网络协议配置

目 录

第 1 章　配置 IP 寻址

1.1　IP概述

1.1.1　IP

Internet 协议 (IP) 是一个以报文形式在计算机网络中交换数据的协议。IP 具有寻址、分片、重组和协议复用功能。它是所有其它 IP 协议（统称为 IP 协议族）的基础。作为网络层协议，IP 包括用于路由的寻址和控制信息。
传输控制协议（TCP）建立在 IP 之上。TCP 是面向连接的协议，所以它规定了数据传输中数据和确认信息的格式。TCP 还规定了计算机用来确认数据正确到达的方法。TCP 允许在同一个系统中的多个应用程序同时进行通信，因为它可以把收到的数据分别送往各个应用程序。
IP 寻址功能，例如地址解析协议（ARP），将在“配置 IP 寻址”中介绍。IP 服务，例如 ICMP, HSRP，IP 统计和性能参数等，都将在“配置 IP 服务”中介绍。

1.1.2　IP 路由协议

在本公司的路由交换机中实现了多个 IP 路由动态协议，它们将在本文中各个协议的说明中分别予以介绍。
IP 路由协议一般分为两类：内部网关路由协议（IGP）和外部网关路由协议（EGP）。本公司路由交换机支持 RIP、OSPF、BGP 和 BEIGRP。您可以根据您的需要分别配置 RIP、OSPF、BGP 和 BEIGRP。在我们的路由交换机上，支持同时配置多个路由协议的进程，包括任意多个的 OSPF 进程（如果内存能够分配），一个 BGP 进程，一个 RIP 进程和任意多个的 BEIGRP 进程。您可以使用 redistribute 将其它路由协议的路由重新发布的当前的路由进程的数据库中，以此来将多个协议进程的路由联系起来。
为了配置 IP 动态路由协议，首先必须配置创建相应的进程，并且将相应的网络端口与一定的动态路由进程相联系起来，指定路由进程在那些端口上启动。为此，你可能需要在相应的配置命令文档中查看相关的配置步骤。

1. 选择路由协议

选择路由协议，这是一个复杂的过程。在选择路由协议的时候，你必须考虑如下的因素：

- 网络的大小以及复杂度；
- 是否需要支持可变长网络；
- 网络流量；
- 安全的要求；
- 可靠性的要求；
- 策略；
- 其它

在这里，我们并不深入的介绍这个问题，只是提醒用户注意，您所选择的路由协议必须要能够满足您网络的情况，适应您的需求。

2. 内部网关路由协议

内部网关路由协议是用来在一个自治系统中的网络目标。所有的 IP 内部网关路由协议在启动的同时必须将其与一定的网络相联系起来（比如配置 network）。每个路由进程都监听网络上的来自其它路由交换机的更新报文，同时在网络上广播它自己的路由信息。本公司路由交换机支持的内部网关路由协议有：

- RIP
- OSPF
- BEIGRP

3. 外部网关路由协议

外部网关路由协议是用来在不同自治系统之间交换路由信息。一般要求配置相应的用来交换路由的邻居、公布为可到达的网络以及本地的自治系统号。本公司路由交换机支持的外部网关路由协议有 BGP。

1.2 配置IP地址任务列表

配置 IP 的一个基本和必需的要求就是要在路由交换机的网络接口上配置 IP 地址。这样才能激活这个接口，使它可以和其它系统用 IP 进行通信。同时还要确定 IP 网络掩码。
为了配置 IP 寻址功能，需要完成下列各项任务，其中第一项任务是必需的，其它都是可选的。在本章的最后，“IP 寻址示例”举例说明如何在网络中建立 IP 寻址。
IP 地址配置任务列表：

- 在网络接口配置 IP 地址
- 在网络接口配置多个 IP 地址
- 配置地址解析
- 配置一个路由进程
- 配置广播报文处理
- 检测和维护 IP 寻址

1.3 配置IP地址

1.3.1 在网络接口配置 IP 地址

IP 地址确定了 IP 报文可以发送到的目的地址。某些 IP 地址是有特殊的意义而被保留的，不能作为主机地址或者是网络地址使用。表格 1 列出了 IP 地址的范围，以及保留地址和可以使用的 IP 地址。

类别	地址或范围	状态

A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	保留 可用 保留
B	128.0.0.0 to 191.254.0.0 191.255.0.0	可用 保留
C	192.0.0.0 192.0.1.0 to 223.255.254.0 223.255.255.0	保留 可用 保留
D	224.0.0.0 to 239.255.255.255	多目广播地址
E	240.0.0.0 to 255.255.255.254 255.255.255.255	保留 广播

有关 IP 地址的正式描述在 RFC 1166 “Internet 数字”中。 如果希望得到可用的网络地址，和 Internet 服务提供商联系。

一个接口只能拥有一个主 IP 地址。要配置网络接口的主 IP 地址和网络掩码，在接口配置态使用下列命令：

命令	目的
ip address *ip-address mask*	配置接口的主 IP地址。

掩码（mask）表示 IP 地址中的网络部分。

注意：

我们只支持按网络字节序从最高位开始连续置位的网络掩码。

1.3.2 在网络接口配置多个 IP 地址

每个接口可以拥有多个 IP 地址，包括一个主 IP 地址和任意个从属 IP 地址。在以下几种情况下，需要配置从属 IP 地址：

当一个特定网段中没有足够的 IP 地址时。例如，某个逻辑子网中最多只有 254 个有效 IP 地址，但是需要在实际的物理网络中连接 300 台主机。在路由交换机或者是访问服务器上配置从属 IP 地址，可以使两个逻辑子网使用同一个物理子网。

许多较早期的网络是基于第二层网桥，而不是被划分成多个子网。正确使用从属 IP 地址可以把这样的网络改造成基于路由的多个子网。在网络中的路由交换机，通过配置的从属 IP 地址，可以了解同样连接在这个物理网络中的多个子网。

