

Cisco Router Configuration Answers!

Certified Tech Support



Cisco

路由器配置疑难解析

(美) Glenn Lepore (CCNA) 等著
 Tony Costa (CCIE,CCSI)
 余志洪 王晓茹 译

技术支持，唾手可得

- 省时——无需等待便可获得技术支持
- 省力——为您解答Cisco路由器配置中遇到的各种问题
- 快速查找——分类编排，便于查找
- 权威——问题解答来自专门从事IT技术开发和研究的技术支持公司：Syngress Media



Cisco 路由器配置 疑难解析

Glenn Lepore (CCNA)
(美) Tony Costa (CCIE, CCSI) 等著
余志洪 王晓茹 译



机械工业出版社
China Machine Press

Cisco路由器应用广泛,并拥有强大的市场占有率。本书精心设计了数百个最常见的路由和交换问题,且给出了详细的解答。全书分12章,讲述了Cisco系统支持的所有IP路由协议,包括RIP、OSPF、IGRP、EIGRP、BGP、EGP和IP组播等。本书还在文中设置了注意、提示和警告,可以帮助读者更好地掌握Cisco路由器的配置技术。

本书是Cisco用户以及Cisco路由器管理和配置人员的必备参考,也是初级和中级学者们的良师益友。

Glenn Lepore,Tony Costa et al: Cisco Router Configuration Answers! Certified Tech Support.

Original edition copyright ©1999 by McGraw-Hill.All rights reserved.

Chinese edition copyright ©2000 by China Machine Press.All rights reserved.

本书中文简体字版由美国麦格劳-希尔公司授权机械工业出版社独家出版。未经出版者书面许可,不得以任何方式复制或抄袭本书内容。

版权所有,侵权必究。

本书版权登记号:图字:01-2000-0579

图书在版编目(CIP)数据

Cisco路由器配置疑难解析/(美)利波尔(Lepore,G.)等著;余志洪,王晓茹译.

-北京:机械工业出版社,2000.4

书名原文: Cisco Router Configuration Answers! Certified Tech Support

ISBN 7-111-07933-7

I. C... II. ①利...②余...③王... III. 计算机网络-路由器配置 IV. TP393

中国版本图书馆CIP数据核字(2000)第15346号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑:瞿静华

北京忠信诚胶印厂印刷·新华书店北京发行所发行

2000年4月第1版第1次印刷

787mm×1092mm1/16·12.75印张

印数:0 001-7 000册

定价:28.00元



凡购本书,如有缺页、倒页、脱页,由本社发行部调换

Cisco 路由器配置快速解答

配置IP

要 完 成	完 成
配置一个WAN服务	在接口指定配置模式下使用ENCAPSULATION命令
为WAN通信创建一个子接口	在全局或接口指定配置模式下使用INTERFACE命令；选择一个点到点或点到多点子接口
向一个接口分配IP地址	在接口或子接口指定配置模式下使用IP ADDRESS命令
向一个接口分配第二个地址	在接口或子接口指定配置模式下使用带SECONDARY关键字的IP ADDRESS命令
配置一条静态路由	在全局配置模式下使用IP ROUTE命令
配置一条缺省路由	在全局配置模式下使用IP DEFAULT-NETWORK命令

配置IP路由协议

要 完 成	完 成
配置RIP路由	在全局配置模式下使用ROUTER RIP命令启动RIP路由协议
选择参加RIP路由进程的接口	在指定路由协议配置模式下使用NETWORK命令
配置OSPF路由协议	在全局配置模式下使用ROUTER OSPF命令启动一个OSPF路由进程
选择一个或多个接口加入OSPF域	在指定路由协议配置模式下使用NETWORK AREA命令进行配置；使用通配符在一个命令行选择多个接口
在ABR上汇总OSPF路由	在指定路由协议配置模式下使用AREA RANGE命令
在ASBR上汇总OSPF路由	在指定路由协议配置模式下使用SUMMARY-ADDRESS命令
配置EIGRP路由	使用ROUTER EIGRP命令在一个自治系统内启动一个EIGRP路由进程
选择参加EIGRP路由进程的接口	在指定路由协议配置模式下使用NETWORK命令
在任何EIGRP路由器上汇总路由	在指定接口模式下使用IP SUMMARY-ADDRESS命令进行配置
启动BGP路由进程	在全局配置模式下使用ROUTER BGP命令进行配置
与一个内部或外部对等节点开始BGP寻路	在指定路由协议配置模式下使用NEIGHBOR REMOTE-AS命令
使一条路由有资格向一个BGP对等节点通告	使用NETWORK命令与当前IP转发表格中的任何路由匹配
向一个BGP对等节点有条件地通告汇总路由	在指定路由协议配置模式下输入AGGREGATE-ADDRESS命令

