IPv6配置

目 录

第 1 章 IPv6 协议配置 1
1.1 IPv6 协议配置 1
1.2 IPv6 协议使能 1
1.2.1 IPv6 地址配置 1
第 2 章 配置 IPv6 服务 3
2.1 配置 IPv6 服务 3
2.1.1 管理 IPv6 连接 3
第 3 章 配置 RIPNG 6
3.1 概述 6
3.2 配置 RIPNG 任务列表 6
3.3 配置 RIPNG 任务 7
3.3.1 允许配置单播路由协议 7
3.3.2 启动 RIPNG 实例 7
3.3.3 Redistribute 非本实例路由 7
3.3.4 允许 RIPng 路由更新分组的单目广播 7
3.3.5 对路由权值应用偏移量 8
3.3.6 对收/发路由过滤 8
3.3.7 设置管理距离 8
3.3.8 调整计时器 8
3.3.9 手动汇总路由 9
3.3.10 最大路由条数 9
3.3.11 激活或禁止水平分割 9
3.3.12 监视和维护 RIPNG 9
3.4 RIPng 配置举例 10
第 4 章 配置 OSPFv3 12
4.1 概述 12
4.2 OSPFv3 配置任务列表 12
4.3 OSPFv3 配置任务 13
4.3.1 启动 OSPFv3 13
4.3.2 配置 OSPFv3 的接口参数 14
4.3.3 不同的物理网络上的 OSPFv3 配置 14
4.3.4 配置 OSPF 网络类型 14
4.3.5 配置 OSPFv3 域参数 15
4.3.6 配置 OSPFv3 域内路由的汇总 15
4.3.7 配置转发路由的汇总 15
4.3.8 生成默认路由 16
4.3.9 由 LOOPBACK 接口选择路由 ID 16
4.3.10 配置 OSPFv3 的管理距离 16

4.3.11 配置路由计算的计时器 16
4.3.12 监视和维护 OSPFv3 16
4.4 OSPFv3 配置举例 17
4.4.1 OSPFv3 路由学习配置举例 17
第 5 章 路由管理模块配置 24
5.1 概述 24
5.2 路由管理模块配置任务列表 24
5.3 路由管理模块配置任务 25
5.3.1 配置静态路由 25
5.3.2 配置路由表路由总数限制 25
5.3.3 监视和维护路由表状态 25
5.4 静态路由配置举例 26
第 6 章 配置物理端口 IPv6 访问列表 29
6.1 配置基于物理端口 IPv6 访问列表 29
6.1.1 过滤 IPv6 报文 29
6.1.2 建立 IPv6 访问列表 29
6.1.3 将访问列表应用到端口 30
6.1.4 访问列表示例 30
第 7 章 DHCPv6 配置 31
7.1 DHCPv6 client PD 前缀配置 31
7.2 开启 dhcpv6 中继功能 31
7.3 配置 dhcpv6 服务器功能 31
7.3.1 配置 ipv6 前缀池 31
7.3.2 配置 dhcpv6 前缀服务器功能 32
7.3.3 配置 dhcpv6 地址服务器功能 32
7.3.4 配置 DNS 服务器 33
7.3.5 配置 DNS IPv6 域名 33
7.3.6 配置租约时间 33
第 8 章 IPv6 Tunnel 配置 35
8.1 IPv6 手工配置隧道 35
8.1.1 配置条件 35
8.1.2 配置流程 35
8.2 IPv6 6to4 隧道 35
8.2.1 配置条件 35
8.2.2 配置流程 36
8.2.3 6to4 中继 36
8.3 IPv6 ISATAP 隧道 36
8.3.1 配置条件 36
8.3.2 配置流程 37
8.3.3 ISATAP 主机 37