当一个网络的两个子网，被另一个网络在物理上分隔开。这时，可以把这个网络的地址作为从属 IP 地址，从而可以把一个逻辑网络中的两个在物理上被分隔开的网络在逻辑上连接在一起。

注意：

如果一个网段上的任意一台路由交换机配置了一个从属地址，则相同网段上的所有其它路由交换机也需要配置同样网段的从属 IP 地址。

在网络接口配置多个地址，在接口配置态使用下列命令：

命令	目的
ip address *ip-address mask* **secondary**	在网络接口上配置多个IP 地址。

注意：

IP 路由协议在发送路由更新信息时，可能会以不同的方式对待从属 IP 地址。

1.3.3 配置地址解析

IP 实现允许在接口上控制 IP 地址解析和其它一些功能。下面介绍如何配置地址解析：

1. 建立地址解析

一个 IP 设备可以同时有两个地址：本地地址（在本地网段或者是 LAN 唯一标识这台设备）和网络地址（表示设备所属的网络）。本地地址也就是通常所说的链路层地址，因为它是包含在链路层报文头部的，而且是由链路层设备读取、使用的。专业人员通常称之为 MAC 地址，因为链路层中的介质访问控制（MAC）子层是用来处理地址的。
例如，如果要与以太网上的一台设备通信，必须首先知道它的 48 比特 MAC 或者是本地数据链路层地址。从 IP 地址得到本地数据链路层地址的过程称为地址解析（ARP）。从本地链路层地址得到 IP 地址的过程称为反向地址解析（reverse address resolution）。
本系统使用两种形式的地址解析：地址解析协议（ARP）和代理 ARP（proxy ARP）。ARP 和代理 ARP 分别定义在 RFC 826 和 1027 中。
ARP 用于映射 IP 地址到介质或者说是 MAC 地址。已知 IP 地址，ARP 确定相应的 MAC 地址。一旦 MAC 地址被确定，IP 地址/MAC 地址的关系就被保存在 ARP 缓存中以便快速取得。然后 IP 报文就可以被封装在链路层报文中，被发送到网络上去。

- 定义一条静态 ARP 缓存

  ARP 和其它的地址解析协议提供了在 IP 地址和介质地址之间的动态映射。由于大多数主机都支持动态地址解析，所以一般不需要配置静态的 ARP 缓存项。如果必须定义的话，可以在全局配置态定义，在 ARP 缓存中建立一个永久的表项。系统将使用这一表项把 32 比特的 IP 地址翻译成为 48 比特的硬件地址。另外，还可以指定路由交换机代替其它主机应答 ARP 请求。

  如果不希望 ARP 表项永久存在的话，可以设置 ARP 表项的生存时间。 下面的两个表格列出了如何配置静态的 IP 地址/介质地址映射。

  在全局配置态，使用下面的其中一条命令：

命令	目的
arp ip-address hardware-address vlan	在ARP缓存中全局地映射一个IP地址到介质地址。
arp ip-address hardware-address vlan **alias**	指定路由交换机以自己的介质地址应答对指定IP地址的ARP请求。

  在接口配置态使用下述命令：

命令	目的
arp timeout *seconds*	设置ARP缓存项在ARP缓存中的超时时间。
arp dynamic	允许端口下的arp进行动态学习

  要显示特定接口的 ARP 超时时间，使用 **show interface** 命令。 使用 **show arp** 命令来检查 ARP 缓存中的内容。使用 **clear arp-cache** 命令清除 ARP 缓存中所有的表项。

- 激活代理 ARP

  系统使用代理 ARP（RFC 1027 定义）帮助没有相应路由的主机得到位于其它网络上的主机的介质地址。例如，当路由交换机收到一个 ARP 请求，如果路由交换机发现它所请求的主机和发出 ARP 请求的主机不连在路由交换机的同一个接口上，而且路由交换机所有到目的主机的路由都是通过其他接口，而不是收到 ARP 请求的接口，则它将发出一个代理 ARP 应答，回答自己的本地链路层地址。那台主机就会把报文发送给路由交换机，然后由路由交换机把它转发到目的主机。代理 ARP 功能缺省是被激活的。

  要激活代理 ARP，在接口配置态使用下列命令：

命令	说明
ip proxy-arp	在接口上激活代理ARP。

- 配置免费 ARP 功能

  交换机可以通过发送免费 ARP 报文来确定网络中其它设备的 IP 地址是否与自己冲突。免费 ARP 报文中携带的源 IP 和目的 IP 地址都是交换机本机地址，报文源 MAC 地址是本机 MAC 地址。

  交换机缺省情况下即可以对接收到的免费 ARP 报文进行处理，当收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址冲突，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。同时交换机也会通过日志来告知用户网络中出现了 IP 地址冲突。

  缺省情况下，交换机的免费 ARP 报文发送功能处于关闭状态。可以通过下面的命令在交换机的路由端口上配置免费 ARP 功能。

命令	说明
arp send-gratuitous	在接口上启动免费ARP报文发送。
arp send-gratuitous interval *value*	配置在当前接口上发送免费ARP的间隔。 默认为 120 秒。

- 配置 ARP 缓存解析的等待时间

  交换机在首次解析 arp 的时候，会创建 incomplete ARP 项，此 incomplete 项等待对端回复正确的 arp 应答报文后生成完整的 ARP 项，至此完成 ARP 解析过程。

  以下命令可以设置此 incomplete 项的生存时间。

命令	说明
arp pending-time *seconds*	配置arp缓存解析的等待时间。默认为 15 秒

- 配置不完全 ARP 条目数量上限

命令	说明
arp max-incomplete *number*	配置不完全ARP条目数量上限。默认为 0

- 配置与路由条目网关关联的 ARP 项在老化时重新探测的重传次数

  作为路由条目网关依赖的 ARP 项（会被打上标志 G）在老化时需要重新探测，以保证硬件子网路由信息的实时准确。此重传次数越大重新探测的成功率越高。

命令	说明
arp max-gw-retries *number*	配置与路由条目网关关联的ARP项在老化时重新探测的重传次数。默认为 3

- 配置是否在 ARP 条目老化时对其进行重新探测
  默认情况下只有路由条目网关依赖的 ARP 项会进行老化重新探测，此命令开启后对所有类型的 ARP 项都采取老化重新探测机制。

