ✧ 优先选择具有最小 MED 属性的路由
- ✧ 优先选择 eBGP Peer 通告的而不是 iBGP Peer 通告的路由
- ✧ 优先选择最近的（IGP）next-hop 的路由
- ✧ 优先选择最老的路由
- ✧ 优先选择 BGP-RID 最小的 Peer 通告的路由
- ✧ 优先选择最小的 Neighbor Address 通告的路由

只有最佳路径的路由才能加入到 IP 路由表中，并能传播给 Peer

六、 强大的路由属性：

关于路由的一些描述性信息

一条路由可能有多个属性，可以人为置值以便执行路由决策

分类：

公认（所有 BGP ROUTER 都认识的）

- ✧ 必遵：必须携带的属性；如 origin ; AS ; next-hop
- ✧ 可选：可携带也可不携带的属性；如 local-pref ; atomic aggregate

任选（所有 BGP ROUTER 不必全认识的）

- ✧ 可传递：必须传递的参数；如 community ; aggregator
- ✧ 非可传递：可以不传递的参数；如 MED

具体属性：

- ■ Origin：起源属性；描述路由的来源；network 的标识为 i；redistribute 的标识为?；越小越好；可以人为改变。

- ■ AS-Path：描述路由被通告时所经过了哪些 AS；eBGP 向 Peer 通告时会把自己的 AS 号添加在 AS-Path 属性中；可以人为增加 AS 号以便影响路由决策；AS set 主要是防止路由聚合时可能出现的循环；可以使用常规表达式进行路由过滤等操作。

- ■ Next-Hop：由于 BGP Peer 之间的连接是逻辑的，可能出现下一跳不可达；eBGP 缺省使用 Peer 地址作为下一跳；iBGP 缺省不改变下一跳；可以人为改变；命令 neighbor *.*.*.* next-hop-self

- ■ Local-preference：一般用于 AS 内部；iBGP Peer 交换路由时携带通过人为改变改属性的值去影响路由决策；越大越好；默认 100。

- ■ Multi-Exit-Disc：eBGP Peer 之间通告路由时携带；越小越好；只能传递一个 AS。

- Weight：cisco 私有；只在本地有效；取值 0~65535；越大越好，缺省从 Peer 学得的路由为 0；本地发现的路由为 32768。

- Community：用来标识一些有共同特征或定义了共同特征的路由，以便统一处理。

- Atomic Aggregate：原子聚合属性；用于在路由聚合时携带改参数以便提醒 Peer 改路由是聚合路由。

- Aggregate：聚合属性；描述聚合路由的 Router-id 及所属的 AS 号。

- Originator ID：起源者 ID；反射路由器为了防止路由循环在路由中附加这个属性。

- Cluster List：反射路由器为了防止路由循环在路由中附加自己的 RID 在这个属性中。

七、 路由策略：

路由策略是通过影响路由决策来操纵路由表的生成而最终控制用户数据的转发路径。

方向：IN OUT

手段：属性控制；路由过滤

步骤：

- ✧ 画出拓扑图，描绘数据流的方向。
- ✧ 希望特定的 Router 有怎样的路由表？
- ✧ 谁会通告路由给我？如何控制？列举所有可能控制的方法。

控制对象：Update 包中的路由；

路由分类：

- 基于前缀长度和前缀
- 基于属性

属性操纵：

- **影响 AS 间的属性：**

  Origin

  Next-hop

  AS-Path

  MED

- **影响 AS 内的属性：**

  Local-pref

- **只影响自己的属性：**

  Weight

路由过滤：

有路由就有数据

没路由就没有数据

汇总（缺省）路由+部分细化路由

路由过滤工具

分布列表：

Neighbor a.b.c.d distribute-list # in/out

分布列表调用 ACL

使用 ACL 定义前缀或前缀长度

基本 ACL 定义前缀

扩展 ACL 定义前缀+前缀长度

前缀列表

Ip prefix # seq 10 前缀/前缀长度 [ge/le] [value]

使用相应的工具调用分类的结果

分布列表只能调用 ACL

使用前缀列表或路由图调用前缀列表

正则表达式：

在 BGP 里面主要应用于 As-path；Community

借助元符号及字符的组合定义字符序列

^：表示以^后面的字符为开始

$：表示以$前面的字符为结束

_：匹配空格、一个字符的开始或结束

.：匹配任何字符，包括空格

*：匹配前面的字符 0 个或多个

+：匹配一个或多个字符序列

?：匹配 1 个字符或 0 个字符

举例：

.*：代表匹配所有

^$：代表匹配自己区域内的 AS（as-path 属性为空）

a+：至少出现一个 a

ab?a：aa、aba

_100_：表示经过 AS100

_100$：表示起源 AS 为 AS100

^100.*：表示传输经过 AS100

As-path 列表：使用正则表达式定义 as-path 属性

Ip as-path access-list # permit/deny ******

使用过滤列表或路由图调用 as-path 列表

Neighbor a.b.c.d filter-list as-path# in/out

大规模 AS

Peer 的稳定性：

使用逻辑连接，利用链路冗余和 IGP 来解决 Peer 的稳定性

路由策略的改变使用软重置刷新

Neighbor a.b.c.d soft reconfiguration inbound

Clear ip bgp a.b.c.d in

路由重更新：引入 route-refresh 建立 Peer 的时候，协商该能力

Clear ip bgp a.b.c.d soft in/out

路由汇总及缺省路由

条件：地址连续分配

手段：

IGP：

Ip route 汇总 掩码 null 0

Bgp as# ； network 汇总

BGP：

Bgp as#

Aggregate-address 汇总 掩码 【参数】

缺省通告汇总路由+细化路由

Summary-only 参数只通告汇总路由

汇总会导致一些属性丢失

汇总后引入新的属性：原子汇总、汇总子

AS-set 参数能够防止循环

缺省路由：

静态，重发布

无条件发布：Neighbor a.b.c.d default-originate

有条件发布：Neighbor a.b.c.d default-originate route-map #

RR 与 Peer-Group

引用 RFC-1966 的几句话

1) A Route from a Non-Client peer

Reflect to all other Clients.

2) A Route from a Client peer

Reflect to all the Non-Client peers and also to the

Client peers other than the originator. (Hence the

Client peers are not required to be fully meshed).

3) Route from an EBGP peer

Send to all the Client and Non-Client Peers.

When a RR reflects a route from its Clients to a Non-Client peer, it must append the local CLUSTER_ID to the CLUSTER_LIST.

自动添加的 CLUSTER_ID 默认为自己的 BGP ID

可以手工修改：bgp cluster-id *数字或 IP*

如果有冗余的 RR，可以指定相同的 cluster-id，这样 RR 只相信从自己 Client 收到的路由，而不会造成互相信任对方的情况了。

RR 解决 iBGP 对等体过多的问题

Peer-Group 解决 Peer 配置过多的问题

iBGP 为防止循环，从 iBGP Peer 收到的路由不能向 iBGP Peer 通告。

为了解决 iBGP 全连接，使用 RR 和 BGP 联盟

选择一个或多个性能强大的设备作 RR；其他 iBGP Peer 作为 RR 的 Client；须考虑 RR 的冗余

通过引入 originator-id 和 cluster-list 解决可能出现的循环问题

RR 可以嵌套

路由反射器通告最佳路径

不改变 as-path、next-hop 等属性，避免次佳路径

Peer-Group：

具有相同属性策略的 Peer 的集合

创建 Peer-Group

Neighbor bluefox peer-group

针对 Peer-Group 作配置

Neighbor bluefox remote-as #

Neighbor bluefox update-source loopback #

Neighbor bluefox route-map #

添加 Peer 到 Peer-Group

Neighbor a.b.c.d peer-group bluefox

可以针对特定的 Peer 作配置

单独设置的策略要大于组里设置的~

Neighbor a.b.c.d route-map ##

Community

具有共同特征的路由可以附加一些数字标识，以便统一处理。

对端根据收到的路由的 Community 属性可以很容易挑选路由作属性操控。

公有团体：

NO_EXPORT：不通告给 eBGP

NO_ADVERTISE：不通告给任何 BGP Peer

LOCAL_AS：不能通告给任何外部的联盟 Peer

私有团体：人为规定的数字标识！

配置步骤：

启用 BGP 新格式的支持

Ip bgp new-format

Ip bgp-community new-format

建立访问列表或前缀列表

Access-list # permit ******

Ip prefix-list # seq 10 ******

建立路由映射

Route-map bluefox permit 10

Match ip address #

Set community {aa:nn | internet | local-as | no-export | ....}

绑定到特定的邻居

Neighbor a.b.c.d route-map #

启用团体属性通告

Neighbor a.b.c.d send-community

路由衰减：

对频繁更新的路由每 UP/DOWN 一次就附加惩罚值，如果一直保持 UP 状态，惩罚值又可以减少。

跟踪路由

快速收敛

不希望引起反复的震荡

每一次的拓扑变化都记录惩罚值，惩罚值可以叠加

累加到一定的惩罚值门限后不再通告这些路由的拓扑变化

路由稳定后，惩罚值减小，小到再使用门限后又可以继续使用

接收最大路由数量

Neighbor a.b.c.d maximum ###

BGP 其他的参考命令：

Distance bgp # # #

Distance # a.b.c.d d.c.b.a

Default-metric #

Bgp always-compare-med

Maximum-paths

Bgp bestpath as-path ignore

Neighbor a.b.c.d remove-private-as

Neighbor a.b.c.d password #

Neighbor a.b.c.d shutdown

Neighbor a.b.c.d timers 20 60

Bgp dampening

Bgp dampening route-map ~

Bgp scan-time #

【返回目录】

Lesson 19 ACL

一、 ACL 简介

Access control list 访问控制列表

数据分类工具：区分流向网络设备的数据流，基于特定数据流的特征区分数据

特征：

源 IP

源、目标 IP

协议号

端口号

其他一些信息

- **ACL 使用目的：**

区分数据以便统一执行规定的动作

包过滤：定义丢弃或放通的数据特征。丢弃一些数据；放通另外一些数据。

NAT：定义要转换的地址。

IPSec/VPN：定义要加密的数据

QoS：区分不同的业务数据

路由策略：定义要控制的路由

按需拨号；定义感兴趣的流量

- **ACL 分类：**

标准 ACL：基于源 IP 进行分类；编号 1~99

扩展 ACL：基于源 IP、目标 IP、协议号、端口号、应用层；编号 100~199

命名 ACL：就是把编号取代为名字，并用关键字区分标准或扩展。

二、 包过滤：

通过定义数据的特征，丢弃/放通一些数据

在特定的设备，特定的接口，特定的方向上绑定

人口 ACL：针对从该接口进入的数据进行包过滤

出口 ACL：针对从该接口离开该设备的数据进行包过滤

针对特定的一个接口，一个协议，一个方向上只能使用一个 ACL

ACL 默认不控制自己产生的数据

路由器处理数据包的流程：

ACL 前：

接口收到数据，还原成二层帧

基于目标 IP 查找路由表，找到出口

针对出口完成二层重写并封装

ACL 后：

入口 ACL：

接口收到数据，还原成二层帧

首先进行基于 ACL 的包过滤

被放通的数据查找路由表找出口

基于出口完成二层重写

出口 ACL：

接口收到数据，还原成二层帧

基于目标 IP 查找路由表，找出口

如果接口有出口 ACL，则进行包过滤

允许的数据基于出口完成二层重写

三、 ACL 的基本原则

ACL 的语句由两部分组成：条件、操作

Access-list 23 permit 192.168.1.8 0.0.0.0

在包过滤中首先检测数据是否符合条件，如果符合条件则执行规定的操纵动作。

ACL 由 ACL 号绑定多条语句

匹配顺序：先上后下执行查找

Cisco ACL 缺省有一条隐藏语句：Deny any；Deny any any

Deny 0.0.0.0 255.255.255.255

ACL 的语句书写顺序决定执行顺序

细化的、经常匹配的放在前面、粗略的放在后面

不能单独删除 ACL 中的某些语句

命名 ACL 支持单独删除 ACL 中的某条语句

ACL 对 CPU 有一定的考验~

四、 ACL 的基本配置

保证基本的连通性

定义数据的特征及相应的操作

Access-list [1-99]permit/deny 源 IP 通配符

在接口上绑定 ACL

Ip access-group acl# in/out

命名 ACL：

Ip access-list standard/extend bluefox

Config-acl# permit ~ or deny ~

可以针对特定的语句进行添加、删除

调用命名 ACL

Ip access-group bluefox in/out

自反 ACL

带 Established 选项的 ACL

检查 TCP 头部中的 Ack 或 Rst 位，如果该位置 1 则符合 Estalbished 选项

【返回目录】

Lesson 20 NAT

一、 NAT 简介

NAT：network address translation

保证 IP 地址的唯一性，私有地址需要转换成公网地址

在边界设备作 NAT 配置

内网满足的数据出去转换源 IP，并记录转换信息

数据回内网时，依照 NAT 记录进行 IP 的转换

NAT 优缺点：

优点： 缓解 ipv4 地址空间的不足

对外隐藏内网

缺点： NAT 使数据转发延时增大，对设备压力大！

无法实现端-端的通讯，影响一些特定的应用~

二、 NAT 术语

Inside local：内网分配的主机地址，私有地址不会向外呈现

Inside global：公有地址池中的地址，全球唯一

Outside local：外部主机呈现在内网中的地址

Outside global：外部主机的真实地址

地址转换关系：

1-----1 简单转换

1-----多 扩展转换

多---多 扩展转换

建议：一个公有 IP 地址转 100 个私有地址

三、 NAT 配置

静态 NAT：

定义外口：

```
Int s0/0

Ip nat outside
```

定义内口：

Int f0/0

Ip nat inside

定义如何转换：

Ip nat inside source static 10.0.0.1 200.0.0.1

动态 NAT：

用户主动访问外网，多个主机利用有限的公有地址

Int s0/0　　ip nat outside

Int f0/0　　ip nat inside

Access-list 1 permit 192.168.1.0 0.0.0.255

Ip nat pool bluefox 起始 IP 结束 IP network 掩码

Ip nat inside source list 1 pool bluefox overload

PAT：

适用只有一个公网 IP 地址或动态获得的 IP 地址

定义接口

定义需要转换的用户

定义转换：

Ip nat inside source list 1 interface s0/0 overload

查看

Show ip nat translation

清除：

Clear ip nat *

NAT 条目存储时间：TCP 的为 24 小时；

可以修改：ip nat translation timeout

【返回目录】

Lesson 21 三层交换

一、 进程交换技术

每个 IP 包的转发处理都需要 CPU 的参与

控制平面：主要负责通过路由协议的运算建立和维护 IP 路由表

数据平面：根据控制平面的信息转发 IP 数据包

二、 MLS

多层交换技术，也叫第一代多层交换，基于数据流的三层路由转发

快速交换，一次路由多次交换

MLS-RP：MLS 路由处理器；这个组件代表路由器选择过程的控制平面

MLS-SE：MLS 交换引擎；完成数据平面的功能

数据流：特定的源和目标之间共享 3 层和 4 层信息的单向数据包集合

MLS-RP 与 MLS-SE 之间运行 MLSP 协议保持联系

MLS 缓存表最多容纳 128000 条，并具有超时机制

三、 CEF

Cisco Express Forwarding

目前主流的多层交换技术，第二代多层交换技术。

基于路由拓扑结构和第二层邻接信息进行快速路由转发

转发信息在接收和转发数据包之前就已经被创建

FIB：精简版路由表，基于拓扑的转发模型

邻接表：一张 ARP 表

数据匹配 CEF 则转发，不匹配 CEF 的则丢弃！

四、 Catalyst 6500 Series Switch

硬件模块：

机箱

引擎

电源

板卡

服务模块

IOS

电路板卡：MSFC，PFC

MSFC：多层交换特征卡

PFC：策略特征卡

SUP1A+MSFC+PFC=MLS

SUP2，集成 PFC，可选 MSFC，系统为 IOS（=CEF）

SUP32/720，集成 PFC 和 MSFC，系统为 IOS（=CEF）

【返回目录】

Lesson 22 RSTP

一、 RSTP 简介

Rapid spanning tree protocol

RSTP 与 STP 的比较：

相同点：都是消除循环的一种二层协议

不同点：RSTP 的收敛比 STP 快

RSTP 别名：IEEE802.1W

目前各个厂商的设备均支持

二、 RSTP 的改进特性

- ✧ RSTP 的端口状态的切换是一种主动协商，而 STP 是被动等待超时
- ✧ STP 没有明确区分端口状态与端口角色，而 RSTP 明确区分端口的状态与角色
- ✧ STP 中的非根网桥只能被动的中继 BPDU，RSTP 中的非根网桥对 BPDU 的中继有一定的主动性。