第 9 章 NATPT 协议配置 38
9.1 NATPT 协议配置 38
9.2 NATPT 协议使能 38
9.2.1 端口下配置 ipv6 nat 命令 38
第 10 章 配置 NATPT 服务 39
10.1 配置 NATPT 服务 39
10.1.1 转换规则的管理 39
10.1.2 地址池的管理 40
10.1.3 转换映射管理 41
第 11 章 VRRP 配置 43
11.1 概述 43
11.2 VRRP IPv6 配置任务列表 43
11.3 VRRP IPv6 配置任务 43
11.3.1 端口开启/关闭 VRRP 43
11.3.2 配置 VRRP 说明信息 43
11.3.3 配置 VRRP 优先级抢占 44
11.3.4 配置 VRRP 优先级抢占延迟 44
11.3.5 配置 VRRP 优先级 44
11.3.6 配置 VRRP 时钟值 44
11.3.7 VRRP 的监控与维护 45
11.3.8 VRRP 配置示例 45
第 12 章 RADIUS 配置 48
12.1 概述 48
12.2 RADIUS IPv6 配置任务列表 48
12.3 RADIUS IPv6 配置任务 49
12.3.1 配置 NAS 的 Identifier 49
12.3.2 配置 NAS 的 ipv4 地址 49
12.3.3 配置 NAS 的 ipv6 地址 49
12.3.4 配置在 Access-Challenge 方式下用户数据不显示 49
12.3.5 配置 RADIUS 服务器不回应时的停止时间 50
12.3.6 配置允许用户以“@server”格式来指定 RADIUS 服务器 50
12.3.7 配置 RADIUS 服务器 50
12.3.8 配置 RADIUS 服务器密匙 51
12.3.9 配置初始 RADIUS 请求无需密码 51
12.3.10 配置 RADIUS 重发次数 51
12.3.11 配置等待 RAIDUS 服务器回答超时值 51
12.3.12 配置 RADIUS 附加属性等 51
12.3.13 配置 radius 服务器组的名称 52
12.3.14 在服务器组中增加服务器 52
12.3.15 指明 RADIUS 数据包的源 IP 地址 52

12.3.16 开启 debug 信息 53
12.3.17 配置示例 53

第1章 IPv6 协议配置

1.1 IPv6协议配置

路由器的 IPv6 地址相关设置仅在 VLAN interface 内有效，物理端口不能配置 IPv6 地址。

IPv6 协议在默认状态下未启用。如需在某个 VLAN 端口中使用 IPv6 协议，应在 VLAN 端口配置态下使能 IPv6 协议。IPv6 协议的使能通过配置 IPv6 地址实现。如某个 VLAN 端口下至少配置有一个 IPv6 地址，则该 VLAN 端口可以处理 IPv6 报文、于其他 IPv6 设备通信。反之如不存在任何 IPv6 地址，则协议不会使能。

为了使能 IPv6 协议，需至少完成下列任务：

- 在 VLAN 端口配置态下配置至少一个 IPv6 地址

1.2 IPv6协议使能

1.2.1 IPv6 地址配置

IPv6 地址确定了 IPv6 报文可以发送到的目的地址。IPv6 地址总共分为 3 类：

类别	参考格式	说明
单播地址	2001:0:0:0:0DB8:800:200C:417A/64	2001:0:0:0:0DB8:800:200C:417A为地址。同时需指明该地址的前缀长度（如参考格式中的64）
组播地址	FF01:0:0:0:0:0:0:101	组播地址均以FF开始。
任意播地址	2002:0:0:0:0DB8:800:200C:417A/64	格式同单播地址。不同VLAN端口可配置相同的任意播地址。发送往任意播地址的报文将“路由“至离发送者最近的一个配置任意播地址的VLAN端口。

更详细的 IPv6 地址的说明可以参考 RFC 4291。

为了使能 IPv6 协议，必须在 VLAN 端口配置态下配置一个单播地址。所配置的单播地址必须为下列地址中的一个或多个：

- IPv6 链路本地（Link-local）地址
- IPv6 全局（Global）地址

在 VLAN 端口配置态下配置 IPv6 链路本地地址：

命令	目的
ipv6 enable	自动配置一个链路本地地址
ipv6 address fe80::x link-local	手工配置一个链路本地地址

注意：

● 链路本地地址必须为 fe80 开始。前缀长度默认为 64。当手工配置时只能指定最后 64 位（bit）的值。

● VLAN 端口下只能配置一个链路本地地址。

● 通过配置链路本地地址使能 IPv6 协议后，协议能处理的“范围”仅为链路本地（即该 VLAN 端口上的 IPv6 协议仅在所连接的链路有效，关于 IPv6 地址的范围可参考 RFC 4007）。