配置路由协议独立特征

要 完 成	完 成
在源和目的协议之间再分配路由信息	在指定路由协议配置模式下为目的协议使用REDISTRIBUTE命令
过滤接口接收到的或发送出去的路由	在接收或发送接口上的指定接口配置模式下配置DISTRIBUTE-LIST命令
过滤路由协议之间交换的路由	在路由协议配置模式下为目的协议输入DISTRIBUTE-LIST命令
在一个接口上禁止路由更新	在指定路由协议配置模式下使用PASSIVE-INTERFACE命令
在一个接口或子接口上启动水平分割	在指定接口或子接口配置模式下输入IP SPLIT-HORIZON命令
在一个接口或子接口上禁止水平分割	在指定接口或子接口配置模式下配置NO IP SPLIT-HORIZON命令

m/64/3107

Cisco 路由器配置快速解答

配置IOS			
要 完 成	在全局配置模式下使用该命令	在指定路由协议配置模式下使用该命令	在指定接口配置下使用该命令
配置一个WAN服务为WAN通信创建一个子接口	INTERFACE <i>type number</i> . <i>sub-if [point-to-point point-to-multipoint]</i>		ENCAPSULATION <i>protocol</i> INTERFACE <i>type number</i> . <i>sub-if [point-to-point point-to-multipoint]</i> IP ADDRESS <i>addressmask</i>
向一个接口分配IP地址			
向一个接口分配第二个地址			IP ADDRESS <i>address mask</i> SECONDARY
配置一条静态路由	IP ROUTE <i>address mask type number</i>		
配置一条缺省路由	IP DEFAULT-NETWORK <i>address</i>		
配置RIP路由和选择接口	ROUTER RIP	NETWORK <i>address</i>	
配置OSPF路由协议和选择接口	ROUTER OSPF <i>process-id</i>	NETWORK <i>address</i> AREA <i>area-id</i> AREA <i>area-id</i> RANGE <i>address address</i> SUMMARY-ADDRESS <i>address</i>	
在ABR上汇总OSPF路由			
在ASBR上汇总OSPF路由			
配置EIGRP路由和选择接口	ROUTER EIGRP <i>autonomous-system</i>	NETWORK <i>address</i>	
在任何EIGRP路由器上汇总路由			IP SUMMARY-ADDRESS <i>EIGRP autonomous-system address mask</i>
启动BGP路由进程	ROUTER BGP <i>autonomous-system</i>		
与一个内部或外部对等节点开始进行BGP寻路		NEIGHBOR <i>address</i> REMOTE-AS <i>autonomous-system</i> NETWORK <i>address mask</i>	
使一条路由有资格向一个BGP对等节点通告			
向一个BGP对等节点有条件地通告汇总路由		AGGREGATE-ADDRESS <i>address mask</i>	
在源和目的协议之间再分配路由信息		REDISTRIBUTE <i>protocol id</i>	
过滤接口接收到的或发送出去的路由		REDISTRIBUTE <i>protocol id</i> DISTRIBUTE-LIST <i>list-num</i> PASSIVE-INTERFACE <i>type num</i>	DISTRIBUTE-LIST <i>list-num [IN OUT]</i>
过滤路由协议之间交换的路由			
在一个接口上禁止路由更新			IP SPLIT-HORIZON
在一个接口或子接口上启动水平分割			
在一个接口或子接口上禁止水平分割			NO IP SPLIT-HORIZON

译者序

随着Cisco路由器的广泛使用和网络规模的不断扩展，使得管理和配置Cisco路由器的工作日益繁重。每个路由器都需要经过一定的配置才能够正常地工作，而完成相同的任务往往可以使用多种命令的组合。大多数的管理和配置人员并没有时间去完全了解每一种路由协议，因此需要一本能够提供快速解答配置和技术问题的指南，使管理和配置人员在遇到问题时能够快速找到答案，并得到一些解释。如果你也有这种体会，那么本书就是一个很好的选择。