命令	说明
arp retry-allarp	配置是否在老化时对所有ARP条目进行重新探测

2. 映射主机名称到 IP 地址

任一 IP 地址都可以有一个主机名称与之对应。系统保存了一个可以被 telnet，ping 等命令使用的主机名到地址的映射缓存。
要指定主机名到地址的映射，在全局配置态使用下列命令：

命令	目的
ip host *name address*	静态地映射主机名到IP地址。

1.3.4 配置一个路由进程

配置到这里，用户可以根据各自网络的需要配置一个或者多个路由协议。路由协议提供有关互联网络的拓扑结构信息。配置 IP 路由协议，例如 BGP，RIP，OSPF 在后面的文档中介绍。

1.3.5 配置广播报文处理

广播报文的目的地址是某个物理网络上的所有主机。网络主机通过特殊的地址识别广播报文。某些协议频繁使用广播报文，其中包括一些重要的 Internet 协议。控制广播报文是 IP 网络管理员的一项基本工作。系统支持定向广播，也就是到特定网络的广播。系统不支持到一个网络中所有子网的广播。
某些早期的 IP 实现使用的不是现在的广播地址标准，它们使用全“0”而不是全“1”表示广播地址。因此，系统可以同时识别和接收这两种形式的报文。

1. 允许从定向广播到物理广播的翻译

缺省情况下，IP 定向广播报文都将被丢弃，而不被转发。丢弃 IP 定向广播报文使路由交换机不易受到“拒绝服务”类型的攻击。
用户可以在定向广播转成物理广播的接口上激活 IP 定向广播的转发功能。如果这一转发功能被激活，所有到这个接口所在网络的定向广播报文都将被转发到这个接口，然后作为物理广播报文发送。
用户可以指定一个访问表来控制广播报文的转发。当指定了访问表以后，只有被访问表允许的 IP 报文才可以从定向广播转变到物理广播。
如果要激活 IP 定向广播的转发，在接口配置态使用下列命令：

命令	说明
ip directed-broadcast [*access-list-name*]	在一个接口上允许从定向广播到物理广播的翻译。

2. 转发 UDP 广播报文

有时，网络主机使用 UDP 广播报文确定地址，配置和名称等信息。如果该主机所在的网络上没有相应的服务器，而一般情况下这些 UDP 报文又不会被转发，则主机无法得到这些信息。为解决这个问题，用户可以在相应的接口上配置把某些类型的广播报文转发到一个帮助地址。一个接口可以配置多个帮助地址。

用户可以指定一个 UDP 目的端口来控制哪些 UDP 报文将被转发。目前，系统缺省转发目的端口是 NetBIOS 名字服务（端口 137）的 UDP 报文。

如果要允许转发并指定目的地址，在接口配置态使用下列命令：

命令	说明
ip helper-address *address*	允许转发UDP广播报文并指定目的地址。

如果要指定转发哪些协议，在全局配置态使用下列命令：

命令	说明
ip forward-protocol udp [*port*]	指定哪些接口的UDP协议被转发。

1.3.6 检测和维护 IP 寻址

要检测和维护网络，执行下列操作：

1. 清除缓存，列表和数据库

用户可以清除某个缓存、列表和数据库中的所有内容。当你认为某个缓存、列表或者数据库中的内容无效时，就需要清除它。

下表中的操作与清除缓存、列表和数据库有关，在管理态使用下列命令：

命令	目的
clear arp-cache	清除IP ARP缓存。

2. 显示系统和网络统计数据

系统可以显示特定的统计数据，如 IP 路由表，缓存和数据库。这些信息可以帮助确定系统资源使用情况，从而解决网络问题。系统还可以显示端点的可到达性以及发出报文在网络中的行进路线。

这些操作都列在下面的表中。这些命令的具体使用方法，请参见“IP 寻径命令”一章。在管理态使用下列命令：

命令	目的
show arp	显示ARP表中的内容。
show hosts	显示主机名-IP地址映射缓存表。
show ip interface [*type number*]	显示接口状态。

show ip route [*protocol*]	显示路由表的当前状态。
ping {**host**	**address**}	测试网络端点的可到达性。

1.4 IP寻址示例

在下面的例子中，在端口 VLAN 11 配置 IP 地址。

interface vlan 11

ip address 202.96.2.3 255.255.255.0

第 2 章　配置 DHCP

2.1　概述

DHCP（*Dynamic Host Configuration Protocol*）协议为 Internet 上的主机提供了部分网络配置参数。DHCP 在 RFC 2131 中讲述。DHCP 最主要的一项功能是分配接口上的 IP 地址。DHCP 协议支持三种机制的 IP 地址分配机制：

- 自动分配
  DHCP 服务器自动分配一个永久性的 IP 地址给某一客户端使用。
- 动态分配
  DHCP 服务器分配一个 IP 地址给某一客户端使用一定的时间，或者直到该客户主动放弃该地址的使用权。
- 手工分配
  DHCP 服务器管理员手工指定一个 IP 地址且通过 DHCP 协议传送给客户端使用。

2.1.1　DHCP 应用

DHCP 有几种应用。当存在以下需求时，可以使用 DHCP 协议：

- 如果需要为某一个以太网接口分配 IP 地址、网段及相关资源（如相应的网关），可以通过配置 DHCP 客户端来实现。
- 交换机上接有多个主机，而交换机能够访问到 DHCP 时，可以通过 DHCP 中继，从 DHCP 服务器上获得一个 IP 地址，将该地址再分配给该主机。