三、 RSTP 的端口状态与端口角色

STP	RSTP
Disabled	Discarding
Blocking	
Listening	
Learning	Learning
Forwarding	forwarding

端口角色：

Root prot：根端口

Designed port：指定端口

Alternative port：作为根端口的备份

Backup port：作为指定端口的备份

Edge port：连接终端设备

Edge port 收到 BPDU 则会放弃快速收敛的特性进行 STP 的正常选举和收敛。

四、 RSTP 的收敛

端口状态切换

Mac 表的收敛

	STP	RSTP	MSTP
Protocol ID	0x0000	0x0000	0x0000
Protocol version	0x00	0x02	0x03
BPDU type	0x00	0x02	0x02
BPDU flags			
ROOT ID			
ROOT path cost			
Bridge ID			
Port ID			
Message age			
Max age	20	20	20
Hello time	2	2	2
Forward delay	15	15	15

标记域：

TCA	Agreement	Forwarding	Learning	Port Role	Proposal	TC

Port Role：

00：未知

01：根端口

10：Alternate/Backup

11：指定端口

初始化时，Learning 和 Proposal 置位（指定端口）

交换机收到比自己好的 BPDU，并看到 Proposal 置位，则进行同步好的 BPDU

同步完成后回应 BPDU，同时 Agreement/Forwarding 置位！

三个过程：建议、同步、回应！

五、 RSTP 的配置

Spanning-tree mode rapid-pvst

Spanning-tree portfast

Spanning-tree link-type {p-to-p | share}

RSTP 端口在 2 个 Hello 里没有收到 RSTP 的 BPDU，则自动降到 STP 模式下工作！

【返回目录】

Lesson 23 MSTP

是一种集成 PVST 的多生成树，有着 CST 的低 BPDU 开销和 RSTP 的快速收敛等优点集于一身的生成树协议！

MSTP 可以将具有相同转发路径的 Vlan 映射到一个生成树！无需每个 Vlan 一个生成树！

可以实现快速的备份冗余，保证网络的高可靠性，又可以实现低 BPDU 开销的流量负载，提高网络的利用率和转发性能。

MSTP 区域：抑制生成树覆盖范围从而加快生成树的收敛

满足属于同一个 MSTP 区域的条件：

- ✧ 具有相同的 MSTP 配置名称
- ✧ 具有相同的 MSTP 配置修订号
- ✧ 具有相同的 Vlan 与生成树实例的映射关系的集合

针对思科设备每个区域只能支持 16 个生成树实例，其中至少有一个 IST 实例。

IST 实例：内部生成树实例，是 MSTP 区域内缺省的生成树实例，编号为 0，缺省 MSTP 交换机上所有的 Vlan 都映射到 IST 中。

其他生成树实例的 BPDU 被包含在 IST 的 BPDU 中进行传递

IST 实例是代表整个交换机网络的 CST 的子集

MSTI：由管理员手工定义的生成树实例，只具有本地意义。

【返回目录】

Lesson 24 VRRP

全称 Virtual Redundancy Router Protocol，和 HSRP 类似

默认具有抢占功能

VRRP 中只有主网关才能发送报文

VRRP 间隔时间 1S，Holdtime 为 3 个 Hello 间隔

VRRP 承载协议不同，直接使用 IP 封装，协议号 112！

VRRP 支持物理接口 IP 作为虚拟的 IP

国际标准

VRRP 技术实现网络的路由冗余和负载均衡

1 问题的提出

随着网络应用的不断深入和发展，用户对网络可靠性的需求越来越高。网络中路由器运行动态路由协议如 RIP、OSPF 可以实现网络路由的冗余备 份，当一个主路由发生故障后，网络可以自动切换到它的备份路由实现网络的连接。但是，对于网络边缘终端用户的主机运行一个动态路由协议来实现可靠性是不可 行的。一般企业局域网通过路由器连接外网，局域网内用户主机通过配置默认网关来实现与外部网络的访问。

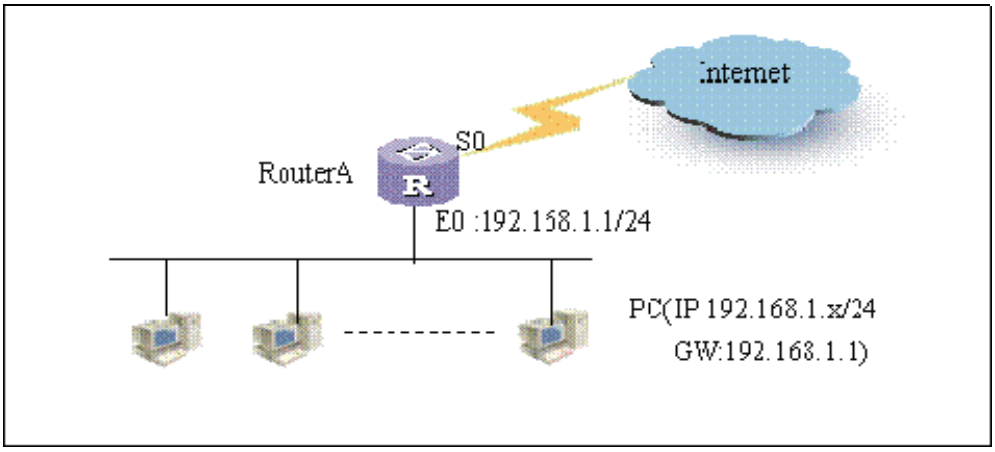


图 1 配置默认网关

如图一所示，内部网络上的所有主机都配置了一个默认网关（GW:192.168.1.1）,为路由器的 E thernet0 接口地址。这样，内网主机发出的目的地址不在本网段的报文将通过默认网关发往 RouterA，从而实现了主机与外部网络通信。路由器在这 里是网络中的关键设备，当路由器 RouterA 出现故障时,局域网将中断与外网的通信。对于依托网络与外部业务往来频繁的企业以及公司的分支机构与总部的 联系、银行的营业网点与银行数据中心的连接等方面的应用将因此受到极大的影响。为提高网络的可靠性，在网络构建时，往往多增设一台路由器。但是，若仅仅在 网络上设置多个路由器，而不做特别配置，对于目标地址是其它网络的报文，主机只能将报文发给预先配置的那个默认网关，而不能实现故障情况下路由器的自动切 换。VRRP 虚拟路由器冗余协议就是针对上述备份问题而提出，消除静态缺省路由环境中所固有的缺陷。它不改变组网情况，只需要在相关路由器上配置极少几条 命令，在网络设备故障情况下不需要在主机上做任何更改配置，就能实现下一跳网关的备份，不会给主机带来任何负担。

2 VRRP 技术分析

VRRP(Virtual Router Redundancy Protocol)是一种 LAN 接入设备容错协议，VRRP 将局域网的一组路由器（包括一个 Master 即活动路由器和若干个 Backup 即备份路由器） 组织成一个虚拟路由器，称之为一个备份组，如图 2 所示。

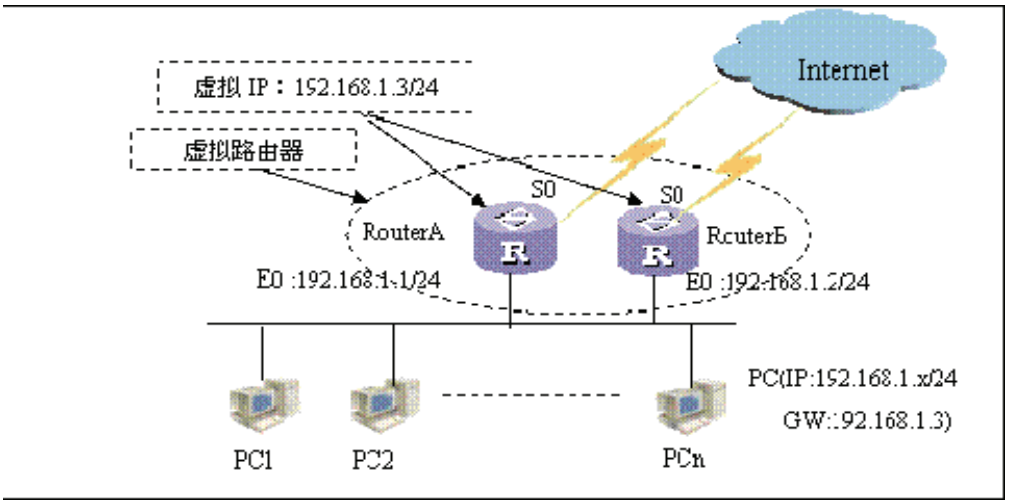


图 2　虚拟路由器示意图

VRRP 将局域网的一组路由器，如图二中的 RouterA 和 RouterB 组织成一个虚拟的路由器。这个虚拟的路由器拥有自己的 IP 地址 192.168.1.3，称为路由器的虚拟 IP 地址。同时，物理路由器 RouterA ,RouterB 也有自己的 IP 地址（如 RouterA 的 IP 地址为 192.168.1.1，RouterB 的 IP 地址为 192.168.1.2）。局域 网内的主机仅仅知道这个虚拟路由器的 IP 地址 192.168.1.3，而并不知道备份组内具体路由器的 IP 地址。在配置时，将局域网主机的默认网关设置为 该虚拟路由器的 IP 地址 192.168.1.3。于是，网络内的主机就通过这个虚拟的路由器来与其它网络进行通信，实际的数据处理由备份组内 Master 路由器执行。如果备份组内的 Master 路由器出现故障时，备份组内的其它 Backup 路由器将会接替成为新的 Master，继续向网络内的主机提供路由 服务。从而实现网络内的主机不间断地与外部网络进行通信。

VRRP 通过多台路由器实现冗余，任何时候只有一台路由器为主路由器，其他的为备份路由器。路由器间的切换对用户是完全透明的，用户不必关心具体过程，只要把缺省路由器设为虚拟路由器的 IP 地址即可。路由器间的切换过程：

⑴ VRRP 协议采用竞选的方法选择主路由器。比较各台路由器优先级的大小，优先级最大的为主路由器，状态变为 Master。 若路由器的优先级相同，则比较网络接口的主 IP 地址，主 IP 地址大的就成为主路由器，由它提供实际的路由服务。

⑵ 主路由器选出后，其它路由器作为备份路由器，并通过主路由器发出的 VRRP 报文监测主路由器的状态。当主路由器正常工作时，它会每隔一段时间发送一个 VRRP 组播报文，以通知备份路由器，主路由器处于正常工作状态。如果组内的备份路由器长时间没有接收到

来自主路由器的报文，则将自己状态转为 Master 。当组内有多台备份路由器时，重复第 1 步的竞选过程。通过这样一个过程就会将优先级最大的路由器选成新的主路由器，从而实现 VRRP 的备份功能。

3 VRRP 技术应用于大型园区网络

VRRP 技术不但用于上述局域网连接外网的路由器的备份，还广泛用于大型园区网络核心层三层交换机的冗余备份。在大型园区网络中，核心层处于网 络的中心，网络之间的大量数据都通过核心层设备进行交换，同时承担不同 VLAN 之间路由的功能。核心层设备一旦宕机，整个网络即面临瘫痪。因此，在园区网 络设计中，核心设备的选择，一方面要求其具有强大的数据交换能力，另一方面要求其具有较高的可靠性，一般选择高端核心三层交换机。同时，为进一步提高核心 层的可靠性，避免核心层设备宕机造成整个网络瘫痪，一般在核心层再放置一台设备，作为另一台设备的备份，一旦主用设备整机出现故障，立即切换到备用设备， 确保网络核心层的高度可靠性。

核心层三层交换机的切换需要应用 VRRP 技术。如图 3 所示（为简便起见，以两层结构的网络为例），为提高网络的可靠性，在网络核心层放置两台三 层交换机（S1、S2），接入层二层交换机（SW1、SW2、…、SWn）分别连接两台核心交换机。在大型园区网络中，为抑制广播信号，提高网络的性能， 同时实现网络的安全访问控制，一般根据具体情况将整个网络分成多个不同的 VLAN，V LAN 中主机的默认网关设置为三层交换机上 VLAN 的接口地址。

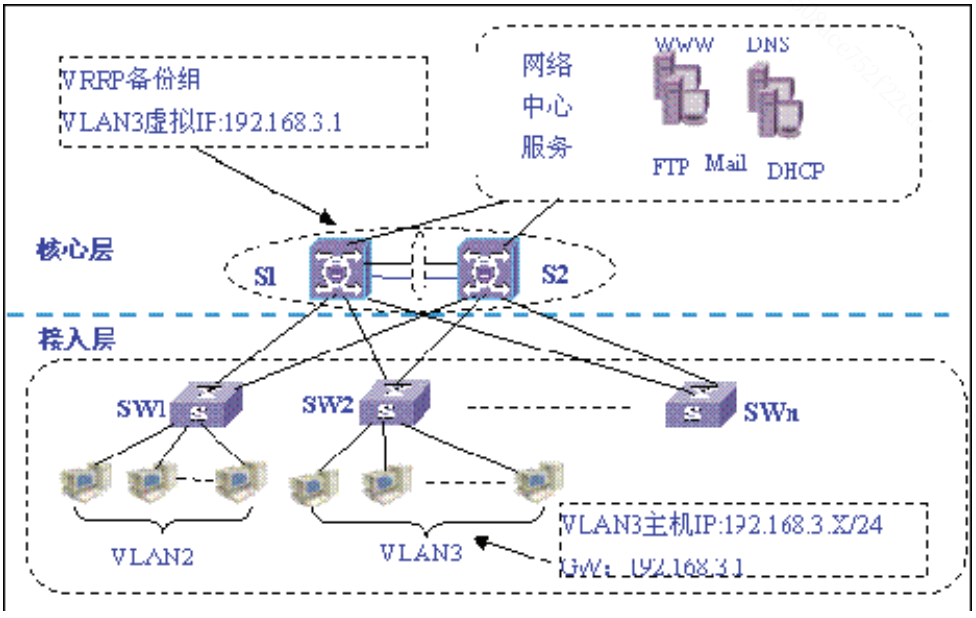


图 3 VRRP 在园区网络中的应用

VRRP 协议将网络中两台三层交换机（S1、S2）组成 VRRP 备份组，针对于网络中每一个 VLAN 接口，备份组都拥有一个虚拟缺省网关地址。 如图以 VLAN3 为例，VRRP 备份组设置 VLAN3 的虚拟 IP 地址（譬如：192.168.3.1）,备份组中 S1、S2 同时分别拥有自己的 VLAN3 的接口 IP（譬如分别为：192.168.3.2，192.168.3.3），VLAN3 内主机的默认网关则设为 VRRP 备份组 VLAN3 的虚拟 IP 地址 （192.168.3.1）。VLAN3 内的主机通过这个虚拟 IP 访问 VLAN3 之外的网络资源，但实际的数据处理有备份组内活动（Master）交换机 执行。如果活动交换机发生了故障，VRRP 协议将自动由备份交换机（Backup）来替代活动交换机。由于网络内的终端配置了 VRRP 虚拟网关地址，发生 故障时，虚拟交换机没有改变，主机仍然保持连接，网络将不会受到单点故障的影响，这样就很好地解决了网络中核心交换机切换的问题。