本书的问题都是有关Cisco路由器配置方面精选的典型问题，是广大Cisco路由器管理和配置人员经常会遇到的问题，或希望了解的知识。本书的解答都是由Cisco路由器专家提供的专业级说明，并带有许多配置的范例，使读者能够深入了解各种路由协议的异同。

对于那些承担运行大型复杂的IP网络的读者而言，本书是极佳的参考书籍；对于那些希望了解目前Internet上使用的各种路由协议的读者而言，本书也可以作为培训的辅导教材。

译者

2000年1月22日于北京

前言

Cisco是网络技术发展最快的公司，其产品拥有80%的市场占有率。本书设计的问题及其解答抓住了Cisco产品工程师经常遇到的路由和交换问题，覆盖了Cisco系统支持的所有IP路由协议，读者可以从中找到许多针对各种路由协议的不同应用的有价值的答案，从而能够配置各种协议，并监测IP网络。

本书分为12章，每章包括有关某个路由技术和协议的问题及其答案。第1章包括10个Cisco路由和交换技术的专题，包括多路由协议、过滤、路由再分配、邻站、兼容性、路由数据库和特殊的路由技术等。有关内部、系统和外部路由问题的解答，解释了路由器协议的不同种类及其功能。有关度量值的章节描述了路由协议使用的计算方法，确定到目的地的最佳路径。

第2章概括了被广泛使用的各种路由协议，包括RIP、OSPF、IGRP、EIGRP、BGP、EGP和IP组播等。第3章回答了有关增强型内部网关路由协议（EIGRP）的问题，它是内部网关路由协议（IGRP）的Cisco增强版本。第4章描述了在一个使用开放最短路径优先（OSPF）协议的网络中如何配置路由器，它综合了不同的用于配置和监测OSPF路由器性能的命令。第5章主要关于路由信息协议版本1（RIPv1），这是最常用的内部网关协议（IGP）。本章还描述了RIP版本2增加的功能。第6章解答了有关中间系统到中间系统（IS-IS）协议的问题，它是一种链接状态、分级路由协议。

第7章提供了有关配置边界网关协议（BGP）的问题解答，包括BGP支持、BGP IP路由支持、ISP与BGP及监测和维护BGP等。EGP——第一个外部网关协议，并在Internet上得到广泛应用——在第8章中解答。第9章、第10章包括配置网关发现协议（GDP）和ICMP路由器发现协议（IRDP）。在第11章中，读者将得到有关配置IP组播路由问题的解答，包括Internet组管理协议（IGMP）和距离向量组播路由协议（DVMRP）。第12章讨论使用路由表、邻站和统计等方法监测IP网络。

除了问题和解答，每一章都包括许多提示与注意事项，可以使读者得到更好的解答，并提醒有关的快捷方法，警告潜在的问题，及解释难于理解的项目。

本书中的约定

为了便于阅读，本书使用了几个约定格式，使读者可以方便地找到解答。

- 全大写字母：在文字中用于表示路由器命令。例如：SHOW IP ROUTE命令。
- 斜体字母：用于在路由器命令中表示变量。例如：OFFSET-LIST *access-list-number*。