2.1.2　DHCP 的优点

在当前软件版本中，支持 DHCP 客户端的功能，在以太网接口上支持该 DHCP 客户端功能。该功能的使用可以提供以下优点：

- 减少配置时间
- 减少配置错误
- 通过 DHCP 服务器集中控制设备部分接口的 IP 地址

2.1.3　DHCP 术语

DHCP 协议本身是基于 Server/Client 结构的，所以在 DHCP 运行环境中，存在 DHCP-Server 和 DHCP-Client：

- DHCP-Server
  用来发放、收回 DHCP 协议所涉及资源（如 IP 地址、租用时间等）的设备。
- DHCP-Client
  从 DHCP-Server 处获取 IP 地址等信息，并且用于本地系统的设备。

如上所述，对于 DHCP 信息动态分配的过程中，存在租用时间的概念：

- 租用时间 —— 某个 IP 地址资源从分配开始计时的一段有效期，在该段时间之后，相应的 IP 地址资源将被 DHCP-Server 收回，若要继续使用，DHCP-Client 需要重新申请。

2.2 配置DHCP Client

2.2.1 DHCP Client 配置任务列表

- 获取一个 IP 地址
- 指定 DHCP-Server 地址
- 配置 DHCP 协议参数
- 监视 DHCP

2.2.2 DHCP Client 配置任务

1. 获取一个 IP 地址

通过 DHCP 协议为接口获取一个 IP 地址，在 VLAN 接口执行下列命令：

命令	作用
ip address dhcp	指定通过DHCP协议来配置该以太网接口的IP地址。

2. 指定 DHCP-Server 地址

如果已知某些 DHCP-Server 地址，可以在交换机上指定这些 Server 的地址以减少协议处理的交互和时间，在全局配置状态下，执行下列命令：

命令	作用
ip dhcp-server *ip-address*	指定DHCP服务器的IP地址。

当进行“获取一个 IP 地址”时该命令为可选命令。

3. 配置 DHCP 协议参数

可以根据需要，调整 DHCP 协议交互时的参数，在全局配置方式下执行下列命令：

命令	作用
ip dhcp client minlease *seconds*	指定最小可接受的租用时间。
ip dhcp client retransmit *count*	指定协议报文的重传次数。
ip dhcp client select *seconds*	指定SELECT间隔时间。
ip dhcp client class_identifier *WORD*	指定供应商分类编码
ip dhcp client client_identifier hrd_ether	指定客户端ID为以太网类型

ip dhcp client timeout_shut	指定客户端超时断开端口

当进行“获取一个 IP 地址”时以上命令为可选命令。

4. 监视 DHCP

可以查看路由交换机当前发现的 DHCP-Server（包括手工指定的）的相关信息，在管理态下执行下列命令：

命令	作用
show dhcp server	显示路由交换机所知DHCP服务器的相关信息。

可以查看路由交换机当前使用 IP 地址的相关信息，在管理态下执行下列命令：

命令	作用
show dhcp lease	显示路由交换机当前所使用的IP地址资源及其相关信息。

另外，如果采用 DHCP 协议为一个以太网接口分配一个 IP 地址，也可以通过“show interface”命令来查看该以太网口所需的 IP 地址是否成功获得。

2.2.3 DHCP Client 配置示例

下面是 DHCP Client 配置示例。

1. 获取一个 IP 地址示例

以下例子将为 vlan11 接口通过 DHCP 协议分配一个 IP 地址。

!

interface vlan 11

ip address dhcp

2.3 配置DHCP Server

2.3.1 DHCP Server 配置任务列表

- 打开 DHCP Server 服务
- 关闭 DHCP Server 服务
- 配置 ICMP 检测参数
- 配置保存 database 的参数
- 配置 DHCP Server 地址池
- 配置 DHCP Server 地址池参数
- 监视 DHCP Server
- 清除 DHCP Server 信息

2.3.2 DHCP Server 配置

1. 打开 DHCP Server 服务

打开 DHCP Server 服务，为 DHCP Client 分配 IP 地址等参数，在全局配置态下执行下列命令（此时，DHCP 服务器也支持 relay 操作，对于自身不能分配的地址请求，配置了 ip helper-address 的端口将转发 DHCP 请求）：