在 VLAN 端口配置态下配置 IPv6 全局地址：

命令	目的
ipv6 address autoconfig	自动配置一个全局地址
ipv6 address [ipv6-address/prefix-length | prefix-name sub-bits/prefix-length] | [eui-64]	配置一个全局地址
ipv6 address X:X:X:X::X/<0-128> anycast	配置一个任意播地址

注意：

● 通过配置全局地址使能 IPv6 协议后，协议能处理的“范围”为所有互联的 IPv6 设备（关于 IPv6 地址的范围可参考 RFC 4007）。

● 如果在配置全局地址时还未配置链路本地地址，则系统会自动配置一个链路本地地址。

第2章　配置 IPv6 服务

2.1　配置IPv6服务

在使能 IPv6 协议之后，可以配置 IPv6 所提供的各种服务。以下为可配置的 IPv6 服务：

- 管理 IPv6 连接

2.1.1　管理 IPv6 连接

IPv6 提供了一系列的服务来控制和管理 IPv6 的连接。主要提供的服务为：

- ICMPv6 报文发送频率设置
- IPv6 源路由配置
- IPv6 最大传输单元配置（MTU）
- IPv6 重定向配置
- IPv6 目的不可达配置
- IPv6 访问列表配置
- IPv6 hop-limit 配置

1. ICMPv6 报文发送频率控制

限制 ICMPv6 的报文的发送频率。如果 ICMPv6 发送的频率大于所设定的值，则会限制发送的频率（即有丢弃一部分 ICMPv6 报文）。

该功能默认发送的频率为 1000us。如需修改可以在全局配置态下修改：

命令	目的
ipv6 icmp6-ratelimit *ratelimit*	设置ICMPv6报文的发送频率

2. IPv6 源路由配置

IPv6 允许主机指定通过 IPv6 网络的路由（源路由）。主机可以通过在 IPv6 报文中使用“路由头”（routing header，具体内容可参考 RFC 2460）来实现源路由。路由器可以根据“路由头”转发报文，或者出于安全考虑丢弃这类报文。

默认状态下路由器支持源路由。如被关闭，可在全局配置态下打开该功能：

命令	目的
ipv6 source-route	允许IPv6源路由

3. IPv6 最大传输单元配置（MTU）

所有的接口都有一个缺省的 IPv6 最大发送单元（MTU），也就是允许发送的最大 IPv6 报文长度。如果 IPv6 报文长度超过这个值的话，路由器就会对报文进行分片。

要设置特定接口上的 IPv6 MTU，在接口配置态使用下列命令：

命令	目的
ipv6 mtu bytes	配置接口的IPv6 MTU

4. IPv6 重定向配置

有时，主机所选择的路由不是最佳的，因此收到报文的路由器发现，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器。在这种情况下，路由器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器，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，路由器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器协议，则这项功能将被自动关闭。如果热备份路由器协议配置被取消，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 IPv6 重定向报文功能：

命令	目的
ipv6 redirects	允许IPv6发送重定向报文

5. IPv6 目的不可达配置

在多种情况下，系统会自动发送目的不可达报文。用户可以管理性地关闭该功能。关闭后系统即不发送 ICMP 目的不可达报文。

如果这一功能被关闭，可以在接口态下使用下列命令打开该功能

命令	目的
ipv6 unreachables	允许IPv6发送目的不可达报文

6. IPv6 访问列表配置

可以使用系统的访问列表控制某个 VLAN 端口收发报文的行为。通过在 VLAN 端口中引用全局配置态下的访问列表，并指明过滤方向即可启用 VLAN 端口对收发的 IPv6 报文进行过滤。

如果要使用该报文过滤功能，可以在接口态下配置

命令	目的
ipv6 traffic-filter *WORD* { in | out }	过滤VLAN端口在某个方向（in：收，out：发）的IPv6报文

7. IPv6 hop-limit 配置

用户可以指定路由器发送（转发报文除外）的报文中 hop-limit 字段的值。所有从本路由器发送的报文，如果上层应用没有显式指定 hop-limit 的值，则使用该所配置的 hop-limit 的值。同时该值会添入在路由器所发送的 RA 报文中。