除了这些约定，读者还将见到一些图表符号，它们的目的是表明这是重要信息，你必须给予注意：提示、注意和警告。



提示 提示提供了配置路由器协议快捷方法，使你的工作更简单。



注意 指那些能够提高你对问题的理解的信息，将这些项目标出使你的同事加深印象。



警告 指警告和需要避免的陷阱等。

目 录

译者序	
前言	
第1章 10个路由与交换专题解答	1
1.1 多路由协议	3
1.2 过滤	4
1.3 路由再分配	8
1.4 毗邻路由器	10
1.5 内部、系统和外部路由	10
1.6 水平分割	13
1.7 度量值	13
1.8 与其他厂家设备的兼容	14
1.9 路由数据库	14
1.10 特殊的路由技术	15
第2章 IP路由协议	16
2.1 RIP	17
2.2 OSPF	20
2.3 IGRP和EIGRP	24
2.4 BGP和EGP	28
2.5 IP组播	31
第3章 配置EIGRP	32
3.1 支持EIGRP IP	33
3.2 EIGRP的概念与术语	33
3.3 EIGRP的基本组件	36
3.4 支持EIGRP IPX SAP	55
3.5 监测EIGRP	57
第4章 配置OSPF	61
4.1 区域边界路由器	62
4.2 路由汇总	63
4.3 端区域和完全端区域	64
4.4 监测	65
4.5 虚链路	70
4.6 非端区域	71
4.7 实战经验	74
第5章 配置RIP	78
5.1 RIP版本1	79
5.2 RIP版本2	91
5.3 触发的RIP	95
5.4 兼容性	95
第6章 配置IS-IS	97
6.1 路由域	98
6.2 消息	102
6.3 区域	104
6.4 链接状态更新	106
6.5 度量值	108
第7章 配置BGP	114
7.1 支持BGP	115
7.2 支持BGP IP路由	119
7.3 ISP与BGP	127
7.4 监测与保持BGP	128
第8章 配置EGP	131
8.1 自治系统	132
8.2 毗邻路由器	132
8.3 更新	135
第9章 配置GDP	136
9.1 GDP语法	137
9.2 GDP综述	137
9.3 配置GDP	142
9.4 网络安全和GDP	143
第10章 配置IRDP	145
10.1 IRDP语法	146
10.2 配置IRDP	148
10.3 IRDP的网络与主机的安全性	151
第11章 配置IP组播路由	163
11.1 Internet组管理协议	164
11.2 协议独立组播	166
11.3 距离向量组播路由协议	168

11.4 OSPF的组播扩展	168	12.2 显示邻站	173
11.5 PIM与DVMRP互操作	169	12.3 显示统计数据	175
第12章 监测IP网络	170	12.4 参数和状态	177
12.1 显示IP路由表	170	术语表	179

第1章 10个路由与交换专题解答

问题

- 多路由协议
 - 什么时候使用多路由协议
 - 定义距离向量路由协议
 - 定义链接状态路由协议
 - 一个路由器使用多种路由协议
- 过滤
 - 确定访问表
 - 支持多种访问表
 - 创建标准IP访问表
 - 创建扩展IP访问表
 - 访问表到接口的链接
 - 使用有名访问表
 - 访问表的定位
 - 访问表的显示和状态
 - IPX标准访问表与SAP过滤器的区别
 - 配置IPX标准访问表
 - 配置IPX SAP过滤器
 - 配置AppleTalk访问表
- 路由再分配
 - 定义路由再分配
 - 使用路由再分配
 - 定义管理距离
 - 管理距离的值
 - 配置路由再分配
- 毗邻路由器
 - 确定毗邻路由器的重要性
 - 距离向量路由协议与链接状态路由协议是如何发现毗邻路由器的
- 内部、系统和外部路由
 - 定义自治系统
 - 内部和外部路由协议
 - 配置路由器使用RIP
 - 确认RIP是激活的

- 关闭RIP路由状态更新的显示
- 确定哪些网络是由RIP路由协议发现的
- 激活IGRP路由协议
- 定义增强型IGRP
- 确定哪些网络是由IGRP路由协议发现的
- 边界网关协议 (BGP)
- BGP支持的连接种类
- 有BGP时的路由再分配
- 在数据库中显示BGP路径
- 水平分割
 - 定义水平分割
 - 路由环的产生
- 度量值
 - 路由度量值
 - IGRP对路由度量值的使用
 - 修改度量值
 - 路由选择需要知道的信息
- 与其他厂家设备的兼容
 - 开放性标准与专利性技术
- 路由数据库
 - 回顾路由选择表
- 特殊的路由技术
 - 建立静态路由
 - 禁止水平分割

本章摘要

每一种路由协议都有一套规则来指示路由器如何以及向哪里发送数据包,使其能到达正确的目的地。这些规则(方法)通过了解路由器接口的连接参数和接口配置情况,计算出一些度量值,然后根据这些度量值选出最优路径,指出数据包发向哪一个接口。一些路由器有多种路由选择协议,包括距离向量路由协议或链接状态路由协议。每一种协议都要根据一些关键信息,如地址,来确定毗邻站点、发现路由、选择路由和保持路由信息。

本章介绍一些广泛使用的路由协议的参数,这些协议有:RIP、OSPF、IGRP和EIGRP。每一节的内容如下:

- 多路由协议 说明距离向量路由协议与链接状态路由协议的区别。
- 过滤 说明如何在网络中使用访问表控制流量。
- 路由再分配 说明路由选择表从一种路由选择协议到另一种路由选择协议的转换。
- 毗邻路由器 说明在寻找路由的过程中如何发现相邻节点。
- 内部、系统和外部路由 解释路由协议的分类及其功能。
- 水平分割 说明避免路由环的步骤。

- 度量值 回顾路由协议确定最优路径时使用的方法。
- 与其他厂家设备的兼容 解释开放性路由协议与专利性路由协议的关系。
- 路由数据库 解释路由选择表的使用及其重要性。
- 特殊的路由技术 解释建立静态路由和禁止水平分割。

1.1 多路由协议



1 什么时候使用多路由协议?