命令	作用
ip dhcpd enable	打开DHCP Server服务

2. 关闭 DHCP Server 服务

关闭 DHCP Server 服务，停止为 DHCP Client 分配 IP 地址等参数，在全局配置状态下，执行下列命令：

命令	作用
no ip dhcpd enable	关闭DHCP Server服务。

3. 配置 ICMP 检测参数

可以根据需要，调整 Server 进行地址检测时，发送的 ICMP 报文的参数：
配置发送 ICMP 报文个数，在全局配置状态下，执行下列命令：

命令	作用
ip dhcpd ping packets *pkgs*	指定地址检测是发送ICMP报文的个数

配置等待 ICMP 报文响应的超时时间，在全局配置状态下，执行下列命令：

命令	作用
ip dhcpd ping timeout *timeout*	指定等待ICMP报文响应的超时时间

4. 配置保存 database 的参数

配置每隔多长时间将地址分配信息保存到 agent database 中，在全局配置状态下，执行下列命令：

命令	作用
ip dhcpd write-time *time*	指定每隔多长时间将地址分配信息保存到agent database中。

5. 配置 DHCP Server 地址池

添加 DHCP Server 地址池，在全局配置态下执行下列命令：

命令	作用
ip dhcpd pool *name*	添加DHCP Server地址池，并进入DHCP地址池配置态。

6. 配置 DHCP Server 地址池参数

在 DHCP 地址池配置态下，可以执行以下命令来配置相关参数
用户可以使用以下命令来配置用于自动分配的地址池的网络地址：

命令	作用
network *ip-addr netsubnet*	配置用于自动分配的地址池的网络地址。

用户可以使用此命令来配置用于自动分配的地址区域：

命令	作用
range *low-addr high-addr*	配置用于自动分配的地址区域。

用户可以使用此命令来配置分配给客户机的缺省路由：

命令	作用
default-router *ip-addr …*	配置分配给客户机的缺省路由。

用户可以使用此命令来配置分配给客户机的 DNS 服务器地址：

命令	作用
dns-server *ip-addr …*	配置分配给客户机的DNS服务器地址。

用户可以使用此命令来配置分配给客户机的域名：

命令	作用
domain-name *name*	配置分配给客户机的域名。

用户可以使用此命令来配置分配给客户机的地址的时间期限：

命令	作用
lease {*days* [*hours*][*minutes*] | *infinite* }	配置分配给客户机的地址的时间期限。

用户可以使用此命令来配置分配给客户机的 netbios 名字服务器地址：

命令	作用
netbios-name-server *ip-addr…*	配置分配给客户机的netbios名字服务器地址。

用户可以使用此命令来配置拒绝为 mac 地址为“hardware-address”的主机提供分配 ip 地址：

命令	作用
hw-access deny hardware-address	拒绝为mac地址为“hardware-address”的主机分配ip地址

7. 监视 DHCP Server

查看 DHCP Server 当前的地址分配信息，在管理态下执行下列命令：

命令	作用
show ip dhcpd binding	显示DHCP Server当前的地址分配信息。

查看 DHCP Server 当前的报文统计信息，在管理态下执行下列命令：

命令	作用
show ip dhcpd statistic	显示DHCP Server当前的统计信息。

8. 清除 DHCP Server 信息

删除 DHCP Server 当前的地址分配信息，在管理态下执行下列命令：

命令	目的
clear ip dhcpd binding {*ip-addr*|*}	删除指定的地址分配信息。

删除 DHCP Server 当前的报文统计信息，在管理态下执行下列命令：

命令	目的
clear ip dhcpd statistic	删除DHCP Server当前的统计信息。

删除 DHCP Server 地址池当前被禁用、丢弃的地址，在管理态下执行下列命令：

命令	目的
clear ip dhcpd abandoned	删除DHCP Server地址池当前被丢弃、禁用的地址。

2.3.3 DHCP Server 配置示例

以下例子将 ICMP 检测包的超时时间设为 200ms，配置一个名为 1 的地址池，并打开 DHCP Server 服务。

```
ip dhcpd ping timeout 2
ip dhcpd pool 1
 network 192.168.20.0 255.255.255.0
 range 192.168.20.211 192.168.20.215
 domain-name my315
 default-router 192.168.20.1
 dns-server 192.168.1.3 61.2.2.10
 netbios-name-server 192.168.20.1
 lease 1 12 0
!
ip dhcpd enable
```

第 3 章　配置 IP 服务

本章介绍如何配置 IP 可选服务。如果要了解本章提到的 IP 服务命令的详细使用方法，请参阅“IP 服务命令”章节。

3.1　配置IP Service

可以配置下列 IP 的可选服务：

- 管理 IP 连接
- 配置性能参数
- **配置默认网关**
- 检测和维护 IP 网络

这些操作并不是必需的，而是根据网络需要进行的。

3.1.1　管理 IP 连接

IP 提供了一系列的服务来控制和管理 IP 连接。大多数这样的服务是由 ICMP 提供的。ICMP 报文一般是在路由交换机或者是访问服务器发现 IP 报头错误时发给主机或者是其它路由交换机的。ICMP 主要由 RFC 792 定义。
要管理 IP 连接的不同方面，执行下列相关操作：

1. 发送 ICMP 不可到达报文

如果系统收到一个报文，但是发现无法把它送到目的地，例如没有相应的路由，它将发送一个 ICMP 主机不可到达报文给源主机。系统的这一功能是缺省打开的。
如果这一功能被关闭的话，用户可以在接口配置态使用下列命令打开这一功能：

命令	目的
ip unreachables	发送ICMP不可到达报文的功能。

2. 发送 ICMP 重定向报文

有时，主机所选择的路由不是最佳的，因此收到报文的路由交换机发现，根据路由表要把这个报文从收到它的接口再次发送出去，转发到和发送主机在同一个网段上的另一台路由交换机。在这种情况下，路由交换机会通知源主机把到这一目的地址的报文直接发送到另一台路由交换机，而不必再经过本机。重定向报文要求源主机以报文中建议的更加直接的路由取代原来的路由。很多主机操作系统会在路由表中添加一条主机路由。但是，路由交换机更信任根据路由协议得到的信息，所以不会根据这条信息添加主机路由。
这一功能是缺省打开的。但是，如果在这个接口上配置了热备份路由交换机协议，则这项功能将被自动关闭。如果热备份路由交换机协议配置被取消，这一功能不会被自动打开。
如果这一功能被关闭，可以在接口配置态使用下列命令打开发送 ICMP 重定向报文功能：

命令	目的
ip redirects	允许发送ICMP重定向报文。

3. 发送 ICMP 掩码应答报文

有时主机必须了解网络掩码，为了得到这一信息，主机可以发送 ICMP 掩码请求报文。路由交换机如果能确定这台主机的掩码，将回应 ICMP 掩码应答报文。缺省情况下，路由交换机会发送 ICMP 掩码应答报文。

如果要求发送 ICMP 掩码请求报文，在接口配置态使用下列命令：

命令	目的
ip mask-reply	发送ICMP掩码应答报文。

4. 支持路径 MTU 发现

系统支持 RFC 1191 定义的 IP 路径 MTU 发现机制。IP 路径 MTU 发现使主机可以动态发现和适应不同路径的最大发送单元（MTU）长度。有时，路由交换机发现收到的 IP 报文长度大于报文转发接口上设置的 MTU，需要把 IP 报文分片，但是该 IP 报文的“不分片”位被置位，报文不允许被分片，所以报文只能被丢弃。这时，路由交换机会发送 ICMP 报文通知源主机转发失败的原因，以及转发接口上的 MTU。源主机会减小发往这个目的地址的报文的长度，以适应这条路径的最小 MTU。