默认的 hop-limit 为 64，如果需要改变该值可再接口配置态下修改：

命令	目的
ipv6 cur-hoplimit *value*	指定路由器发送报文的hop-limit

第3章　配置 RIPNG

3.1　概述

这一章描述怎样配置 RIPng。如果想得到本节中出现的 RIPng 命令的详细描述，请参考“网络协议命令参考”中的“RIPng 命令”一章。如果想查找本节中出现其它命令的文档，请使用命令参考主索引或在线查询。

下一代路由信息协议 RIPng 是 v6 下的 rip 协议，但是在设备中 ripng 和 rip 是两个完全独立的模块，分别负责 v6 和 v4 下的路由信息的学习和管理。

RIPng 在内部的运行机制上和 RIP 是一样的，Ripng 通过用户数据报协议 UDP 数据分组的广播来交换路由信息。在路由路由器中，每 30 秒钟发送一次路由信息的更新。如果一台路由路由器在 180 秒内没有接收到来自相邻路由路由器的更新，便把路由表中来自该路由路由器的路由标记为“不可用的”。如果接下去的 120 秒内仍然没有接收到更新，便把这些路由从路由表中删除。

RIPNG 也同样适用于小型网络。它使用跳跃计数（hop count）来作为衡量不同路由的权值。这个跳跃计数是指一个分组从信源到达新宿所经过的路由路由器的数目。直接相连网络的路由权值为 0，不可到达网络的路由权值为 16。由于 RIPNG 使用的路由权值范围较小，所以对大规模的网络就显得不大适合。

如果路由路由器有一条缺省路由，RIPNG 就宣告通向伪网络 0::0/0.的路由。实际上，网络 0::0/0 并不存在，它只是用来在 RIPNG 中实现缺省路由的功能。如果 RIPNG 学习到了一条缺省路由，或者路由路由器中设置了默认网关并配置了缺省权值，路由路由器都将宣告这个缺省的网络。

RIPNG 向被实例覆盖的接口发送路由更新。如果一个接口没有被配置为 ipv6 接口，将不能被 ripng 实例覆盖。

本公司路由路由器的 ripng 支持多实例。一个接口可以配置多个实例（最多四个），一个实例可以覆盖在多个接口上（最多四个）。

3.2　配置RIPNG任务列表

如果想配置 RIPNG，必须完成下面的任务。你首先要激活 RIPNG，其余的任务则是可选的。

- 允许配置单播路由协议
- 启动 RIPNG
- 允许 RIPNG 路由更新分组的单目广播
- 对路由权值应用偏移量
- 对收/发路由设置过滤
- 设置管理距离
- 调整计时器
- Redistribute 非本实例路由
- 手动汇总路由
- 最大路由条数

- 激活或禁止水平分割
- 监视和维护 RIPNG

3.3 配置RIPNG任务

3.3.1 允许配置单播路由协议

要配置 ripng 协议，必须先启用允许配置单播路由开关

命令	目的
Ipv6 unicast-routing	使能设备上单播路由协议的配置。

3.3.2 启动 RIPNG 实例

在接口配置模式下启动 ripng 实例进程，使用下面的命令：

命令	目的
ipv6 rip *instance-name* **enable**	在该接口上使能ripng协议。

要进入 ripng 实例，在全局配置模式使用下面的命令：

命令	目的
Ipv6 router rip *instance-name*	进入RIPng路由实例，进入该实例的配置模式。

注意：直接在接口上使能一个 ripng 实例，若该实例不存在将会生成该实例；也可以在全局配置模式下直接进入 ripng 实例，过该实例不存在也将生成该实例

在一个接口上 enable 多个 ripng 实例，最多不超过四个实例；同时一个 ripng 最多可以覆盖四个接口

3.3.3 Redistribute 非本实例路由

RIPNG 可以 redistribute 非本实例的路由信息到本实例的路由信息库里，然后以本实例信息库里的路由同别的设备进行路由交互。要达到这样的目的，在路由路由器 ripng 协议配置模式中使用如下命令：