当两种不同的路由协议要交换路由信息时,就要用到多路由协议。当然,路由再分配也可以交换路由信息。下列情况不必使用多路由协议:

- 从老版本的内部网关协议 (Interior Gateway Protocol, IGP) 升级到新版本的IGP。
- 你想使用另一种路由协议但又必须保留原来的协议。
- 你想终止内部路由,以免受到其他没有严格过滤监管功能的路由器的干扰。
- 你在一个由多个厂家的路由器构成的环境下。



2 什么是距离向量路由协议?



距离向量路由协议是为小型网络环境设计的。在大型网络环境下,这类协议在学习路由及保持路由将产生较大的流量,占用过多的带宽。如果在90秒内没有收到相邻站点发送的路由选择表更新,它才认为相邻站点不可达。每隔30秒,距离向量路由协议就要向相邻站点发送整个路由选择表,使相邻站点的路由选择表得到更新。这样,它就能从别的站点(直接相连的或其他方式连接的)收集一个网络的列表,以便进行路由选择。距离向量路由协议使用跳数作为度量值,来计算到达目的地要经过的路由器数。

例如,RIP使用Bellman-Ford算法确定最短路径,即只要经过最小的跳数就可到达目的地的线路。最大允许的跳数通常定为15。那些必须经过15个以上的路由器的终端被认为是不可到达的。

距离向量路由协议有如下几种: IP RIP、IPX RIP、AppleTalk RTMP和IGRP。



3 什么是链接状态路由协议?



链接状态路由协议更适合大型网络,但由于它的复杂性,使得路由器需要更多的CPU资源。它能够在更短的时间内发现已经断了的链路或新连接的路由器,使得协议的会聚时间比距离向量路由协议更短。通常,在10秒钟之内没有收到邻站的HELLO报文,它就认为邻站已不可达。一个链接状态路由器向它的邻站发送更新报文,通知它所知道的所有链路。它确定最优路径的度量值是一个数值代价,这个代价的值一般由链路的带宽决定。具有最小代价的链路被认为是最优的。在最短路径优先算法中,最大可能代价的值几乎可以是无限的。如果网络没有发生任何变化,路由器只要周期性地将没有更新的路由选择表进行刷新就可以了(周期的长短可以从30分钟到2个小时)。

链接状态路由协议有如下几种: IP OSPF、IPX NLSP和IS-IS。



4 一个路由器可以既使用距离向量路由协议,又使用链接状态路由协议吗?



可以。每一个接口都可以配置为使用不同的路由协议;但是它们必须能够通过再分配路

由来交换路由信息。(路由的再分配将在本章的后面进行讨论。)

1.2 过滤



什么是访问表?



访问表是管理者加入的一系列控制数据包在路由器中输入、输出的规则。它不是由路由器自己产生的。访问表能够允许或禁止数据包进入或输出到目的地。访问表的表项是顺序执行的,即数据包到来时,首先看它是否是受第一条表项约束的,若不是,再顺序向下执行;如果它与第一条表项匹配,无论是被允许还是被禁止,都不必再执行下面表项的检查了。每一个接口的每一种协议只能有一个访问表。



支持哪些类型的访问表?



一个访问表可以由它的编号来确定。具体的协议及其对应的访问表编号如下:

- IP标准访问表编号: 1 ~ 99
- IP扩展访问表编号: 100 ~ 199
- IPX标准访问表编号: 800 ~ 899
- IPX扩展访问表编号: 1000 ~ 1099
- AppleTalk访问表编号: 600 ~ 699



提示 在Cisco IOS Release 11.2或以上版本中,可以用有名访问表确定编号在1~199的访问表。



如何创建IP标准访问表?