如果路径中的一条链路断开，将导致报文采用其它路径，它的最小 MTU 可能和原来的路径不同。这时，路由交换机会通知源主机新路径的 MTU。在可能的情况下，应该尽量采用路径中最小的 MTU 封装 IP 报文，这样，既避免分片，又发送尽可能少的报文，从而提高通信效率。

相应的主机必须支持 IP 路径 MTU 发现，它才会根据路由交换机通知的 MTU 值调整发送的 IP 报文的长度，避免在转发过程中分片。

5. 设置 IP 最大发送单元（MTU）

所有的接口都有一个缺省的 IP 最大发送单元（MTU），也就是允许发送的最大 IP 报文长度。如果 IP 报文长度超过这个值的话，路由交换机就会对报文进行分片。

改变接口的 MTU 值将会影响接口的 IP MTU 值。如果 IP MTU 与 MTU 相等的话，改变 MTU，IP MTU 将自动调整到和新的 MTU 值相同。但是，改变 IP MTU 不会影响 MTU。IP MTU 不能大于当前接口上配置的 MTU。连接在同一物理介质上的所有设备必须具有相同的协议 MTU，才能正常通信。

要设置特定接口上的 IP MTU，在接口配置态使用下列命令：

命令	目的
ip mtu *bytes*	设置接口的IP MTU。

6. 允许 IP 源路由

路由交换机检查每个报文的 IP 报头选项，它支持 RFC 791 定义的 IP 报头选项：严格源路由、松弛源路由、记录路由和时戳。如果发现选项错误，将发送 ICMP 参数问题报文给源主机并丢弃报文。如果在源路由过程中发现错误，将发送 ICMP 不可到达（源路由失败）报文给源主机。

IP 允许源主机指定报文通过 IP 网络的路由，这称为源路由，可以在 IP 报头选项的源路由选项中指定。路由交换机必须根据该选项转发 IP 报文，或者出于安全考虑丢弃这类报文，并发送 ICMP 不可到达（源路由失败）报文给源主机。路由交换机缺省支持源路由。

如果 IP 源路由功能被关闭的话，可以在全局配置态使用下列命令允许 IP 源路由：

命令	说明
ip source-route	允许IP源路由。

7. 允许 IP 快速交换

IP 快速交换使用路由缓存转发 IP 报文。当转发第一个到某目的地址的报文时，系统查找路由表，根据路由转发报文。然后，这条路由将被保存在系统软件路由缓存中，以后到达该主机的报文，将直接根据软件路由缓存中的路由转发，每转发一次对应路由表项的命中次数增加 1，当命中次数到达用户设定值时，该路由缓存将被保存到系统硬件路由缓存中，以后再有到达该主机的报文将直接通过硬件转发。如果缓存一段时间不被使用，将被超时删去。当系统软件或硬件缓存条目已满时，新的目的主机将不被缓存；可以容纳 2047 条硬件缓存和 1024 条软件缓存。

在全局配置态使用下列命令配置软件缓存条目保存到硬件路由缓存时需要的命中次数：

命令	目的
ip route-cache hit-numbers *hitnumber*	软件缓存中的路由条目命中次数达到*hitnumber*时，将被保存到硬件路由条目中。

全局配置态下使用。若某非直连硬件主机路由的下一跳与某硬件子网路由下一跳相同， 该命令用于设置是否删除该硬件主机路由：

命令	目的
ip route-cache age-exf	删除下一跳与硬件子网路由下一跳相同的非直连硬件主机路由。
no ip route-cache age-exf	保留下一跳与硬件子网路由下一跳相同的非直连硬件主机路由。

在全局配置态使用下列命令配置有 arp 变化引起的删除硬件路由缓存的延迟指数：

命令	目的
ip route-cache age-delay *age-delay*	当arp变化时，在延迟一段时间（与*age-delay*相关）后将与此arp相关的所有硬件路由缓存删除。

在全局配置态使用下列命令配置软件路由缓存的生存时间：

命令	目的
ip route-cache softcache-alive-time *milliseconds*	软件路由缓存的从创建开始经历了*milliseconds*毫秒之后，将其删除。

在全局配置态使用下列命令配置软件路由缓存操作时间指数：

命令	目的
ip route-cache software-index *ticks*	*ticks*越大，交换机就能更快地老化无效的软件路由缓存。

在全局配置态使用下列命令配置硬件路由缓存操作时间指数：

命令	目的

ip route-cache hardware-index *ticks*	*ticks*越大，交换机就能更快地添加硬件路由缓存。

在全局配置态下使用下列命令配置硬件路由缓存的生存时间：

命令	目的
ip route-cache-aging-time *seconds*	交换机硬件路由缓存的生存时间

在全局配置态下使用下列命令允许把使用策略路由方式查找路由的路由缓存也加入硬件表：

命令	目的
ip route-cache cache-pbr	将策略路由方式查找路由的路由缓存加入硬件表

8. 允许同一接口上的 IP 快速交换

用户可以在允许同一 VLAN 接口上的 IP 路由缓存，即接收接口和发送接口相同。通常情况下，建议不要开启这一功能，因为这和 router 的重定向功能冲突。

要允许同一接口的 IP 路由缓存，在接口配置态使用下列 command：

命令	说明
ip route-cache *same-interface*	允许发送接口与接收接口相同的IP报文进行路由缓存。

9. 允许在学到 arp 时创建 route cache。

用于可以在学到 arp 时为 arp 创建 route cache 条目，在接口配置态使用下列 command：

命令	说明
ip route-cache *create-on-arp*	允许学到arp时创建route cache。

3.1.2 配置性能参数

要调节 IP 性能，执行下列操作。

1. 设置 TCP 连接等待时间

当路由交换机进行 TCP 连接时，如果在 TCP 连接等待时间之后连接还没有建立，路由交换机将认为连接失败，并把这一结果返回给上层应用程序。用户可以设置 TCP 连接等待时间，系统的缺省值是 75 秒。这项配置与路由交换机转接的 TCP 连接无关，只与路由交换机本机建立的 TCP 连接有关。