命令	目的
Redistribute *protocol [instance-name | process-id]*	Redistribute 静态路由、ospfv6别的进程、ripng别的实例等的路由信息。

3.3.4 允许 RIPng 路由更新分组的单目广播

RIPNG 通常是一个多播型协议，如果要使 RIPng 路由更新能够到达非广播型网络，你必须对路由路由器进行配置以允许路由信息的交换。要达到这样的目的，在路由路由器 ripng 协议配置模式中使用如下命令：

命令	目的

neighbor *ipv6-address*	定义一个邻居路由路由器，与之交互路由信息。

另外，如果你想控制哪些接口可以用来交换路由信息，可以使用命令 ipv6 rip instance-name passive 指定在某个（某些）接口上禁止路由更新的发送。

3.3.5 对路由权值应用偏移量

偏移量列表是用来对那些由 RIPng 学习到的入站和出站路由增加一个偏移量。这就提供了一个本地的机制来增加路由权值。另外，你还可以使用访问列表或接口来限制偏移量列表。要增加路由权值，在路由路由器 ripng 协议配置模式中使用如下命令：

命令	目的
offset｛[interface-type number]|* ｝{**in**|**out**} *access-list-name* offset *value*	对路由权值增加一个偏移量。

3.3.6 对收/发路由过滤

通过设置，可以使 ripng 实例在相应的接口上对收发的路由进行过滤，以实现灵活的配置策略。要对路由过来，在路由路由器 ripng 协议配置模式中使用如下命令：

命令	目的
filter *interface-type interface-number* **{in | out}** access-list | gateway | prefix-list	对收/发的路由信息进行过滤。

3.3.7 设置管理距离

通过设置管理可以改变 ripng 实例路由的可信度。一般情况下，这个数值越大，可信任度就越小。要设置管理，在路由路由器 ripng 协议配置模式中使用如下命令：

命令	目的
distance *weight* [*X:X:X:X::X/*<0-128> [Acc-list_name]	设置ripng实例路由的管理距离。

3.3.8 调整计时器

路由协议使用几个计时器来判断发送路由更新的频率、多长时间内路由变为无效以及其它参数。你可以调整这些计时器使路由协议的性能更适合网络互联的需要。

也有可能调整路由协议来加速各种 Ipv6 路由算法的收敛时间，做到向冗余路由路由器的快速备份，以达到在需要快速恢复（quick recovery）的场合中向终端用户保证最小的崩溃时间。要调整计时器，在路由路由器 ripng 协议配置模式中使用如下命令：

命令	目的
timers holddown *value*	经过多长时间（单位：秒）从路由表中删除某一条路由。
timers garbage *value*	经过多长间隔（单位：秒）路由被宣告为无效。
timers update *value*	发送路由更新的频率（发送更新的间隔，单位：秒）。

3.3.9 手动汇总路由

RIPng 必须手动汇总路由信息，以减少和邻居交互的路由数量。在路由路由器 ripng 协议配置模式下，使用下面命令来汇总路由信息。

命令	目的
aggregate-address *ipv6-prefix/prefixlen*	汇总路由信息。

3.3.10 最大路由条数

缺省情况下，RIPng 本地路由表最大路由条数是 8192 条。当路由表中路由条数超过最大值时，不再向路由表中增加路由，同时提示用户路由表中路由条数已达最大值。在路由路由器配置模式下使用如下命令对 RIPng 本地路由表中最大路由条数进行配置：

命令	目的
max-routes *number*	配置RIPng本地路由表最大路由条数。
no max-routes	恢复缺省最大路由条数。

3.3.11 激活或禁止水平分割

正常情况下，与广播型 Ipv6 网络相连并使用距离向量路由协议的路由路由器采用水平分割机制来减小路由环路的可能性。水平分割阻塞路由信息向接收到该路由信息的接口进行宣告。这样做可以优化多个路由路由器间的通信（尤其是在环路打破的时候）。但是，对于非广播型网络（例如帧中继），情况并非那么理想。此时，你可能要禁止水平分割。

要激活或禁止水平分割，在 VLAN 配置模式下使用如下命令：

命令	目的
Ipv6 rip *instance-name* **split-horizon**	激活水平分割。
no ipv6 rip *instance-name* **split-horizon**	禁止水平分割。