一个IP标准访问表的创建可以由如下命令来完成:

```
Access-list access list number {permit | deny}
source [source-mask]
```

在这条命令中:

- **access list number**: 确定这个入口属于哪个访问表。它是从1到99的数字。
- **permit | deny**: 表明这个入口是允许还是阻塞从特定地址来的信息流量。
- **source**: 确定源IP地址。
- **source-mask**: 确定地址中的哪些比特是用来进行匹配的。如果某个比特是“1”,表明地址中该位比特不用管,如果是“0”的话,表明地址中该位比特将被用来进行匹配。可以使用通配符。

以下是一个路由器配置文件中的访问表例子:

```
Router# show access-lists
Standard IP access list 1
deny 204.59.144.0, wildcard bits 0.0.0.255
permit any
Router#
```

下面是给定一个访问表的名字,使用SHOW IP ACCESS-LIST命令的输出:

```
showcase# show ip access-list Internetfilter
Extended IP access list Internetfilter
permit tcp any 171.69.0.0 0.0.255.255 eq telnet
deny tcp any any
deny udp any 171.69.0.0 0.0.255.255 lt 1024
deny ip any any log
```



如何创建IP扩展访问表？



创建IP扩展访问表可以用：

```
Access-list access list number {permit | deny}
protocol source [source-mask] destination
destination-mask [operator operand] [established]
```

在这条命令中：

- **access list number**：用在100 ~ 199中的数字确定访问表。
- **permit | deny**：表明这个入口是允许还是阻塞特定地址的信息流量。
- **protocol**：IP、TCP、UDP、ICMP、GRE、IGRP。
- **source**和**destination**：确定源和目的IP地址。
- **source-mask**和**destination-mask**：确定地址中的哪些比特是用来进行匹配的。如果某个比特是“1”，表明地址中该位比特可以忽略，如果是“0”的话，表明地址中该位比特将被用来进行匹配。可以使用通配符。
- **operator**和**operand**：lt、gt、eq、neq（小于、大于、等于、不等）和端口号。
- **established**：如果数据包使用一个已经建立的连接（如ACK位有效），则允许TCP流量通过。



注意 一个访问表必须有一个对所有使用访问表的数据包都适用的表项。最后一个隐含的表项用来处理那些前面的表项都不处理的数据包，即它能匹配所有的剩余的数据包。



链接访问表和接口使用什么命令？



使用IP ACCESS-GROUP命令将访问表链接到一个接口：

```
ip access-group access-list-number { in | out }
```

在这个命令中：

- **access-list-number**：表明要链接的访问表的编号。
- **in | out**：选择访问表是用于输入还是输出接口，未指明就使用缺省值。



提示 要去除一个访问表，首先键入NO ACCESS-GROUP命令及其相应的参数，然后再键入NO ACCESS-LIST命令及其相应的参数。



如何使用有名IP访问表？



你可以使用有名IP访问表从一个特定的访问表中删除一个单独的表项。这使得你能够方便地修改访问表，而不用删除它然后重新配置。在下列情况下可以使用有名访问表：

- 你想使用一个字母数字（alphanumeric）名确认一个访问表。

- 对于一个给定的协议，你有超过99个简单的，超过100个扩展的访问控制表需要配置。



注意 你不能对多个访问表使用相同的名字，不同种类的访问表也不能有相同的名字。



为什么访问表的位置很重要？



管理者使用访问表来减少不必要的流量。被禁止的终端不能使用网络资源发送数据包到目的地。标准访问表没有指明目的地的地址，所以应该放在离目的地近的地方。扩展访问表指明了目的地，就应该放在距离数据流的源较近的地方。



如何找出已配置的访问表及其状态？



使用SHOW IP INTERFACE命令来显示哪些访问表是激活的。使用SHOW ACCESS-LISTS命令来显示所有访问表的内容。如果你指明了访问表的名字或编号，你就可以看到这个访问表的具体内容了。



IPX标准访问表和SAP过滤器有何区别？



IPX标准访问表能够过滤源和目的地址。SAP过滤器是为在一个或多个网络上的服务器服务的。IPX标准访问表检查源地址或源和目的地址，可以使用通配符掩码，像IP的通配符掩码一样。SAP过滤器能够控制获得最近的服务器（GNS）、IPX RIP和NetWare的链路服务协议（NLSP）等产生的流量。



如何配置IPX标准访问表？



可以使用如下命令配置IPX标准访问表：

```
Access-list access-list number { deny | permit }
Protocol source-network [. source-node] [source-node-mask]
[destination-network] [.destination-node]
[destination-node-mask]
```