要设置 TCP 连接等待时间，在全局配置态使用下列命令：

命令	目的
ip tcp synwait-time *seconds*	设置TCP连接等待时间。

2. 设置 TCP 窗口尺寸

缺省的 TCP 窗口尺寸是 2000 字节。如果要改变缺省的窗口尺寸，在全局配置态使用下列命令：

命令	目的
ip tcp window-size *bytes*	设置TCP窗口尺寸。

3.1.3 检测和维护 IP 网络

要检测和维护网络，执行下列操作：

1. 清除缓存，列表和数据库

用户可以清除某个缓存、列表或者是数据库中的所有内容。如果认为某个缓存、列表或是数据库中的数据不正确，则需要清除它。
使用下列命令进行清除：

命令	目的
clear tcp statistics	清除TCP统计数据。

2. 清除 TCP 连接

如果要关闭某个 TCP 连接，使用下列命令：

命令	目的
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	清除指定的TCP连接。(TCB为TCP控制块：TCP Control Block)

3. 显示系统和网络统计数据

系统可以显示缓存、列表和数据库中的内容。这些信息可以帮助了解系统资源使用情况，解决网络问题。
可以在管理态使用下列命令。这些命令的具体使用方法，参见“IP 服务命令”章节。

命令	目的
show ip access-lists *name*	显示某个或所有访问列表的内容。
show ip cache [prefix mask] [type number]	显示用于快速交换IP报文的路由缓存。
show ip sockets	显示路由交换机所有socket的信息。
show ip traffic	显示IP协议统计数据。
show tcp	显示所有的TCP连接状态信息。
show tcp brief	显示简要的TCP连接状态信息。
show tcp statistics	显示TCP统计数据。
show tcp tcb	显示特定的TCP连接的状态信息。

4. 显示调试信息

当网络出现问题时，可以用 debug 命令要求系统显示调试信息。
可以在管理态使用下列命令。这些命令的具体使用方法，参见“IP 服务命令”章节。

命令	目的
debug arp	显示地址解析协议（ARP）的交互信息。
debug ip icmp	显示Internet控制信息协议（ICMP）的交互信息。

debug ip raw	显示收到的和发送的Internet协议（IP）报文信息。
debug ip packet	显示Internet协议（IP）的交互信息。
debug ip tcp	显示传输控制协议（TCP）的交互信息。
debug ip udp	显示用户数据报协议（UDP）的交互信息。

3.2 配置访问列表

3.2.1 过滤 IP 报文

过滤报文帮助控制包在网络中的运动。这样的控制可以帮助限制网络传输并通过一定的用户或设备限制网络使用。为了从交叉指定的接口中使包有效或无效，本公司路由交换机提供了访问列表。可以用以下方式使用访问列表：

- 控制在接口上的包传输
- 控制虚拟终端线路访问
- 限制路由更新内容

本节概括了如何建立 IP 访问列表以及如何应用它们。

IP 访问列表是应用 IP 地址的允许和禁止条件的有序集合。本公司路由交换机的软件在访问列表中逐个按规则测试地址。第一个匹配决定是否该软件接受或拒绝该地址。因为在第一个匹配之后，该软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，拒绝该地址。

在使用访问列表中有以下两个步骤：

(1) 通过指定访问列表名及访问条件，建立访问列表。

(2) 将访问列表应用到接口。

3.2.2 建立标准的和扩展的 IP 访问列表

用一个字符串建立 IP 访问列表。

注意:

标准的访问列表和扩展的访问列表不能用相同的名字。

为了建立标准的访问列表，在全局配置态执行下列命令。

命令	目的
ip access-list standard *name*	使用名字定义一个标准的IP访问列表。
deny {*source [source-mask]* | **any**|**src-range**}[**log**] or **permit** {*source [source-mask]* | **any**|**src-range**}[**log**]	在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。
Exit	退出访问列表配置模式。

为建立扩展的访问列表，在全局配置态执行下列命令：

命令	目的

ip access-list extended *name*	使用名字定义一个扩展的IP访问列表。
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**]{**deny** | **permit**} *protocol* {**any**|**src-range**} {**any**|**src-range**}	在扩展访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。（precedence表示ip包优先级，TOS表示Type of Service）
Exit	退出访问列表配置模式。

在初始建立访问列表后，任何后续的增加部分(可能从终端键入)都放入表的尾部。换句话说，你不能从指定的访问列表选择增加访问列表命令行。但是，你可以使用 no permit 和 no deny 命令从名字访问列表中删除项。

注意：

当建立访问列表时，记住缺省时访问列表的结尾包含隐含的 deny 语句。进一步讲，标准的访问列表，如果从相关的 IP 主机地址访问列表指定中省略了掩码，那么 255.255.255.255 就假定是掩码。

在建立了访问列表后，必须将它应用到线路或接口上。如下一节“将访问列表应用到接口”所描述。

3.2.3 将访问列表应用到接口

当建立了访问列表后，可以将它应用到一个或多个接口上，可以应用到进或出这两种情况。

在接口配置态使用以下命令。

命令	目的
ip access-group *name* {**in** | **out**}	将访问列表应用到接口。

访问列表既可用在出接口也可用在入接口。对于标准的入口访问列表，在接收到包之后，对照访问列表检查包的源地址。对于扩展的访问列表，该路由交换机也检查目标地址。如果访问表允许该地址，那么软件继续处理该包。如果访问表不允许该地址，该软件放弃包并返回一个 ICMP 主机不可到达报文。

对于标准的出口访问表,在接收和路由一个包到控制接口以后，软件对照访问列表检查包的源地址。对于扩展的访问表，路由交换机还检查接收端访问表。如果访问表允许该软件就传送这个包。如果访问列表不允许该地址，软件放弃这个包并返回一个 ICMP 主机不可达报文。