4 VRRP 用于负载均衡

在 VRRP 中，允许一台路由器加入多个备份组，通过多备份组设置可以实现负荷分担。

如图二所示，路由器 RouterA 作为备份组 1 的 Master 路由器，同时又为备份组 2 的 Backup 备份路由器。而路由器 RouterB 正相反，作为备份组 2 的 Master，并为备份组 1 的 Backup 备份路由器。一部分主机使用备份组 1 的虚拟 IP 作网关，另一部分主机使用备份组 2 的虚拟 IP 作为网关。这样，既达到分担数据流，又实现相互备份的目的。

路由器配置（实际 IP, RouterA :192.168.1.1/24，RouterB：192.168.1.2/24）

	备份组 1	备份组 2
虚拟 IP	192.168.1.3	192.168.1.4
备份组成员	Master:RouterA，Backup：RouterB	Master:RouterB，Backup：RouterA

局域网主机配置（假如网络有 100 台主机）

	PC1——PC50	PC51——PC100
IP Address	192.168.1.X/24	192.168.1.X/24
Gateway	192.168.1.3	192.168.1.4

两台路由器互为备份。在路由器正常时，两台路由器各自分担一部分数据流量；当其中一台路由器出现故障时,另一台路由器就会自动分担起所有数据流量,数据的传输不会受到任何的影响。这样既达到负载均衡，又实现相互备份的目的。

5 结论

对于使用固定网关的网络，当此网关出现故障时，要想将故障对用户的影响降低到最小，VRRP 协议无疑是最低价的选择。对于使用多个网关的网络中 可以使用 VRRP 协议让不同的网关之间互相备份，这样既不会增加网络设备，同时又达到了热备份的目的，使网络故障发生时用户的损失降至最低。而且 VRRP 是 RFC 标准协议，能方便地实现各厂家设备间的互通。正是由于 VRRP 具有这些优点，使得它成为建设一个稳定可靠网络所需的有力工具。

6 参考配置

Router A

```
interface ethernet 1/0
ip address 10.1.0.2 255.0.0.0
vrrp 1 priority 120
vrrp 1 authentication cisco
vrrp 1 timers advertise 3
vrrp 1 timers learn
vrrp 1 ip 10.1.0.10
vrrp 5 priority 100
vrrp 5 timers advertise 30
vrrp 5 timers learn
vrrp 5 ip 10.1.0.50
vrrp 100 timers learn
no vrrp 100 preempt
vrrp 100 ip 10.1.0.100
no shutdown
```

Router B

```
interface ethernet 1/0
ip address 10.1.0.1 255.0.0.0
vrrp 1 priority 100
```

vrrp 1 authentication cisco

vrrp 1 timers advertise 3

vrrp 1 timers learn

vrrp 1 ip 10.1.0.10

vrrp 5 priority 200

vrrp 5 timers advertise 30

vrrp 5 timers learn

vrrp 5 ip 10.1.0.50

vrrp 100 timers learn

no vrrp 100 preempt

vrrp 100 ip 10.1.0.100

no shutdown

【返回目录】

Lesson 25 GLBP

1）GLBP 介绍

cisco ios 支持版本 IOS 12.2（15）T 以上

全称 Gateway Load Banancing Protocol，

和 HRSP、VRRP 不同的是，GLBP 不仅提供冗余网关，还在各网关之间提供负载均衡，而 HRSP、VRRP 都必须选定一个活动路由器，而备用路由器则处于闲置状态。

和 HRSP 不同的是，GLBP 可以绑定多个 MAC 地址到虚拟 IP，

从而允许客户端选择不同的路由器作为其默认网关，而网关地址仍使用相同的虚拟 IP，从而实现一定的冗余。

2）活动网关选举

使用类似于 HRSP 的机制选举活动网关，

优先级最高的路由器成为活动落由器，称作 Acitve Virtual Gateway，其他非 AVG 提供冗余。备份的 AVF，也是实现数据的转发，而在 GLBP 中，同一个 GROUP 的所有路由器（最多 4 个）可以同时转发流量。

某路由器被推举为 AVG 后，和 HRSP 不同的工作开始了，AVG 分配虚拟的 MAC 地址给其他 GLBP 组成员。

所有的 GLBP 组中的路由器都转发包，

但是各路由器只负责转发与自己的虚拟 MAC 地址的相关的数据包。

3）地址分配

每个 GLBP 组中最多有 4 个虚拟 MAC 地址，非 AVG 路由器有 AVG 按序分配虚拟 MAC 地址，

非 AVG 也被称作 Active Virtual Forwarder(AVF)。

AVF 分为两类：Primary Virtual Forwarder 和 Secondary Virtual Forwarder。

直接由 AVG 分配虚拟 MAC 地址的路由器被称作 Primary Virtual Forwarder，

后续不知道 AVG 真实 IP 地址的组成员，只能使用 hellos 包来识别其身份，然后被分配虚拟 MAC 地址，此类被称作 Secondary Virtual Forwarder。

4）GLBP 配置

如果 AVG 失效，则选举就会发生，决定哪个 AVF 替代 AVG 来分配 MAC 地址，推举机制依赖于优先级。

最多可以配置 1024 个 GLBP 组，不同的用户组可以配置成使用不同的组 AVG 来作为其网关。

```
router#conf t
router(config)#int fastethernet 0/0
router(config-if)#ip address 10.1.1.1
router(config-if)#glbp 99 ip 10.1.1.254
router(config-if)#glbp 99 priority 105
```

router(config-if)#glbp 99 preempt delay 10

router(config-if)#glbp 99 weighting track int s0 10

router(config-if)#exit

router(config)#^Z

使用下面的接口命令来为路由器分配 GLBP 的优先级：#glbp group priority level 组号的范围从 0-1023 优先级从 1- 255，越大优先级越高。

如果使用 HSRP，那么其他的路由器只能在当前活跃的路由器失效时才能接替活跃的角色，如果路由器要比当前路由器有更高的优先级，GLBP 将剥夺主路由器并成为 AVG，可以使用下面的命令剥夺启动并且在剥夺之前延迟一段时间。一般是 4S

glbp group preempt [delay minimum seconds]

GLBP 使用一个加权函数来决定哪台路由器成为组中虚拟 MAC 得知的 AVF，每台路由器开始时都带一个最大权值（1 到 254）。当某个特定接口失效的时候，权值所配置的值减少，GLBP 使用门槛值来确定路由器是否能成为 AVF，如果权值降到较低的门槛以下，路由器必须放弃 AVF 的角色，在权值上升到较高的门槛以上的时候，路由器可以继续它的 AVF 角色。在缺省的情况下，路由器设置的最大权值为 100，如果要动态改变权值，GLBP 必须要知道所跟踪的接口并且知道如何调整权值，首先必须定义跟踪的接口，可以使用下面的全局配置命令#track object-number interface type mod/num {line-protocol | ip routing} object-number 是一个任意的索引值 1-500，这个值用作权值的调节，触发调整的条件可以是线协议也可以是路由协议。

还必须定义接口权值门槛：#glbp group weighing maximum [lower lower] [upper upper] 最大权值的范围从 1-254 缺省值为 100 较高门槛值缺省值为 MAXIMUM，较小门槛值缺省值为 1，各自定义为可以或者不能成为 AVF 的门槛。

还必须配置 GLBP 知道跟踪了哪个接口，以便权值可以使用下面接口配置命令来改变权值：

#glbp group weighting track object-number [decrement value] 当所跟踪的接口失效的时候，权值减少了 VALUE 从 1-254 缺省值是 10，在 AVF 的路由器有更高权值的时候，它也不能剥夺另一台路由器。

在 AVF 路由器上，用下面的接口命令来定义负载均衡的方式：#glbp group

load-balancing [round-robin | weighted | host-dependent]

要启动 GLBP，必须给该组分配一个虚拟 IP 地址，可以通过以下的接口配置命令来实现：

#glbp group ip [ip-address [secondary]]

注意 GLBP 是 CISCO 专有的，而且目前只能在 Catalyst 6500 Supervisor 720 的 Cisco IOS 软件版本 12.2（14）SX 中使用。

【返回目录】

Lesson 26 端口汇聚

一、 基本定义

将两台设备之间的多个物理以太网接口进行逻辑绑定，形成一条虚拟链路，以便增加带宽。实现负载均衡、主备备份等的一种链路技术

二、 实施

注意事项：

Speed Duplex 要一致

相关特性要一致

具体实施：

Int range f0/0 – 3

Channel-group 1 mode on

Int range f0/0 – 3

No switchport

Channel-group 1 mode on

Int port-channel 1

No switchport

Ip add 192.168.3.254 255.255.255.0

自动协商：

Pagp：思科私有，desirable/auto

Lacp：国际标准，active/passive

三、 负载均衡

负载均衡的参数：

源 Mac	目标 Mac	源+目标 Mac
源 Ip	目标 IP	源+目标 IP
源 Port	目标 Port	源+目标 Port

负载均衡的算法：

异或运算：相同为 0，不同为 1

【返回目录】

Lesson 27 模块冗余

一、 模块化交换机组件

Cisco 模块化交换机：4500、6500

机箱：

4500	4503	4506	4507R	4510R	
6500 以前	6503	6506	6509	6509-NEB	6513
6500 目前	6503E	6506E	6509E		6513E

引擎：

	II	II+	II+TS	IV	V	V-10G
4500	4013	4013+	4013+-TS	4515	4516	4516-10G
	不支持三层，CatOS	支持三层，IOS	只支持 4503			

4507R、4510R 目前引擎只能做主备

4510R 最下面的插槽不能插线卡，只能插服务模块

	SUP1A	SUPII	SUP32	SUP720
6500			32G	720G
				主流引擎，默认开启三层

SFM：交叉交换矩阵，提升背板带宽

6500 的引擎都支持冗余，6503 不支持 SUP72 引擎

6500 引擎第一二个插槽（SUPI/SUPII）

6500 引擎第五六个插槽（SUP720）

二、 引擎冗余

RPR：路由处理器冗余，4500、6500 默认支持的模式，切换时间 1~4Min

RPR+：路由处理器冗余+，切换时间 30~60S

SSO：状态化切换引擎冗余模式，不支持路由协议

SSO/NSF：状态化切换非停止转发，支持 SUPII 和 SUP720；支持路由协议

RPR：同步 Startup-config 文件；备份引擎替代主引擎时会自动重新加载 Startup-config，重新初始化。

RPR+：只有 6500 的才支持，思科私有，主备引擎正常情况下，进行同步 startup-config，running-config 文件。备份引擎处于完全初始化状态。当主引擎失效时，备份引擎马上进行工作！切换时间<1Min。

SSO：主备切换时不会造成二层数据流的中断，会造成三层中断。正常情况下，进行同步 Mac 表、startup-config、running-config 文件，4500，6500 都支持。

SSO/NSF：目前只有 6500 的才支持。主备切换 L2,L3 都不会中断数据流。主备同步 startup-config、running-config、Mac 表、CEF 表。

三、 电源冗余

电源功率：6500-----1400W、2700W、3000W、6000W、8700W

电源工作模式：

联合供电：一起供电

冗余供电：正常两个同时供电，一个电源出现故障另一个电源能全部承担的供电模式。

【返回目录】

Lesson 28 交换网络安全

一、 设备访问安全

物理安全

口令

Enable 密码：从用户模式进入特权模式时使用的密码

Console 密码：Console 线登陆的密码

VTY 密码：Telnet 登陆密码

密码加密显示：service password-encryption

密码最小长度：security password min-length [0-16]

控制特定的主机访问：access-list 1 permit host 192.168.5.8

Line vty 0 4

Access-class 1 in

用户名和密码：缺省都是 cisco

创建：username cisco password bluefox

Line vty 0 4

Login local　　#用户账号优先

Password haohaoxuexi

特权级别

16 个级别：

0~1：用户模式，权限低

15：特权模式，拥有全局权限

2~14：自定义级别

Privilege exec/config level 2 router ospf

Enalbe secret level 2 123456

Enable 2

******

SSH：

Username cisco password bluefox

Crypto key generate rsa # modulus 1024

Line vty 0 4

Transport input ssh

二、 AAA

基于 C/S

服务器：安装了 Cisco 的 ACS 软件的 OS 或者其他的一些服务器软件。华为的 Cams，锐捷的 Sams。

安全协议：

Tacacs+：采用 TCP49

Radius：采用 UDP1812，1813

开启 AAA 服务：

Aaa new-model

Radius-server host 192.168.3.8

Radius-server key bluefox

AAA 认证的配置：

Aaa authentication login default group radius local none

Login default 作用于所有线路模式下的密码

Aaa authentication login t24 group radius local

Line vty 0 4

Login authentication t24

AAA 授权的配置

Aaa new-model

Tacacs-server host 192.168.3.8 key bluefox

Aaa authorization command default group tacacs+ local

Username xiaoge privilege 5 password cisco

AAA 审计的配置

Aaa accounting command default start-stop tacacs+

【返回目录】

Lesson 29 802.1x

802.1x 客户端：能够支持 802.1x，能发起 EAP 报文的 PC 终端（802.1x 软件或系统自带）

802.1x 认证代理

802.1x 认证服务器（AAA 服务器）

802.1x 认证协议：EAP，Extend Authentication Protocol，扩展认证协议

EAPoL：EAP over Lan

EAPoRadius：EAP over Radius

EAP 工作模式：

透传：将 EAP 报文封装在 Radius 中

终结：直接封装在 Radius 报文中

Code	Identifier	Length	Type	Type-data

Code：

1：-----Request

2：-----Response

3：-----Success

4：-----Failure

Identifier：用于匹配对应的 Request 和 Response，每一个 Request 就有一个 Response，相当于 TCP 的序列号。

Type：

1：Identifier

2：Notification

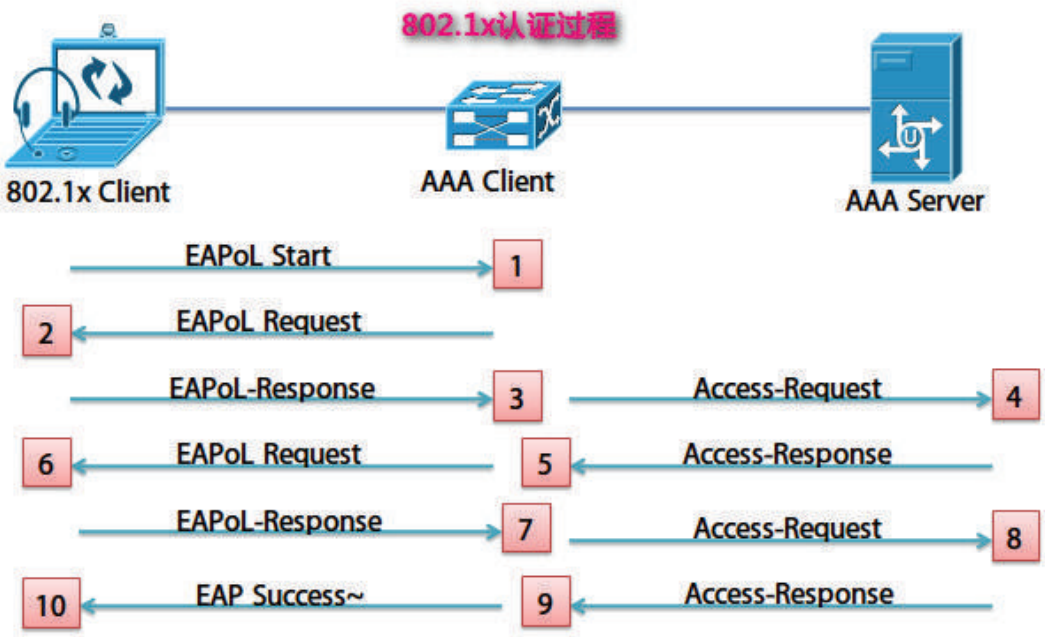
3：Nak（Response Only）

4：MD5-Challege

5：One-Time Password

6：Generic Token Card

802.1x 认证过程：



各数据包完成的任务：

1：802.1x 客户端发起 EAPoL 的连接。

2：AAA Client 请求 802.1x 客户端的用户名。

3：802.1x 客户端把用户名发送给 AAA Client。

4：AAA Client 把用户名发送给 AAA Server。提取 AAA Client 发来的用户名，查找服务器的数据库找到相应的密码并产生一个随机数，把（用户名、密码、随机数）进行 MD5 散列码计算，存储这个结果。