在这个命令中：

- **access-list-number**：是一个IPX过滤器列表的编号，从800到899。
- **protocol**：是协议类型的编号，0表示任何协议；1表示RIP；4表示SAP；5表示SPX；17表示NCP；20表示IPX NetBIOS。
- **source-network**：指明源网络编号，用8个十六进制数表示。
- **source-node**：指明在源网络中的节点编号，是一个48比特的数字，可以由每4个就用点分开的十六进制数表示。
- **destination-network**：指明报文的目的网络编号。
- **destination-node**：指明报文的目的节点号。

用IPX ACCESS-GROUP命令可以将访问表链接到一个接口：

```
ipx access-group access-list-number
```

下面是创建一个名叫sal的扩展访问表的例子，它禁止所有的SPX报文：

```
ipx access-list extended sal
deny spx any all any all log
permit any
```

下面是一个IPX标准访问表的例子:

```

Hostname Router
!
!
ipx routing 00e0.1e68.5c62
!
interface Ethernet0
ip address 192.168.68.1 255.255.255.0
ipx access-group 800
ipx network 100
!
interface Serial0
ip address 172.16.1.1 255.255.255.252
no fair-queue
!
!
access-list 800 deny 1 200
access-list 800 permit FFFFFFFF

```



如何配置IPX SAP过滤器?



SAP过滤器可以按以下格式创建:

```

access-list access-list-number { deny | permit } network
[.node] [network-mask node-mask]
[service-type [server-name]]

```

下一行可以是:

```
ipx input-sap-filter access-list-number
```

或:

```
ipx output-sap.-filter access-list-number
```

在这个命令中:

- **access-list-number**: 指明一个IPX过滤器的编号, 从1000到1099, 它是指向一个SAP过滤器。
- **network[.node]**: 指明Novell源内部网络编号和选项节点号 (-1表示所有网络)。
- **network-mask node-mask**: 指明网络和节点的掩码。1表示该位不作处理。
- **service-type**: 指明要过滤的SAP服务类型。每一种服务类型用一个十六进制数表示: 4代表文件服务器, 7代表打印服务器, 24代表远端网桥服务器(路由器)。
- **server-name**: 指明提供该项服务的服务器名称。

使用IPX INPUT | OUTPUT-SAP FILTER命令将过滤器与接口进行链接, 同时决定在进入SAP表之前, 在哪儿SAP报文被过滤, 或者在下一次更新时进行过滤。

如下的配置文件显示了一个IPX SAP过滤器:

```

Hostname Router
!
!
ipx routing 00e0.1e68.5c62
!

```

```

interface Ethernet0
ip address 192.168.68.1 255.255.255.0
ipx input-sap-filter 1000
ipx network 100
!
interface Serial0
ip address 172.16.1.1 255.255.255.252
no fair-queue
!
!
access-list 1000 deny 1 200 7
access-list 1000 permit FFFFFFFF

```

下面是创建一个名叫Merchant的SAP访问表的例子。它使得在SAP广告中，只允许Merchant被传送：

```

ipx access-list sap Merchant
permit 1234 4 Merchant

```



12 AppleTalk访问表的主要概念是什么？



AppleTalk的访问表能够过滤扩展的网络或电缆范围。你也可以在一个扩展的网络内选择部分电缆范围。使用AppleTalk I时，你可以指定一个网络；但在AppleTalk II中，你可以指定电缆范围的全部或一部分。访问表可以控制数据报文和使用RTMP和ZIP的路由更新报文。



13 如何配置AppleTalk访问表？



AppleTalk使用两种格式进行配置。定义一个全电缆范围的过滤器，使用如下命令：

```
access-list number {permit | deny} cable-range cable-range
```

定义一个部分电缆范围的过滤器，使用如下命令：

```
access-list number {permit | deny} within cable range cable-range
```

在这个命令中：

- number: AppleTalk的访问表编号（从600到699）。
- cable-range: 指明特定的电缆范围。

可以使用APPLETALK ACCESS-GROUP命令将访问表链接到一个或多个接口：

```
Appletalk access-group access-list-number
```

1.3 路由再分配



什么是路由再分配？



路由再分配允许一个寻找路由进程发现的路由可以更新其他进程的路由选择表。例如，RIP的路由选择表可以输入到OSPF或EIGRP的路由选择表中，反向亦可。



提示 你只能在支持相同协议栈的路由协议之间进行路由再分配。例如，IP RIP和OSPF之间可以进行路由再分配是因为它们都支持TCP/IP协议栈。但是，IPX RIP和