如果指定的访问列表不存在，所有的包允许通过。

3.2.4 扩展访问列表示例

在以下例子中，第一行允许任何新到的 TCP 与大于 1023 的目标端口连接。第二行允许新来的 TCP 与主机 130.2.1.2 的 SMTP 端口连接。

```
ip access-list extended aaa

permit tcp any 130.2.0.0 255.255.0.0 gt 1023

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in
```

另一个使用扩展访问列表的例子,假定有一个连接到 Internet 的网络,你希望在以太网上的任何主

机都能够建立 TCP 连接到任何 Internet 上的主机。但是，并不希望 Internet 上主机能够建立 TCP 连接到以太网上的主机,除非是到邮件主机的 SMTP 端口。
SMTP 使用连接的一端上的 TCP 端口 25 和另一端的随机端口号。在连接期间,使用同样的两个端口号。来自 Internet 的邮件包将有一个端口号为 25 的目标端口。出站包将有一个反向的端口号。事实上，在路由交换机后面的安全系统总是会接收连接在端口 25 上的邮件，这也正是能够单独控制入站服务和出站服务的原因。访问列表既可以配置成出站服务又可以配置成入站服务。以下例子中，以太网是一个带有地址 130.20.0.0 的 B 类网络，邮件主机的地址是 130.20.1.2。关键字 established 只用于 TCP 协议，表示一个建立的连接。如果 TCP 数据报有 ACK 或者 RST 位设置，匹配就会出现，表示该包属于一个现存的连接。

ip access-list aaa

permit tcp any 130.20.0.0 255.255.0.0 established

permit tcp any 130.20.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in

3.3 配置基于物理端口IP访问列表

3.3.1 过滤 IP 报文

过滤报文帮助控制包在网络中的运动。这样的控制可以帮助限制网络传输并通过一定的用户或设备限制网络使用。为了从交叉指定的端口中使包有效或无效，本公司路由交换机提供了访问列表。可以用以下方式使用访问列表：

- 控制在端口上的包传输
- 控制虚拟终端线路访问
- 限制路由更新内容

本节概括了如何建立 IP 访问列表以及如何应用它们。
IP 访问列表是应用 IP 地址的允许和禁止条件的有序集合。本公司路由交换机的软件在访问列表中逐个按规则测试地址。第一个匹配决定是否该软件接受或拒绝该地址。因为在第一个匹配之后，该软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，拒绝该地址。
在使用访问列表中有以下两个步骤：

(1) 通过指定访问列表名及访问条件，建立访问列表。
(2) 将访问列表应用到端口。

3.3.2 建立标准的和扩展的 IP 访问列表

用一个字符串建立 IP 访问列表。
注意:
标准的访问列表和扩展的访问列表不能用相同的名字。

为了建立标准的访问列表，在全局配置态执行下列命令。

命令	目的
ip access-list standard *name*	使用名字定义一个标准的IP访问列表。
{**deny**|**permit**} {*source [source-mask]* | **any**|**src-range**}	在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。
Exit	退出访问列表配置模式。

为建立扩展的访问列表，在全局配置态执行下列命令：

命令	目的
ip access-list extended *name*	使用名字定义一个扩展的IP访问列表。
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] {**deny** | **permit**} *protocol* {**any**|**src-range**} {**any**|**src-range**}	在扩展访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。（precedence表示ip包优先级，TOS表示Type of Service）。若protocol是TCP/UDP，则还可以指定单个或者某个范围内的l4 端口号，详细设置方法及注意事项可见扩展访问列表示例。
Exit	退出访问列表配置模式。

在初始建立访问列表后，任何后续的增加部分(可能从终端键入)都放入表的尾部。换句话说，你不能从指定的访问列表选择增加访问列表命令行。但是，你可以使用 no permit 和 no deny 命令从名字访问列表中删除项。

注意：

当建立访问列表时，记住缺省时访问列表的结尾包含隐含的 deny 语句。进一步讲，标准的访问列表，如果从相关的 IP 主机地址访问列表指定中省略了掩码，那么 255.255.255.255 就假定是掩码。

在建立了访问列表后，必须将它应用到线路或端口上。如下一节“将访问列表应用到端口”所描述。

3.3.3 将访问列表应用到端口

当建立了访问列表后，可以将它应用到一个或多个端口上，可以应用到入口或者出口。

在端口配置态使用以下命令。

命令	目的
ip access-group *name* [**egress**]	将访问列表应用到端口。

对于标准的入口访问列表，在接收到包之后，对照访问列表检查包的源地址。对于扩展的访问列表，该路由交换机也检查目标地址。如果访问表允许该地址，那么软件继续处理该包。

如果指定的访问列表不存在，所有的包允许通过。

3.3.4 扩展访问列表示例

1. 基于端口的 IP 访问列表支持 TCP/UDP 端口范围的过滤

如下格式：

{**deny | permit**} {tcp | udp}
source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt|eq|neq } port] }]
destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt |eq|neq} port] }]
[**precedence** *precedence*] [**tos** *tos*]

这样就能对 TCP 和 UDP 的端口号进行访问列表的控制，若定义端口范围来配置访问列表的情况需要注意如下问题：

(1) 若在源和目的上都使用指定端口范围的方法来配置访问列表，这时可能有些配置由于会耗费大量资源而导致配置失败，如果出现这种情况建议在一个方向使用指定端口范围的方式，而在另一个方向使用指定端口的方式。

(2) 另外需要注意的是，使用端口范围过滤的时候需要占用较多的资源，所以过多的使用会导致访问列表对其他应用支持能力的下降。

2. 基于端口的 IP 访问列表支持 TCP/UDP 指定端口的过滤

在以下例子中，第一行允许新来的 TCP 与主机 130.2.1.2 的 SMTP 端口连接。

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface  g0/1
ip access-group aaa
```