5：把用户名和随机数发送给 AAA Client

6：AAA Client 发用户名和密码发送给 802.1x 客户端，客户端软件根据用户输入的用户名和密码并使用接收到的随机数进行 MD5 计算，产生一个结果。

7：客户端把这个结果发送给 AAA Client

8：AAA Client 把这个结果发送给 AAA Server

9：AAA Server 根据这个结果来匹配自己的产生的值，匹配成功则返回成功，否则返回失败，或重新连接。

10：AAA Client 把成功或失败的消息告诉给 802.1x 客户端，如果成功则开发此端口，不成功则继续连接或超时作其他策略，如 Guest Vlan 等。

802.1x 端口状态：

受控端口

非受控端口

802.1x 认证配置：

客户端：安装 802.1x 客户端软件

代理：

Aaa new-model

Radius-server host 192.168.3.8 key bluefox

Aaa authentication dot1x defautl group radius local

Dot1x system-authentication-control

Int f0/1 ; sw mo ac ; dot1x port-control auto

服务端：指定 AAA 客户端、添加用户名和密码

802.1x 的高级特性：

Guest Vlan：将预先配置的 Vlan 用来做 Guest Vlan

Int f0/2 ; dot1x guest vlan 8

需要用 Pvlan、ACL 等控制 Pvlan 的策略

基于用户的 Vlan：

账号与 Vland 的对应关系，该账号拥有的权限

基于用户的 ACL：

ACL 语句写在 AAA 服务器上

【返回目录】

Lesson 30 交换网络中的ACL

一、 ACL 的作用

流量的定义

访问控制

二、 ACL 的分类

IP 流

非 IP 流

三、 ACL 的查询规则

自上而下的查找顺序

四、 交换网络中的 ACL

Racl：路由 ACL

应用于交换机三层接口上的 ACL（IP 流的 ACL）

Pacl：端口 ACL

应用于交换机二层接口的 ACL，只对 In 方向的匹配，可以定义 IP 流和非 IP 流

Mac-Acl：

Mac access-list 1 deny mac_pc1

Int f0/2 ; mac access-group 1 in

Vlan-map：

定义 ACL：定义数据流

Vlan-map：决定数据流的行为

Access-list 100 permit 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255

Vlan access-map bluefox 10

Match ip address 100

Action drop

Vlan filter bluefox vlan 2

【返回目录】

Lesson 31 Pvlan与端口镜像

一、 Pvlan 技术

定义：Vlan 内部再划分 Vlan，二个层次 Vlan，内部 Vlan 叫子（辅助）Vlan，外部 Vlan 叫主 Vlan

应用背景：智能小区、商务写字楼、城域以太网

操作机制：

Vlan 的分类：主 Vlan、子 Vlan

团体 Vlan：内部数据可以通讯

隔离 Vlan：内部数据不可以通讯

接口的类型：

团体 Vlan 端口：位于团体 Vlan 的那个端口

隔离 Vlan 端口：位于隔离 Vlan 的那个端口

混杂端口：可以与子 Vlan 内所有的端口通讯

华为交换机的混杂端口：允许不同的 Vlan 内的数据通过这个端口并且不打标记！

二、 端口镜像技术

SPAN：

目标端口：安装网络分析仪的那个端口（IDS/IPS）

源端口：被监控的那些设备所连的端口流经源端口的数据复制一份发送给目标端口

本地 SPAN：

远程 SPAN：

RSPAN-Vlan：专门承载被捕获的流量

三、 应用场景

PVLAN 主要应用于电信级网络和写字楼网络

端口镜像应用于网络分析和接 IDS/IPS 的环境

三、 基本配置

1.更改模式：

Vtp mode transparent

2.创建主 Vlan

Vlan 20

Private-vlan primary

3.创建私有 Vlan

Vlan 201

Private-vlan isolated //隔离 Vlan

Vlan 202

Private-vlan community //团体 Vlan

4.关联私有 Vlan 到主 Vlan 下面

Vlan 20

Private-vlan association 201-202

5.更改接口模式

Int f0/2

Switch mode private-vlan host/promiscuous　　//主机模式、混杂模式

Switch private-vlan host-association 20 201　　//主机模式关联对应的主私 Vlan

Switch private-vlan host-association 20 201-202　　//主机模式关联对应的主（所有）私 Vlan

6.在对应的主 Vlan 的 SVI 接口上映射私有 Vlan

Int vlan 2

Ip add a.b.c.d *.*.*.*

Private-vlan mapping 201-202

【返回目录】

Lesson 32 DHCP

一、 DHCP 的基本情况

CS 工作模式：

二、 DHCP 的配置

Windows

非 Windows（IOS）

Service dhcp

Ip dhcp relay information option

Ip dhcp pool vlan2

Network 192.168.2.0 255.255.255.0

Default-router 192.168.2.254

Dns-server 202.103.96.112

Netbios-name-server ~

Lease ~

Ip dhcp excluded-address 192.168.2.250 192.168.2.254

Ip dhcp ping packets 3

三、 DHCP 的安全威胁

DHCP 服务器冒充

DHCP DoS 攻击

ARP 攻击

IP 地址欺骗

四、 DHCP 的安全威胁的解决方案

DHCP Snooping：

解决 DHCP 服务器的冒充；为 DHCP Dos、ARP 攻击、IP 欺骗提供帮助。

定义信任端口与非信任端口来防止 DHCP Server 的冒充

信任端口：所有 DHCP 报文都可以流通

非信任端口：不允许从这个端口出去的 DHCP Ack 和 DHCP Offer 包

DAI：Dynamic ARP Inspection

基于端口进行 ARP 报文的检测（参照物：DHCP Snooping Binding）

解决 ARP 攻击

IP Source Guard：

利用 DHCP Snooping Binding 表的信息，检查交换机端口上所有过滤的流量；可以检测 IP 地址甚至 Mac 地址是否为 DHCP 服务器合法分配的，如果不是则丢弃该数据

解决 IP 地址的冲突问题~

【返回目录】

Lesson 33 链路与介质

一、 100M 链路

- 100Base-TX

介质：UTP 双绞线（5 类、超 5 类）

传输距离：100m

连接器：RJ-45

应用场景：设备---终端

- 100Base-FX

62.5um-mmF：400m（半双工）、2000m（全双工）

9um-smF：10km

介质：光纤

光缆：适应于室外，建筑物之间

跳线：两头都有连接器

尾纤：一头有连接器

单模：激光二极管，距离远，黄色

多模：发光二极管，10km 以内，橙色

光纤连接器：

GBIC：非主流

SFP：主流

接头：

LC：用来接 SFP

SC：用来接 GBIC

FC：用来光端机、光纤配线架

MT-RJ：

应用场景：建筑内部互连或与服务器的连接

光纤收发器：应用于局域网的光电转换

二、 1000M 链路

- 1000Base-TX：

  超 5 类双绞线，100m，RJ-45

- 1000Base-SX：

  短波光纤，62.5/50um-MMF，850nm，275m/550m

- 1000Base-LX：

  长波光纤，1300nm，62.5/50/9，400m/550m/10km

- 1000Base-ZX：

  超长波光纤，1500nm，9um，750km

✧ GBIC 型号：

GBIC-5483：1000Base-TX

GBIC-5484：1000Base-SX

GBIC-5486：1000Base-LX

GBIC-5487：1000Base-ZX

✧ SPF 型号：

GLC-T：

GLC-SX-MM：

GLC-LH-SM：

GLC-ZX-SM：

三、 10000M 链路

10G-Base-SR：<850nm，介质：62.5um---33m，50um---66m~300m

连接器：LC、SC、FC

10G-Base-LR：1310nm，介质：9um-SMF，10km，LC/SC

10G-Base-ZR：1550nm，介质：9um-SMF，40km，LC/SC

10G-Base-LX4：1310nm，WWDM

10G-Base-TX：双绞线标准

Catalyst：3750、4500、6500、4900 支持 10G 接口

【返回目录】

Firewall Technology

Lesson 34 Firewall

一、 定义

控制介于网络之间不同区域的流量，是一套系统或设备

保护内网资源，免受攻击（隔离+保护）

二、 部署

- 基于主机 FW：天网、瑞星、卡巴、金山毒霸等（分布式）

  优点：简单、易用

  缺点：管理困难

- 基于网络 FW：使用网络设备保护并隔离网络流量（集中式）

  优点：管理方便

  缺点：需要一定的网络基础

三、 OSI 七层模型

层次	功能
应用层	如何与用户交互
表示层	确定数据类型
会话层	建立、监控、拆除连接
传输层	提供可靠与非可靠的传输
网络层	定义逻辑地址
链路层	定义物理地址
物理层	定义物理链路的特性

四、 ICMP

- 差错报告报文：终点不可达、原点抑制、超时等
- 查询报文：回送请求与回答等

ICMP 报文包括 8 个字节的首部和可变长的数据部分

类型	代码	校验和
首部的其余部分		
数据部分		

常见的 PING 命令就是利用了 ICMP 的回送请求和回送回答报文

- 回送请求报文的类型是 8、代码是 0
- 回送回答报文的类型是 0、代码是 0

相关的攻击：

Ping of Death：

Ping Flood：

Smurf：

五、 传输层

TCP、UDP

产生 ISN 的方法：

- 以一定的值增加，64K 规则
- 与时间有关的产生规则
- 伪随机数的产生规则（PIX、ASA）

相关的攻击：

SYN Flood：

UDP Flood：

六、 应用层

七、 服务层面和工作层面

服务层面：2、3、4、5、7

工作层面：2、3

八、 根据 FW 服务层面的不同进行分类

类别	服务层面
包过滤 FW	3、4
状态 FW	3、4、5
应用网关 FW	3、4、5、7
NAT FW	3、4
主机 FW	3、4、7
混合 FW	2、3、4、5、7

PIX/ASA 属于混合 FW

【返回目录】

Lesson 35 各类FW介绍

一、 包过滤 FW

- 概述：简单、利用 ACL 工作，可以过滤 IP 包、协议数据、UDP/TCP 包
- 优点：处理快、配置简单
- 缺点：不能防范应用层攻击；配置过多；不支持应用层认证
- 场景：第一道防线（边界路由器）

二、 状态 FW

- 概述：跟踪连接的状态：初始化状态、数据传输状态、终止状态。把这些状态维持在一张连接表中，数据通过时，查找这张连接表。
- 优点：弥补包过滤 FW 的缺点（单向访问）
- 缺点：不是所有协议都有状态，所以就需要模拟状态，ICMP、UDP 利用计时器来模拟；不能防范应用层攻击；不支持应用层认证
- 场景：带状态的边界路由器

有状态 ACL：自反 ACL、CBAC（Context-Based Access Control）

三、 应用网关 FW（AGF）

- 概述：又叫代理 FW，使用软件
- 分类：
  - CGF：连接网关 FW；首先截取用户连接并发给用户一个认证的请求提示，认证通过后并维持一张用户合法信息表。对用户的每个数据包进行应用层检测。安全性高，但处理速度慢。
  - CTP：又叫直通式代理；首先截取用户连接并发生给用户一个认证提示，认证通过后并维持一张合法信息表。对用户数据进行 3、4 层过滤。
- 优点：支持应用层认证和应用层检测
- 缺点：只有少数协议支持该类 FW 的触发认证：HTTP、TELNET、FTP
- 场景：

四、 NAT FW

- 概述：为了解决 IP 地址紧缺而使用 NAT
- 优点：
- 缺点：延时大、有些应用不支持 NAT
- 场景：边界路由器

五、 主机 FW

- 概述：就是在个人 PC 或服务器上安装杀毒软件或其他安全软件
- 优点：方便、易使用
- 缺点：管理困难
- 场景：个人 PC、服务器

六、 混合 FW

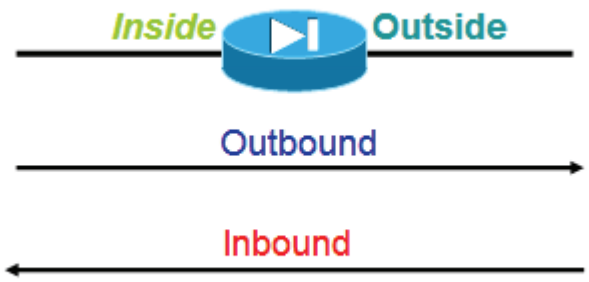
- 典型设备：PIX、ASA
- 支持功能：DHCP、VPN、IDS、IPS、URL Filtering、路由协议

【返回目录】

Lesson 36 PIX

一、 作用

- 控制介于不同网络区域流量的设备（每个接口定义一个安全级别）
- 穿过 FW 的连接分类



OutBound：从高安全级别到低安全级别

InBound：从低安全级别到高安全级别

- FW 的默认行为
  - ✧ OutBound 是允许通信的
  - ✧ InBound 是不允许通信的，需要 ACL 放通
- FW 的处理流程

OutBound → 初始化检测 → Xlate 表 → Conn 表 → ACL → Uauth 表 → 检测引擎

二、 配置文件

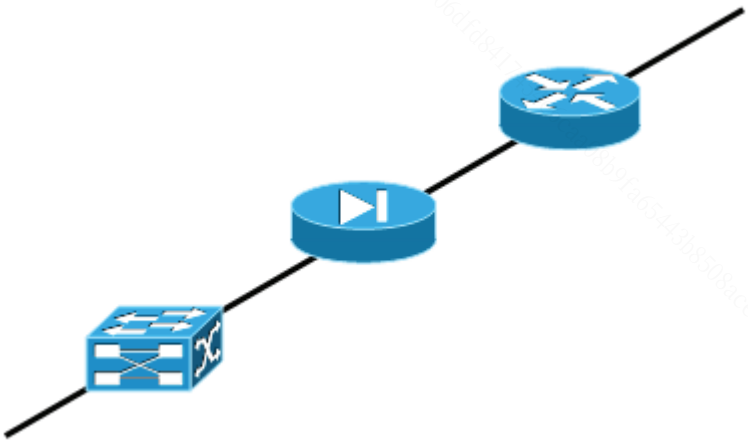
- 运行配置文件：正在运行的配置文件
- 启动配置文件：保存在 Nvram 里的配置文件，作为启动加载的