在缺省情况下，对于点对点接口，水平分割是激活的；对于点对多点接口，水平分割是禁止的。

注意：

在一般情况下，推荐你不要改变缺省状态，除非你能肯定你的应用程序需要状态的改变才能正确地宣告路由。如果水平分割在一个串行接口上被禁止（并且与该接口相连的是一个分组交换网），你必须对该网络上任何相关多目广播组中的路由路由器禁止水平分割。

3.3.12 监视和维护 RIPNG

监视和维护 RIPng,可以显示网络的统计信息，如：RIPng **协议参数配置、使用网络、网络通信实时跟踪等**。这些信息能帮助你判断网络资源的利用，解决网络问题。能了解网络节点的可达性。

在管理态输入命令 ，使用下面的命令，可以显示各种路由统计信息。

命令	目的
show ipv6 rip *instance-name* summary	显示RIPng实例路由信息汇总。
show ipv6 rip *instance-name* database	显示RIPng实例所有路由。
show ipv6 rip *instance-name* interface	显示RIPng实例覆盖的所有接口。

在管理态输入命令 ，使用下面的命令，可以跟踪路由协议信息。

命令	目的
debug ipv6 rip *instance-name* database	跟踪RIPng实例的路由加入路由表、从路由表中删除路由、路由改变等过程信息。
debug ipv6 rip *instance-name* event	跟踪RIPng实例运行中出现异常以及ripng实例redistribute等过程信息。
debug ipv6 rip *instance-name* send	跟踪RIPng实例向外发送报文的过程信息。
debug ipv6 rip *instance-name* recv	跟踪RIPng实例接收报文的过程信息。
debug ipv6 rip *instance-name* msg	跟踪RIPng实例启动停止等重要事件的过程信息。
debug ipv6 rip *instance-name* all	跟踪RIPng实例全部的过程信息。

3.4 RIPng配置举例

这一节中包含 RIPng 配置的举例：

两台设备 A 和 B 直接相连，配置如下：

设备 A：

```
interface VLAN2
 no ip address
 no ip directed-broadcast
 ipv6 address 4444::4444/64
 ipv6 enable
 ipv6 rip dang2 enable
 ipv6 rip dang2 split-horizon
!
ipv6 router rip dang2
 redistribute static
 exit
!
!
```

设备 B：

```
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
 duplex half
 ipv6 address 4444::2222/64
```

```
 ipv6 enable
 ipv6 rip dang enable
 ipv6 rip dang split-horizon
!
ipv6 router rip dang
 redistribute static
 exit
!
```

这样他们都学习到了对方的静态路由信息

第4章　配置 OSPFv3

4.1　概述

这一章介绍 OSPFv3 的配置。为了更详细了解 OSPFv3 的全部命令，请参考网络协议配置参考中的有关 OSPFv3 命令的相关章节。

OSPFv3 是 IETF 的 OSPF 工作组开发的 IGP 路由协议，为 IPv6 网络设计的 OSPFv3 支持 IPv6 子网和外部路由信息标记，也允许报文的认证。

OSPFv3 和 OSPFv2 在很多方面是相同的：

- Router ID，Area ID 仍然是 32 位的。
- 相同类型的报文：Hello 报文，DD 报文，LSR 报文，LSU 报文和 LSAck 报文。
- 相同的邻居发现机制和邻接形成机制。
- 相同的 LSA 扩散机制和老化机制。

OSPFv3 和 OSPFv2 的不同主要有：

- OSPFv3 是基于链路（Link）运行，而 OSPFv2 是基于网段（Network）运行。
- OSPFv3 在同一条链路上可以运行多个实例。
- OPSFv3 是通过 Router ID 来标识邻接的邻居，而 OSPFv2 则是通过 IP 地址来标识邻接的邻居。
- OSPFv3 定义了七类 LSA。