- 清除运行配置文件：clear configure all/?　　//可以清除特定的配置
- 清除启动配置文件：write erase
- 保存配置文件：write memory　　copy running-config startup-config

三、 工作模式

- 路由防火墙模式：转发数据依靠路由表，还需查找安全策略
- 透明模式：从 PIX7.0 开始，可以将 FW 作为一台二层设备，无需 IP 地址，但必须配置管理地址；维持一张 Mac 地址表；不洪泛未知单播；不支持 NAT。

四、 透明 FW 的应用场景



五、 透明 FW 的配置

- 修改模式：firewall transparent
- 配置接口：nameif *****　　security 0-100
- 管理地址：ip address a.b.c.d ……
- 其他配置：放通流量（非 TCP、UDP 流量）

- ARP 检测：防止 ARP 欺骗；ARP 默认都放通；
  - 首先手工建立一张合法 ARP 表
  - FW 检测 ARP 应答包的 IP 和 Mac 地址对应关系与合法的 ARP 表的匹配关系
  - 匹配成功则允许通过 FW
  - 匹配不成功则认为是非法的或是欺骗的 ARP，FW 丢弃之
  - 如果没有找到匹配的项，FW 的处理则依据配置来转发或丢弃，默认是洪泛的！
- ARP 配置：
  - 定义合法的 ARP 表：arp *if_name* ip mac
  - 启用 ARP 检测：arp-inspection *if_name* enable [flood/no-flood]

【返回目录】

Lesson 37 PIX 2

一、 接口安全级别相同的互访

不同接口相同级别：same-security-traffic permit **inter-interface**

相同接口相同级别：same-security-traffic permit **intra-interface**

二、 FW 的机型和硬件体系

- PIX---500 Series：

  501、506E、515E、525、535

- ASA---5500 Series：

  5505、5510、5520、5540、5550、5580-20、5580-40

- Cisco IOS Firewall： （ISR）带“8”的型号都支持

  Cisco 800、1800、2800、3800

- FWSM：

  6500/7600

- 基于 x86：受制于 PCI 总线、CPU、内存的限制
- 内嵌 Linux+web：
- 基于 ASIC：
- 基于 NP（Network Processor）：
- NP+ASIC：

三、 FW 性能指标

	PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
吞吐量	60M	100M	190M	330M	1.7G
VPN 支持	3-3.4M 10 个	15-25M 25 个	130M 2000 个	145M 2000 个	425M 2000
连接数	7500	10000	12800	280000	500000
硬件结构	1 个	2 个 10M	6 个 10/100M	支持 1000M	支持 10000M
虚拟 FW	---	---	√	√	√
FO			√	√	√

四、 ASA

- 该系列设备集成了 PIX500/IPS-4200/VPN-3000 的最新技术
- 高级防火墙服务：
- IPS 服务（AIP-SSM）：
- Anti-X 服务（CSC-SSM）：与趋势科技合作的
- IPSec/SSL-VPN：

	5505	5510	5520	5540	5550	5580-20	5580-40
吞吐量	150M	150-300M	450M	650M	1.2G	5G	10G
VPN	100M	170M	225M	325M	425M	1G	1G
并发连接	10000-25000	50000-130000	280000	400000	650000	1000000	2000000
SSL/VPN	10-25	10-250	10-750	10-2500	10-5000	10000	10000
FO	---	√	√	√	√	√	√
SSM	---	√	√	√	√	√	√
VFW	---	√	√ /20	√ /250	√ /250	√	√

FO：FailOver

VFW：Virtual Firewall

SSM：Security Service Module

ASA 支持的 SSM 的模块：

- ✧ AIP-SSM：
- ✧ CSC-SSM：
- ✧ AntiX-SSM：
- ✧ GE-SSM：

五、 Cisco IOS FW

ISR：集成多业务路由器；“全线速安全并发多业务”；2800；3800

ASR：高聚合路由器；

多业务：数据、语音、视频、安全、无线

六、 FWSM

Cisco Catalyst 6500 Switches

Cisco 7600 Routers

吞吐量达 5G、并发连接达 1000000

该服务模块没有接口，安装好这个模块后其他的设备接口默认全部为防火墙接口

七、 FW 厂商介绍

Cisco：http://www.cisco.com/

Juniper：http://www.juniper.net/

华赛：http://www.huaweisymantec.com/cn/

深信服：http://www.sinfors.com/cn/

天融信：http://www.topsec.com.cn/

趋势：http://cn.trendmicro.com/cn/home/

……

八、 PIX NAT Feature

- PIX 在 7.0 版本之前必须做 NAT
- 内存在 64M+才能安全 PIXOS 7.0+
- PIX 501、506E 只能安装 PIXOS 6.0
- 先 NAT 后 IPSec
- NAT 必需的命令：nat-control

- NAT 分类：

优先级	NAT 类型	流量分类	特性
1	Exempt NAT	Inbound Outbound	NAT0+ACL，不产生转换表
2	Policy NAT	Inbound Outbound	
3	Static NAT	Inbound	
4	PAT	Outbound	
5	Identity NAT	Outbound	NAT0，产生转换表
6	Dynamic NAT	Outbound	

配置：

Static (inside,outside) local-global-ip local-ip

Nat (inside) **1** access-list #　　//定义某个接口需要做 NAT 的条件

Global (outside) **1** interface/IP　　//定义匹配的条件转换成哪个 IP

【返回目录】

Lesson 38 虚拟FW

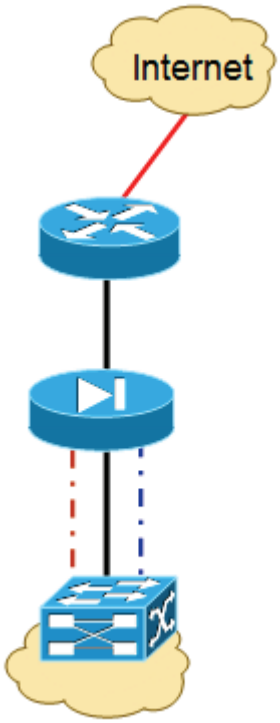
一、 概述

- 把一个防火墙虚拟成多个 FW，“security context”
- 每个 context 都拥有自己的接口、安全策略
- 为了管理 FW，管理员必需设置一个 admin context
- 当 FW 配置为 multiple 时，不支持动态路由协议，只支持静态路由，也不支持 VPN、Multicast

二、 应用场景

- 电信级应用
  - 里外接口都用子接口隔离
  - 拓扑参考

- 企业级应用
  - 共享外口，里面用子接口
  - 参考拓扑



三、 虚拟机 FW 的组织形式

- FW 支持单模式
- 在多模式下，一台 FW 中包含三种功能模块

  系统执行环境：system-config

  管理 context：admin-config

  用户 context：user-config

四、 基本配置：

- 开启多模式：**mode multiple** **//重启生效~**

当防火墙工作在多模式下，admin context 自动生成！但还需把该 context 设置成管理 context，也需为该 context 分配接口以及配置。配置文件默认保存在 **flash:/admin.cfg**

- 指定管理 Context：admin-context ***admin***
- 验证多模式：**show mode**
- 创建 Context：

changeto system //进入系统执行环境

为各个 context 分配接口，并命名接口。

context *name* //创建一个安全 context

allocate-interface *physical-interface* [*map-name*] //为特定 context 指定接口

…

Config-url url //定义 context 的配置文件存放位置

- 配置 context：

Changeto context *name*

其他的配置与真实 FW 的配置一样~!!!!!

【返回目录】

Lesson 39 AAA

一、 分析与 FW 相关的流量

- 穿过 FW 的流量
- 终止于 FW 的流量
- VPN 流量

二、 对 FW 相关的流量进行 AAA

- Authentication：who you are?
- Authorization：who you can do?
- Accounting：what you do.

三、 管理 FW 的流量

- Telnet：默认只允许内口访问
- SSH：通过配置后，允许外口访问
- Console：基本的配置通道
- HTTPS：需要 FW 具有 ASDM，且 client 需要安装 JRE

四、 基本配置

- Telnet
  - ✧ 启用：telnet 0 0 inside　　//定义允许哪些主机能 Telnet 访问 FW
  - ✧ 线路密码：passwd *******
  - ✧ Enable 密码：enable password ********
  - ✧ AAA：aaa-server 3A protocol radius/tacacs

    Aaa-server (dmz) host 192.168.x.y key ********

    Aaa authentication **telnet** console 3A/LOCAL [LOCAL]
  - ✧ 定义本地 DB：username cisco password ********

- SSH
  - ✧ 支持 Version 2
  - ✧ Hostname XiaoGe　　//配置主机名，生成密钥的材料。
  - ✧ Domain-name xiaoge.cn　　//配置域名，生成密钥时有用，有默认值的
  - ✧ Crypto key generate rsa [general-keys] modulus 1024
  - ✧ Ssh 0 0 inside/outside
  - ✧ AAA：aaa authentication **serial** console ……
  - ✧ 验证：show ssh　；　show crypto key mypubkey rsa
  - ✧ SSH 客户端登陆：Secure-CRT、Putty、路由器
  - ✧ 路由器客户端登陆：ssh –l *username* –c 3des *ip_addr*
  - ✧ SSH 默认的用户名：pix
  - ✧ SSH 默认的密码：cisco
  - ✧ 只允许 5 个 SSH 同时登陆

- HTTPS
  - ✧ 保证 ASDM 文件在 FLASH 里面
  - ✧ 启用 ASDM：asdm image flash:/asdm-603.bin
  - ✧ 启用服务：http server enable
  - ✧ 启用主机：http 0 0 inside/outside

五、　对终止 FW 的流量进行授权

- 授权内容：什么用户可以执行什么命令
- 授权方式：Tacacs+或本地 DB

六、　对穿过 FW 的流量进行 AAA

- CTP 处理
- 默认可以触发 CTP 的流量：Telnet、HTTP、HTTPS、FTP

- CTP 过程：
- CTP 配置：
  - aaa-server 3A protocol …
  - aaa-server (dmz) host …. Key ********
  - aaa authentication match *acl# if_name 3A*
  - aaa authentication include/exclude
- 其他协议的 CTP：
  - 采用 Virtual telnet 和 Virtual HTTP
  - Virtual telnet *ip_addr*
  - Virtual http *ip_addr*

七、 FW 的 ACL 下载

- Downloadable ACL：
- Cisco Radius cisco-av-pair
- IETF RADIUS Filter-id attribute (per-user)
  - 预先在 FW 上配置好 ACL
  - [011] filter-id = *acl_name* *//配置在 FW 上对应的 ACL 名字即可~*

更多配置参见《PIX Downloadable ACL》

【返回目录】

Lesson 40 防火墙系统管理与维护

一、 PIX 密码恢复

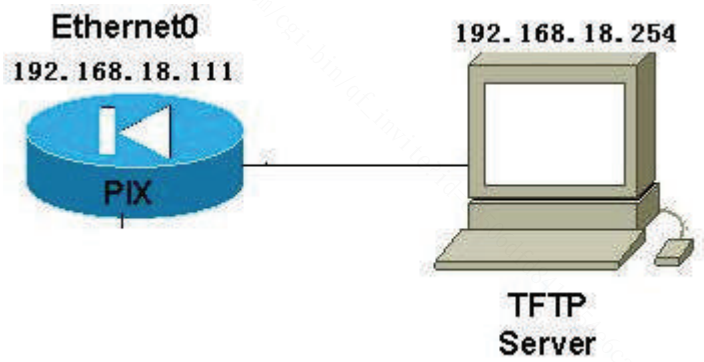
1、准备：

1）PC 一台，其上安装 TFTP 服务器

2）交叉线一条，连接 PIX 以太网口和 PC 网卡

3）下载密码恢复软件（根据 PIXOS 的版本选择不同的恢复软件），放到 TFTP 服务器的目录下

2、网络拓扑示意图



3、详细恢复过程：

启动 PIX，ctrl+breack，进入到 monitor>模式下，执行下面的操作：

monitor> interface 0

0: i8255X @ PCI(bus:0 dev:13 irq:10)

1: i8255X @ PCI(bus:0 dev:14 irq:7)

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9

monitor> address 192.168.18.111

address 192.168.18.111

monitor> server 192.168.18.254

server 192.168.18.111

monitor> file np63.bin

file np63.bin

monitor> gateway 192.168.18.254

gateway 192.168.18.254

monitor> ping 192.168.18.254

Sending 5, 100-byte 0xf8d3 ICMP Echoes to 192.168.18.254, timeout is 4 seconds:

!!!!!

Success rate is 100 percent (5/5)

monitor> **tftp**

tftp np63.bin@192.168.18.254 via 192.168.18.254.....

Received 92160 bytes

Cisco Secure PIX Firewall password tool (3.0) #0: Tue Aug 22 23:22:19 PDT 2000

Flash=i28F640J5 @ 0x300

BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] **y**

Passwords have been erased.

Rebooting....重新启动后就可以了！

4、相关软件：根据 PIX 的不同 OS 版本进行选择。

np70.bin　　#适合 PIXOS 版本为 7.0 以后的~

np50.bin

np51.bin

np52.bin

np53.bin

np60.bin

np61.bin

np62.bin

np63.bin　　#适合 PIXOS 版本为 6.3 的~

二、 ASA 密码恢复

普通的恢复类似 IOS 路由器：

进入 CONSOLE 的物理连接，重启设备

You can press the Esc (Escape) key after "Use BREAK or ESC to interrupt boot" is shown. This will take you into ROMMON mode, as follows:

rommon #0>

rommon #0> confreg

Current Configuration Register: 0x00000011

Configuration Summary: boot TFTP image, boot default image from Flash on netboot failure

Do you wish to change this configuration? y/n [n]: y

disable system configuration? y/n [n]: y

红色部分是需要键入的命令

设备接着执行，将提示：

Current Configuration Register: 0x00000040

Configuration Summary: boot ROMMON ignore system configuration

Update Config Register (0x40) in NVRAM...

这里将 0X11 启动模式转变到 0X40 模式——类似 IOS 的 0X2102 到 0X2142

rommon #1> boot

重新启动，将进入以下模式：

ciscoasa>

ciscoasa> enable

Password:<cr>

ciscoasa#

现在

ciscoasa# copy startup-config running-config 完成密码重设

Chicago# config terminal

Chicago(config)# passwd cisco123

Chicago(config)# enable password cisco123

改回启动方式

Chicago(config)# config-register 0x11

最后需要保存

Chicago(config)# copy running-config startup-config

三、 软件升级与许可

- 升级很简单：把新版本的 OS 拷贝到 FLASH 即可
- 版本分类：主版本.次版本(补丁) 7.2(2) 8.0(3)
- 许可：
  - ✧ UR：支持最大的功能
  - ✧ R：不支持 FO、有一定的功能限制
  - ✧ FO：可以参与 FO、但只能作为备份实体
  - ✧ FO-AA：可以参与 FO、而且可以作 A/A 模式，但还是作为备份实体
  - ✧ 支持 FO 的许可组合：UR-UR、UR-FO、UR-(FO-AA)

【返回目录】

Lesson 41 Failover

- **系统需求：**

硬件配置一样（内存、FLASH、Model、接口数目级型号）

软件要求：主版本和次版本一样、升级补丁可以不同；相同的操作模式

许可要求：UR、FO

UR：Unrestricted；可以支持相应硬件平台的最大值；支持 FO

R：Restricted；连接数和吞吐量不受限制；内存和接口等特性有一定的限制；不支持 FO

FO：可以参与 FO 但只能作为备份实体

FO-AA：可以参与 FO 而且支持 A/A 模式；但还是作为备份实体

- **Failover 线：**心跳线；可以传递配置信息和检测信息

专用 Cable 线（DB-15）：主次在接头上体现

LAN 线：主次基于配置上体现

FO 方式：基于 Cable、基于 LAN

FO 工作模式：A/S 主备、A/A 负载均衡

Failover Statful 线：时刻传递状态信息从主 FW 到次 FW；如 conn 信息、xlate 信息

该接口的速率必须 ≥ 用户数据接口的速率

PIX 支持专用 Cable 线

ASA 不支持专用 Cable 线

- **接口检测：**(5S)

链路 UP、Down 测试：检查网卡本身，如果没有处于 UP 状态则认为该接口出现了故障

网络 Activity 测试：测试网络的活动状态，PIX 将统计 5 秒内收到的所有的包，只

要在这个时间范围内收到任何一个包，就认为该接口正常，并停止测试，如果没有收到任何信息则进行 ARP 测试。

ARP 测试： ARP 测试将读取 PIX 的 ARP cache 中最近的 10 条记录，PIX 将以一次测试的方式向这些主机发出 ARP 查询，在每个查询过后，将等待 5 秒，如果 5 秒内有响应则说明网络正常，如果没有响应则进行下一条测试，如果所有的都没有响应，则进行 PING 测试。

广播 PING 测试： PIX 发出一个广播 PING，并统计 5 秒内是否有响应包，如果没有，再次进行 ARP 测试 。

- **Unit 检测：**

如果一个 Unit（45s）不能从 FO 线接收 hello 包，它就从自己的所有接口发送 ARP 请求，包括 FO 接口。

- **基本配置：**
  - Cable 方式：

主 FW：

Failover

Failover link state ethernet2

Failover interface ip state 10.0.0.254 255.255.255.0 standby 10.0.0.253

备 FW：

Failover

  - LAN 方式：

主 FW：

Failover

Failover lan unit primary

Failover lan interface state ethernet2

Failover lan enable

Failover link state ethernet2

Failover interface ip state 10.0.0.254 255.255.255.0 standby 10.0.0.253

AA 模式的附加配置：

Failover group 1

Preempt

Failover group 2

Secondary

Preempt

备 FW：

Failover

Failover lan unit secondary

Failover lan interface state ethernet2

Failover lan enable

Failover link state ethernet2

Failover interface ip state 10.0.0.254 255.255.255.0 standby 10.0.0.253

测试：

1. 分别配置好主备 FW，并保存。
2. 重启备 FW，如果没出错，备 FW 启动后会被主 FW 同步。
3. 重启主 FW，这时备 FW 会变成主 FW。
4. 主 FW 启动后，不会再变成主 FW 了（除非配置了抢占）。
5. show failover

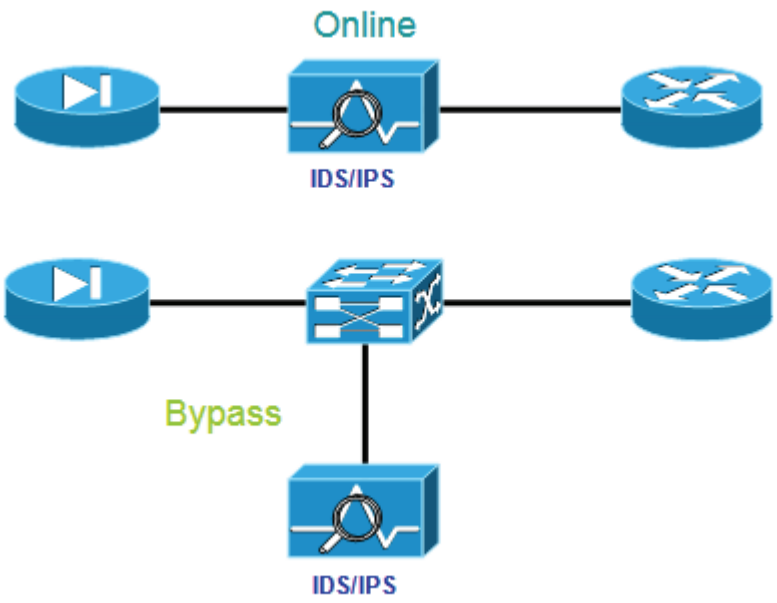
高级配置：

Failover key ******** //密码 failover polltime *** //hello 包的间隔时间

【返回目录】

Lesson 42 PIX ACL、IDS/IPS

一、 应用场景



二、 FW-ACL

- 标准、扩展 ACL：
- 动态 ACL：
- 自反 ACL：
- CBAC：基于上下文的访问控制
- 时间 ACL：周期性时间、绝对性时间
- Turbo ACL：Cisco 7200、7500、12000、PIX 支持

  启用：access-list compiled

ACL 工具：object-group

用于对主机、网络、协议和服务进行归纳，简化配置

Object-group network/protocol/service *name*

Network-object 10.0.0.0 255.255.255.0

……

Access-list # permit ip object-group *name* object-group *name*

查看：show access-list

三、 FW-IDS

- 防火墙内嵌的 IDS 是一个限制版本的 IDS
- 和路由器上的 IDS 类似
- 支持 51 个 signature
- Signature 分类：

  Info：简单的探测，或是威胁很小的攻击。

  Attack：威胁很大的攻击、对网络造成了实际的威胁。

- 配置 IDS：

  Ip audit name *bluefox* attack action alarm drop reset

  Ip audit name bluefox2 info action alarm

  Ip audit interface inside *bluefox*

  Ip audit interface inside bluefox2

  查看 signature：show ip audit count

  关闭特定的 signature：ip audit signature 2004 disable

- 配置 LOGGING：

  Logging enable

  Logging trap debugging

  Logging host dmz 192.168.1.8

  Logging buffered 0-7

- 安装 SYSLOG 服务器：

  下载安装 Kiwi_Syslogd_8.3.30.setup.exe 后，启动就 OK 了。

四、 IDS、IPS

三要素：触发器、监控位置、入侵检测响应技术

基于主机：Cisco CSA

基于硬件：Cisco 4200 Series；4215、4235、4240

- 检测：（触发器）
  - 异常检测
  - 滥用检测
  - 协议分析

- 响应技术：
  - TCP 拦截
  - IP 拦阻
  - 记录
  - 访问限制

- 通信协议：
  - SSH
  - TLS/SSL
  - RDEP
  - SDEE Standard
  - FW 只能通过 SYSLOG 形式发送

- 硬件
  - Cisco IDS 4200 Series
  - Cisco 6500 Module
  - Cisco Module for Router
  - Cisco Router IOS
  - Cisco Firewall

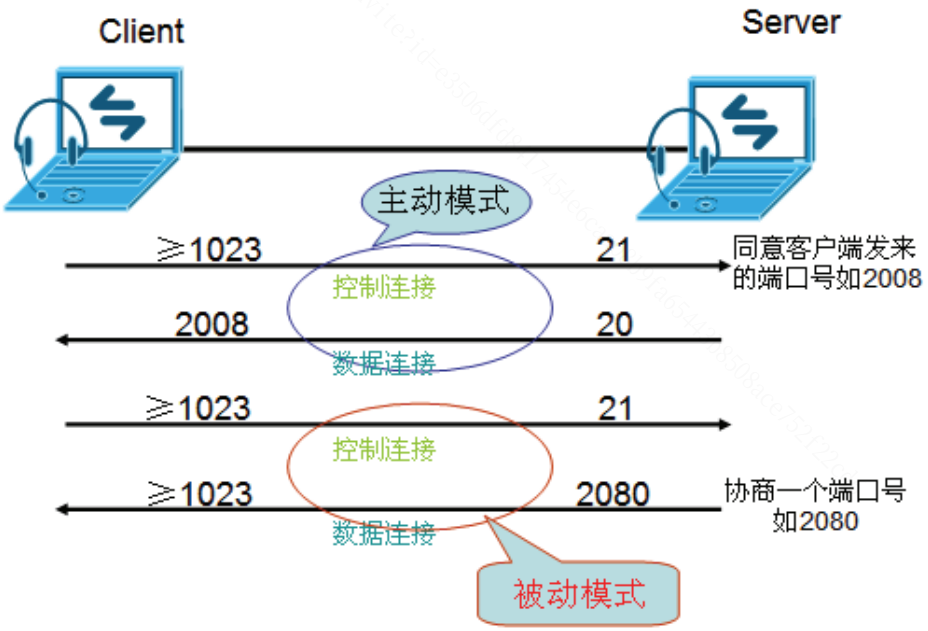
【返回目录】

Lesson 43 FTP 工作模式

控制连接：用来协商一些控制指令

数据连接：用来传输数据

FTP 深度检测：默认已经开启



【返回目录】

VPN Technology

Lesson 44 VPN

一、 广域网

- **专线技术**
  - 优点：安全、稳定、带宽高、易实现和易维护
  - 缺点：成本高、移动性差、覆盖范围有一定的局限性
- **拨号技术**
  - 优点：费用低、覆盖范围广、移动性强、具有一定的安全性
  - 缺点：低带宽、质量差、不稳定、配置复杂
- **分组交换技术**
  - 优点：费用低、扩展性强
  - 缺点：带宽有限、移动性差、安全性一般、配置与维护复杂
- **Internet 业务传输技术**
  - 优点：费用低、移动性强、覆盖范围广、带宽灵活
  - 缺点：容易受攻击（窃听攻击、伪装攻击、中间人攻击）

二、 常见攻击

- **窃听攻击：**
  - 传输中，数据包中的内容被人非法查看
  - 协议分析可以作为窃听的工具
  - 可以采用 OTP、SSL、VPN 等加密方式进行保护

链路加密：整个数据帧在两个设备之间被加密；主要用于 PPP/HDLC 链路环境

数据包负荷加密：只对数据包的负荷加密，这种加密的数据可以被路由，典型代表为 VPN。

- **伪装攻击：**
  - 往往通过隐藏自己的身份或冒充别人的身份来进行非授权的访问或发起 DoS 攻击
  - 通过改变数据包中的源地址信息来实现
  - 通常的解决方案是使用一个通过散列函数来实现数据包的完整性。散列函数允许用户验证传输的数据包的源。
  - VPN 中，最通常使用的散列函数是 MD5 和 SHA-1

- **中间人攻击：**
  - 会话重放攻击
  - 会话截取攻击
  - ARP 攻击和 TCP 会话截获等均属于中间人攻击，可以使用防火墙来随机化 TCP 序号。防止 TCP 会话截获最好使用 VPN。

三、 VPN

- **什么是 VPN？**
  - 实质上就是一种受保护的连接
  - 主要用于穿越公网的环境，内网也可以使用

- **VPN 的作用**
  - 使用加密技术防止数据包被窃听
  - 使用数据包完整性检验防止数据包被修改
  - 使用认证机制防止中间人攻击
  - 使用序列号防止回放攻击
  - 定义数据包如何被封装保护及如何传输
  - 定义被保护的数据流

- **VPN 的功能组件**
  - 验证
  - 封装
  - 数据加密
  - 数据包的完整性
  - 密钥管理
  - 抗抵赖性
  - 应用程序和协议的支持
  - 地址的管理

- **VPN 的基本连接模式**
  - 传输模式：
    - 设备的真正源 IP 和目标 IP 之间传输数据时使用
    - 端---端 VPN
    - 仅仅保护分组的有效载荷，原始 IP 头部保持原状
  - 隧道模式：
    - 传输模式的限制是不具备很好的扩展性的
    - 隧道模式的扩展性强

- **VPN 的类型**

  根据参与 VPN 连接实体的不同
  - 站点---站点
    - 通常也被称为局域网到局域网 VPN
    - 在 VPN 网关之间使用隧道模式来保护 VPN 流量
    - 这种保护对站点内的终端是透明的
  - 远程访问客户端
    - 通常用于一台单用户设备、一个硬件客户端和 VPN 网关之间的低带宽或

宽带连接的 VPN 的应用

- 防火墙 VPN
  - 本质上是一个带有增强的安全防火墙功能的 L2L 或远程访问 VPN
- 用户---用户 VPN
  - 就是两台设备之间的传输模式的 VPN 连接

根据 VPN 应用环境的不同

- Intranet
  - 通过公司内网建立的 VPN 连接
- Extranet
  - 公司合作伙伴之间的 VPN 连接
- Internet
  - 使用公网作为骨干建立的 VPN 连接

根据 VPN 连接实现技术的不同

- **GRE：通用路由封装**
  - 是一个工作在第 3 层的封装协议，使得其他协议的数据可以封装在 IP 数据包中，并且将封装后的数据包通过 IP 骨干网传输
  - 在所有具备 VPN 功能的产品中，目前只有 IOS 路由器支持 GRE
  - 不具备加密、完整性检查、身份验证等功能

- **IPSec：IP Security**
  - 三层协议，特别设计用来处理在非安全的网络上传输敏感的数据
  - 核心功能：数据机密性、数据完整性、数据验证
  - 缺点：只支持 TCP/IP 协议、不支持组播广播流量

- **PPTP：Point-2-Point Tunnel Protocol**
  - 点---点隧道协议、二层协议
  - 最早由微软开发的一种基于 Windows 系统的 VPN 解决方案
  - 配置简单、但安全性不高

- **L2TP：Layer 2 Tunnel Protocol**
  - 第二层隧道协议，兼容性强
  - 是 Cisco 和微软半开放标准的组合，目的是为了提供替代 IPSec 的更好的、应用于小型的基于 WindowsPC 环境的多厂商兼容的 VPN 解决方案。
  - 配置简单、安全性不高

- **SSL：Secure Socket Layer**
  - 安全套接字层协议
  - 保护应用层 HTTP 数据
  - 不需要专门的客户端
  - 使用浏览器就可以登陆

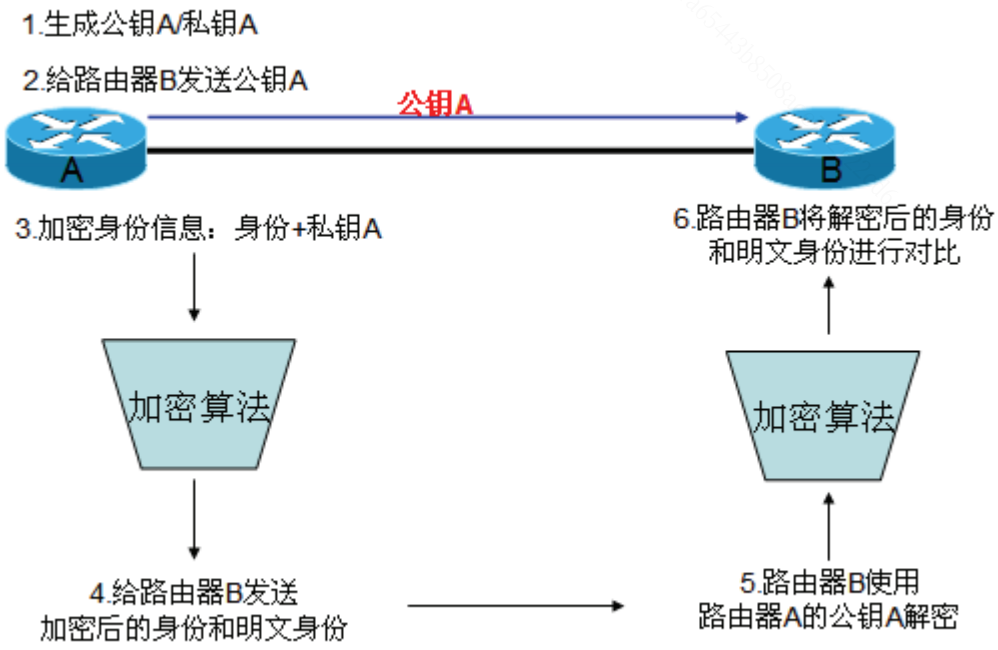
- **MPLS：MultiProtocol Label Switch**
  - 多标签协议转发协议

【返回目录】

Lesson 45 VPN技术

一、 密钥

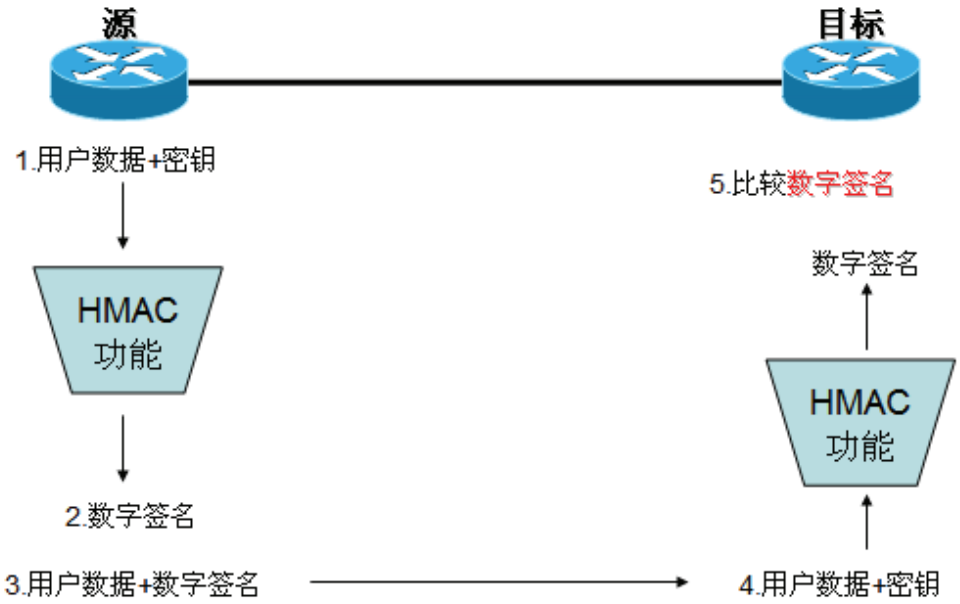
- **对称密钥**：使用同一把钥匙对信息提供安全的保护
  - 预共享密钥：在带外确定两台设备之间的预共享密钥
  - 使用一个安全连接：可以使用一个现有安全的、受保护的连接传送密钥
- **非对称密钥**：使用两把钥匙对信息提供安全的保护
  - 私钥：被自己收藏，永远不共享给其他设备，用来解密数据包的密钥
  - 公钥：传递给对方，对方用这个公钥加密数据
  - 标准、算法
    - RSA 公钥
    - DSA 数字签名算法
    - Diffie-Hellman（DH）
    - KEA 密钥交换算法
  - 提供的安全功能：
    - 加密：使用对方共享的公钥加密，对方使用自己的私钥解密
    - 验证：



二、 加密

- **加密算法：**
  - DES：数据加密标准
  - 3DES：增强型 DES 标准
  - AES：先进的加密标准

三、 数据包验证

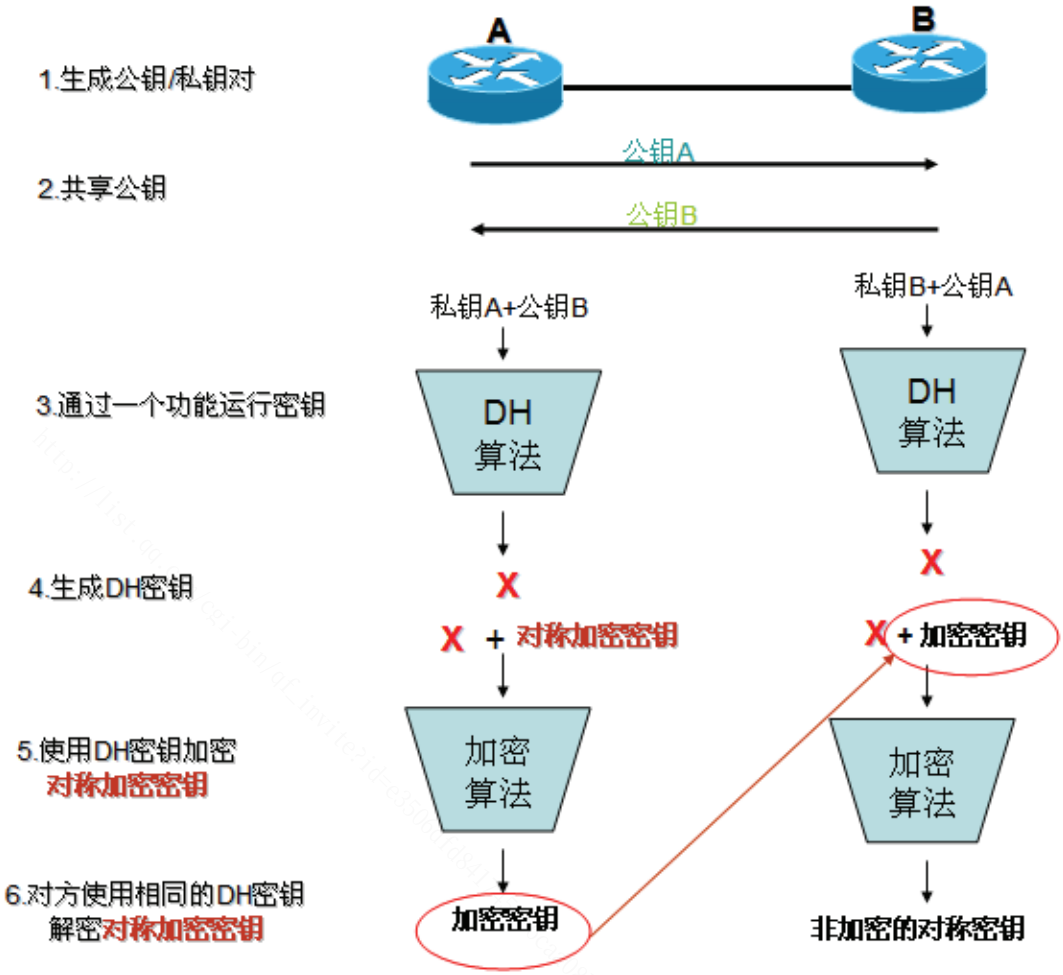


- MD5 HMAC 功能
  - 在 1994 年由 Ronald Rivest 开发的。MD5 创建一个 128 位的签名
- SHA HMAC 功能
  - 是由 NIST 开发的，SHA-1 产生一个 160 位的签名

四、 密钥交换

- 预共享的密钥
- 使用一个已经加密的连接
- 使用非对称密钥算法加密密钥

- Diffie-Hellman



五、 验证方法

- 设备验证
  - *预共享对称密钥*

    在对等体之间带外共享密钥，使用加密算法或 HMAC 功能来作验证

  - *预共享非对称密钥*

    1. 每个对等体产生一个公钥/私钥，并通过带外把公钥共享
    2. 使用对方的公钥加密，对方收到数据后使用自己的私钥解密

  - *数字证书*

1. 包含有 VPN 对等体设备的身份信息、公钥以及基于私钥产生的签名，因此唯一的代表了 VPN 连接中的设备
2. 数字证书不需要预先共享，只有在建立 VPN 连接时、需要身份认证时才需要对方的证书
3. 为保证数字证书的合法性，这个证书往往由一个被信任的第三方设备提供
4. 采用数字证书来实现身份认证可以帮助用户减少配置量
5. CA：证书颁发机构；是一个被所有想使用证书的 VPN 设备所信任的一台设备。能核实设备的身份和能产生、验证、删除证书
6. 组件与标准
   a) CA
   b) PKI：
   c) PKCS#10：定义设备向 CA 发出证书请求时所提交的信息以及格式信息的内容：
      - ✧ CN：设备的名字或者身份；必须的
      - ✧ O：设备所属的公司名称，可选的
      - ✧ L：设备所位于的城市，可选的
      - ✧ SP：设备所位于的省份，可选的
      - ✧ FQDN：设备的完全域名，可选的
      - ✧ E-mail：负责这台设备人员的 Email，可选的
      - ✧ 密钥大小：用于建立公钥/私钥对的密钥大小，必须的，取值：512、768、1024、2048 等，默认 512
      - ✧ 公钥：该设备的公钥，必须的
      - ✧ 随机数口令：CA 验证一台设备的证书请求或注销的口令
      - ✧ 带内：PKCS#10 信息直接通过网络发送给 CA。如果 CA 被配置为自动产生证书，它会产生证书并把它回送给请求者。
      - ✧ 带外：PKCS#10 的信息通过其他媒介的形式发送给 CA 管理员。
   d) X.509V3
      i. 定义 CA 产生证书的内容以及过程
      ii. 对收到的证书请求消息验证

iii. 产生证书：

e) PKCS#7

i. 定义 CA 返回给设备证书的内容以及格式

f) SCEP：

i. 简单证书注册协议

ii. 带内实现设备与 CA 之间的信息交互的一种协议

g) CRL：

i. 吊销证书列表

ii. 原因：有效期到期、安全参数改变、其他

- 用户验证

i. Xauth

【返回目录】

Lesson 46 IPSEC/VPN技术

一、 IPSec 的基本概述

- 专用于在不安全网络安全地承载数据而开发的协议
- 它是安全的协议、IETF 标准、支持 TCP/IP、不支持组播广播
- 功能：数据加密、数据包完整性检验、身份验证、抗回放攻击

二、 IPSec 的标准

- RFC2401：定义 IPSec 的整体框架
- RFC2402：定义 AH
- RFC2403：定义 MD5
- RFC2404：定义 SHA
- RFC2405：定义 DES
- RFC2406：定义 ESP
- RFC2407，08，09：定义 ISAKMP/IKE
- ISAKMP：Internet Security Associte Key Protocol
- IKE：Internet Key Exchange
- 管理连接：ISAKMP/IKE 阶段一
- 数据连接：ISAKMP/IKE 阶段二

三、 IPSec/VPN 建立的基本步骤

- 触发 IPSec：定义感兴趣流量
- 使用 ISAKMP/IKE 来建立管理连接和身份验证
- 建立数据连接
- 基于数据连接安全传输数据，实现加密、数据包完整性检验
- 生存周期到期尝试重新建立 VPN 连接

四、 IPSec 的安全参数

- **SA：安全关联**
  - 一组（所有）安全参数的集合
  - 加密算法与对称密钥
  - HMAC 与对称密钥
  - 连接的生存周期
  - DH 密钥组
  - 设备验证类型
  - 封装协议
  - SPI
  - 受保护的流量

五、 管理连接与数据连接的安全参数

a) 通过加密 ACL 所定义的感兴趣流量

b) 协商安全参数建立管理连接

i. 采用何种验证方法

ii. 采用何种加密算法和 HMAC 算法

iii. 采用何种 DH 密钥组

iv. 采用何种工作模式：主模式（思科默认）、积极模式（深信服默认）

v. 生存周期

c) 协商安全参数，建立数据连接

i. 何种安全封装：ESP、AH

ii. 何种连接模式：隧道模式、传输模式

iii. 生存周期

iv. 何种加密算法

v. 何种散列函数

vi. 共享密钥的方法：DH/管理连接

六、 IPSec/VPN 连接的建立过程

a) 站点---站点 VPN

i. VPN 网关触发一个 VPN 连接

ii. 开始协商用于管理连接的安全参数

iii. 使用 DH 共享密钥

iv. 管理连接建立成功并开始进行身份验证

v. 身份验证成功，开始阶段二的工作，协商数据连接

vi. 数据连接一旦建立，开始安全传输数据

vii. 生存周期到期，重新建立连接

b) 远程访问 VPN

i. 用户验证

ii. 自动下发策略：IP 地址、隧道分离、DNS 分离

iii. 反向路由注入

c) EzVPN

i. IP 地址下发

ii. 连接类型：客户模式、局域网扩展模式

iii. 分离隧道：

iv. 防火墙策略：

v. 分离 DNS：

七、 ISAKMP/IKE 阶段二

a) 主要任务：建立安全数据连接，提供数据保护

b) 工作模式：快速模式；协商安全参数以及（交互安全参数所需的）密钥

c) 封装协议：

	IP 协议号	NAT 支持度	加密内容	应用场景
AH	51	不支持 N/P(AT)	不对数据加密	内网
ESP	50	支持 NAT	对数据加密	外网

八、 每个阶段经过的状态变化

a) 阶段一

i. 主模式：Main Mode

1. MM_NO_STATE：SA 建立好了，安全策略还没有协商好
2. MM_SA_SETUP：安全参数已经协商好了
3. MM_KEY_EXCH：发生了 DH 交换并产生吧 KDH
4. MM_KEY_AUTH：成功完成了对等体的认证。标志阶段一完成。

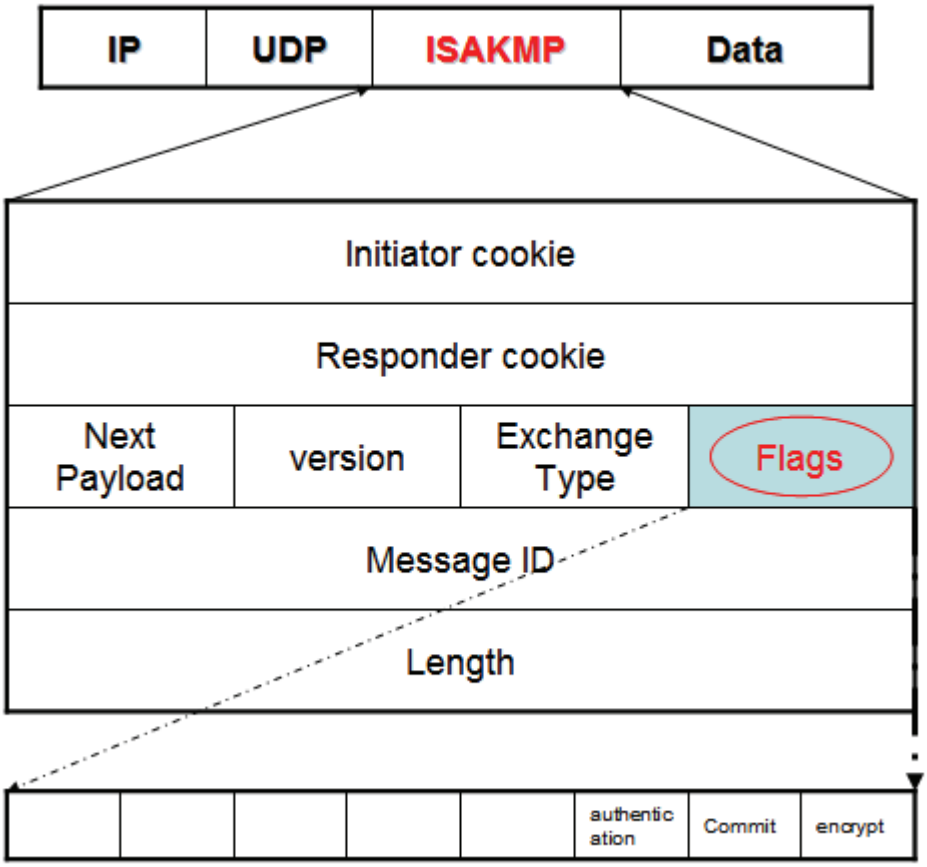
ii. 积极模式：Aggressive Mode

1. AG_NO_STATE：SA 已经建立，安全参数还没有协商好
2. AG_INIT_EXCH：成功协商好安全参数，并发生了 DH 交换和 KDH
3. AG_AUTH：完成对等体的认证。标志阶段一完成。

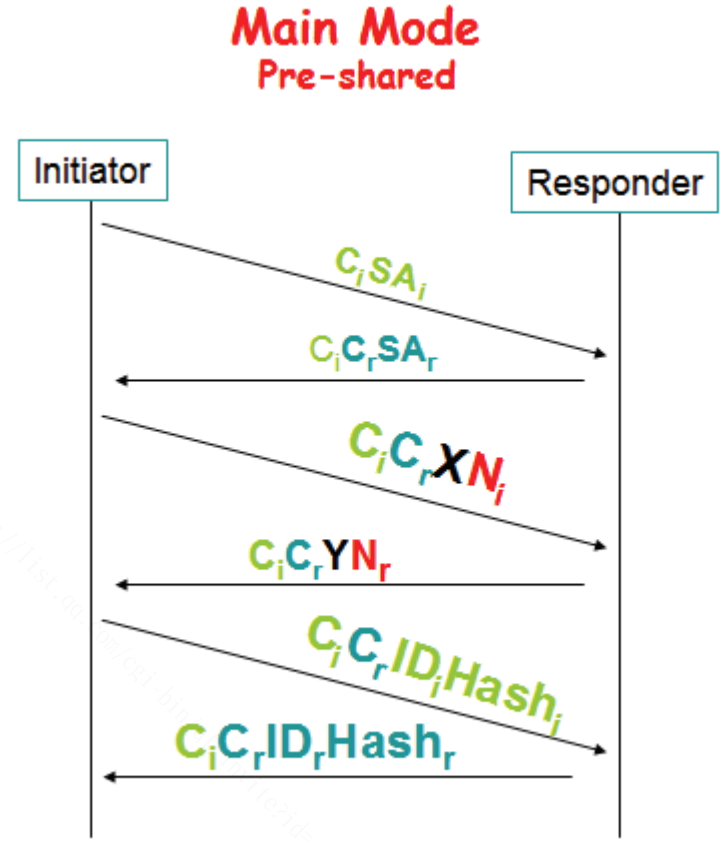
b) 阶段二：Quick Mode

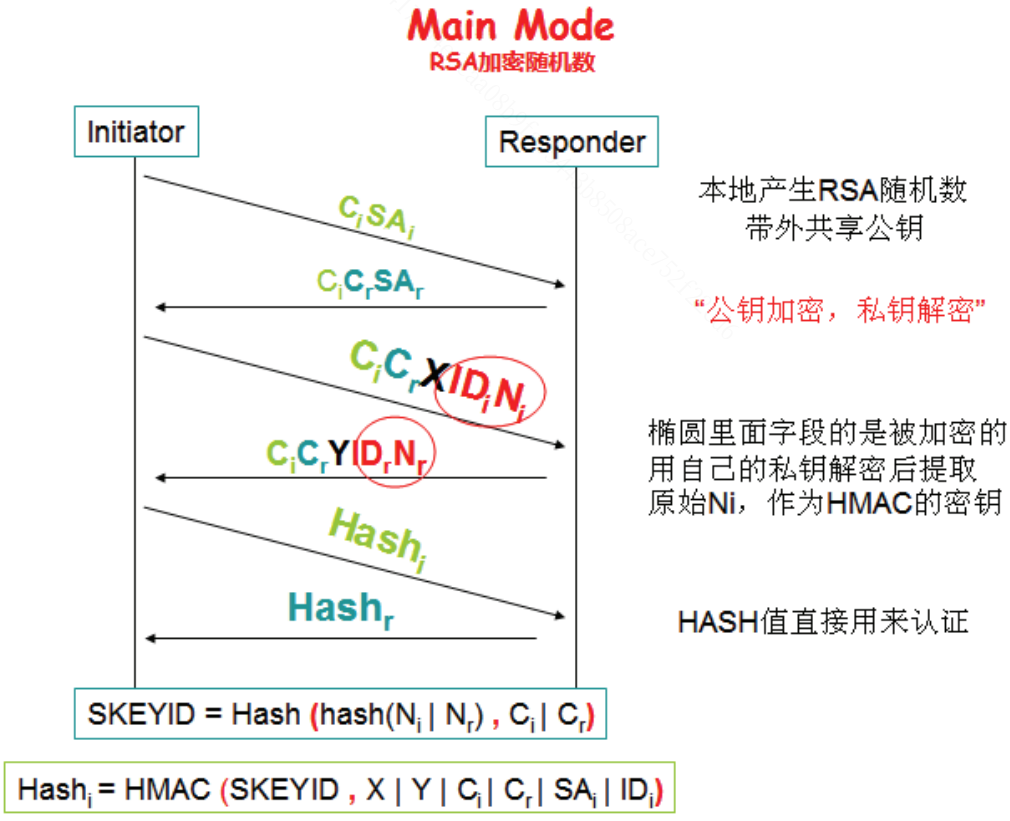
i. QM_IDLE：完成了阶段一，开始或者已经结束阶段二。

九、 数据结构的分析

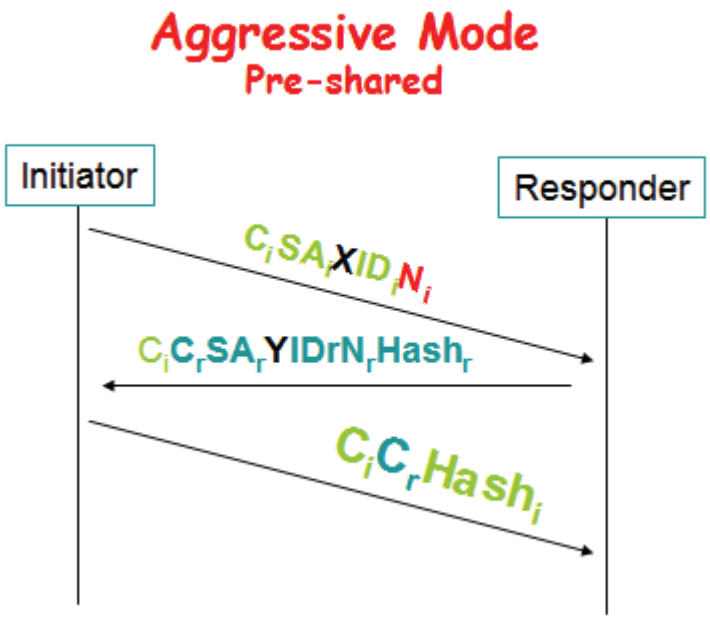


- 阶段一具体的协议过程
  - 主模式

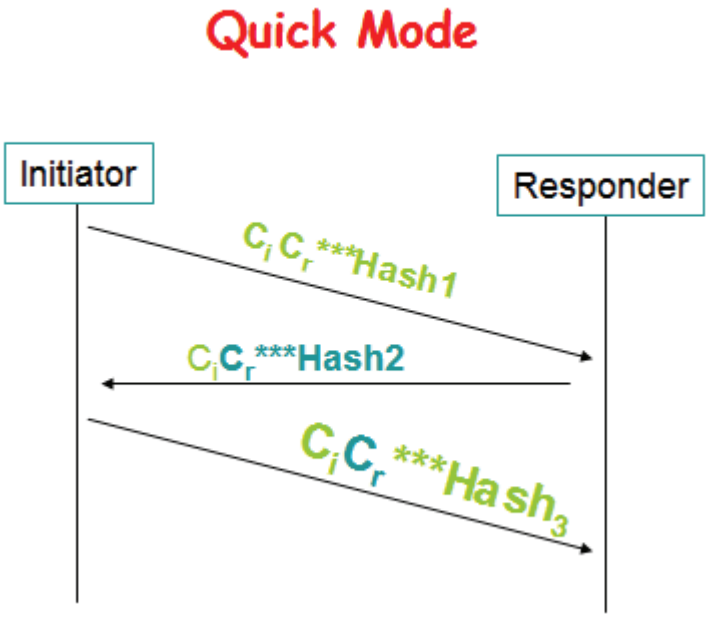




- 积极模式



- **阶段二具体的建立**
  - 任务：建立 IPSec-SA 并协商 SP、为数据传输生成密钥



KEYMAT （no PFS）= PRF (SKEYID_d ， protocol | SPI | Ni | Nr)

KEYMAT (with PFS) = PRF (SKEYID_d ， QM_key | protocol | SPI | Ni | Nr

- **SKEYID 的计算**
  - Pre-shared 认证
    - KDH：由 DH 产生
    - SKEYID = PRF（‘pre-shared’ ， Ni | Nr）
    - SKEYID_d = PRF （SKEYID ， KDH | Ci | Cr |0）
    - SKEYID_a = PRF （SKEYID ， SKEYID_d | KDH | Ci | Cr |1）
    - SKEYID_e = PRF （SKEYID ， SKEYID_a | KDH | Ci | Cr |2）
    - a，authentication：验证数据包的完整性
    - e，encryption：加密数据
    - d，datum：作为第二阶段的材料
  - RSA 随机数认证
    - SKEYID = PRF （hash(Ni | Nr) ， Ci | Cr）
    - Hash_i = HMAC_Hash (SKEYID , X | Y | Ci | Cr | SAi | IDi)

十、 IPSec 的发展

a) 1995：RFC1825---1829

b) 1998：RFC2401---2412

c) 2005：RFC4301---4309

【返回目录】

Lesson 47 IPSEC/VPN配置步骤

一、 配置阶段一策略

a) 认证

b) 加密算法

c) Hash

d) DH 组

e) 生命周期

二、 配置设备认证的参数

a) ID

b) Pre-shared、公钥、证书

三、 配置阶段二策略

a) 安全协议

b) 加密算法

c) Hash 算法

d) 工作模式

四、 定义感兴趣流量

a) ACL

五、 配置加密图

a) 绑定所有 IPSec 策略，还有其他功能的启用

b) PFS；Perfect Forward Secrecy

i. 在阶段二再一次发生 DH 交换

六、 接口绑定加密图

a) Int s1/0

b) Crypto map *****

七、 测试 IPSec 的连接

a) Show crypto engine connections active

b) Debug crypto isakmp

c) Debug crypto ipsec

d) Clear crypto sa

e) Clear crypto sessions

【返回目录】

Lesson 48 IPSEC/VPN与NAT

一、 NAT 的作用

- 解决 Ipv4 地址的紧张

- 保护内网

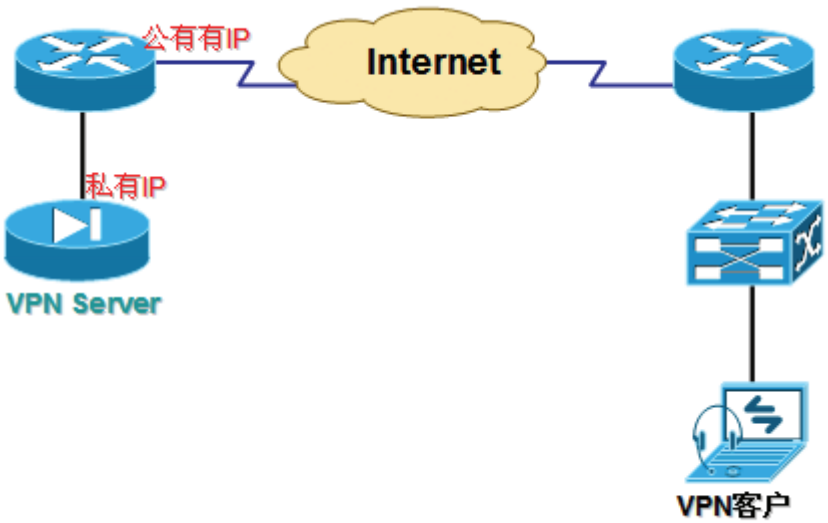
二、 NAT 与 IPSec 的部署

- NAT 设备放在 IPSec 设备之前
- NAT 设备和 IPSec 设备是同一台设备
- AH Tunnel 和 AH Translation 都不支持 NAT 和 PAT

三、 NAT 与 IPSec 在同一台设备

- 处理顺序：先 NAT 后 IPSec
- 路由器的配置：两个 ACL
  - NAT：access-list 100 deny IPSec 流量　　access-list 100 permit 内网 any
  - IPSec：access-list 120 permit 内网 内网
- 防火墙的配置：
  - 排除 NAT：nat 0 acl*

四、 IPSec 设备在 NAT 设备之后



必须在路由器上作静态映射，如 ISAKMP 的 500 端口

五、 IPSec 流量穿越 NAT 设备

- ISAKMP 协议兼容 NAT、PAT
- 用户数据分析：
  - ESP Tunnel：支持 NAT，不支持 PAT
  - ESP Translation：不支持 NAT 和 PAT

六、 如何使 ESP Tunnel 来支持 PAT

- 解决方案：
- 设备启用 NAT-T 特性之前做的三件事情
  1. 首先双方通告自己支持 NAT-T 特性。（第一包和第二包）
     - 用 Vendor ID 字段表示自己支持 NAT-T 特性
  2. 检测设备间是否有 NAT-T 设备（第三包和第四包）
     - 用 NAT-Discovery 字段
  3. 启用 NAT-T 特性
     a) 把 UDP 500 改为 4500
     b) ESP 头部与新 IP 间加个 UDP 头部（4500，4500）

【后记】

此文档当中的 VRRP 和 GLBP 的资料来源于网络，仅供学习使用~

此文档作为自己学习笔记的总结和备份~

此文档献给网络爱好者和喜欢蓝狐的兄弟姐妹们~

此文档也为上课没有做好笔记的同学提供参考~

更希望大家能通过蓝狐的平台不仅在技术上有所提高，其他方面也应有所提高~

【关于作者】

偶的网名叫（疯狂的）小格，QQ：844978372，欢迎网络爱好者加偶。

2003-2007 .在湖南农业大学就读动植物检疫专业

2007.5-7 .参加在长沙蓝狐网络技术培训学校中级班 57 期

2007.9-2008.4.在浙江普通服务市场有限公司任职网络工程师

2008.4-9 .参加长沙蓝狐网络技术培训学校高级班 24 期

2008.8 .第一次独立完成了一个小规模的网络工程

2008.9 .开始找工作

通过这几个月的学习，对网络有了比较深刻的认识，也以最好的心态和状态完成了学习，并得到了广大讲师和学友们的认可，在此感谢你们陪我走过的这些日子。

感谢蓝狐这个网络平台，让我们学到了很多实用的网络技术和很多非技术性的东东，为我们走向社会和在社会上立足打下了坚实的基础，也结识了更多为之奋斗的新朋友。希望大家在网络的道路上走的更高、更远！

【返回首页】

Bluefox-T24-XiaoGe

2008-09-01

QQ：844978372