本公司 OSPFv3 功能的实现遵守 OSPF V3 的要求（参见 RFC5340）。下面列出了实现中的一些关键特征：

关键特征	关键特征描述
Stub 域	支持stub域
路由转发	即被任何一种路由协议学习生成的路由都可以被转发到其他路由协议域。在自治域内，这表示OSPFv3能输入RIPng学习到的路由。OSPFv3学习到的路由也可以输出到RIPng。在自治域间，OSPFv3能输入 BGP学习到的路由； OSPFv3路由也能输出到BGP中去。
路由接口参数	可配置的接口参数有：输出花费、重传间隔、接口传输时延、路由器的优先级别、判定路由器的关机的时间间隔与hello包的时间间隔以及认证密钥。
虚链路	支持虚链路

4.2　OSPFv3配置任务列表

OSPFv3 要求在全部域内路由器、ABR 与 ASBR 之间进行交换路由数据。为了简化配置，可以让它们全部工作在默认参数，不需认证等；但如果要修改某些参数，则必须保证在所有路由器上的参数一致。

为了能配置 OSPFv3，完成下面的任务。除了激活 OSPFv3 是必须的外，其他配置都是可选配置。

- 启动 OSPFv3；
- 配置 OSPFv3 的接口参数；
- 在不同的物理网络上的 OSPFv3 配置；
- 配置 OSPFv3 域参数；
- 配置 OSPFv3 的 NSSA 域
- 配置 OSPFv3 域内路由的汇总
- 配置转发路由的汇总
- 生成默认路由
- 在 LOOPBACK 接口上选择路由 ID
- 配置 OSPFv3 的管理距离
- 配置路由计算的计时器
- 监视和维护 OSPFv3

另外，配置路由转发， 可以参见配置独立协议的 IPv6 路由协议的特性配置的转发路由信息的有关内容。

4.3 OSPFv3配置任务

4.3.1 启动 OSPFv3

在启动 OSPFv3 之前，需要先使能 IPv6 报文转发功能。

激活OSPFv3要求创建OSPFv3路由进程、指定该进程的Router ID 以及在接口上使能 OSPFv3 功能。在全局配置模式下，使用下面的命令：

命令	目的
router ospfv3 *process-id*	这个命令激活OSPFv3路由协议，并且进入路由配置模式。
router-id *router-id*	这个命令配置运行OSPFv3协议的路由器的Router ID。

在接口配置模式下，使用下面的命令：

命令	目的
ipv6 ospf *process-id* **area** *area-id* **[instance** *instance-id***]**	这个命令在接口上使能OSPFv3协议。

注意：若在接口上使能 OSPFv3 协议前，还没有创建该 OSPFv3 进程，会自动创建该进程。

4.3.2 配置 OSPFv3 的接口参数

在 OSPFv3 实现中，允许按照需要修改接口有关的 OSPFv3 参数。并不需要改变任何一个参数，但必须保证某些参数在相连网络的所有路由器上保持一致。

在接口配置模式，使用下面的命令配置接口参数：

命令	目的
ipv6 ospf cost *cost*	配置OSPFv6 接口发送包的开销值。
ipv6 ospf retransmit-interval *seconds*	配置邻居之间重传LSA的时间值。
ipv6 ospf transmit-delay *seconds*	配置在一个OSPFv3接口传输LSA的延迟时间。
ipv6 ospf priority *number*	配置路由器成为OSPFv3 DR路由器的优先值。
ipv6 ospf hello-interval *seconds*	配置在OSPFv3接口发送hello 包的时间间隔。
ipv6 ospf dead-interval *seconds*	在这个规定的时间间隔内，未收到邻居的任何OSPFv3报文，则认为邻居路由器已关机。

4.3.3 不同的物理网络上的 OSPFv3 配置

OSPFv3 把网络的物理媒体，分成以下三类：

- 广播网络(Ethernet, Token Ring, FDDI)
- 非广播、多访问网络 (SMDS, Frame Relay, X.25)
- 点对点网络 (HDLC, PPP)

能配置你的网络或者广播网络或者是非广播、多访问网络。

X.25 和帧中继网络提供了可选的广播能力，能通过 map 命令配置 OSPF 工作在广播网络。Map 命令可以参见广域网命令参考中有关 x.25 与帧中继的 map 命令的描述。

4.3.4 配置 OSPF 网络类型

不管网络的物理媒体类型，你都可以配置你的网络或者为广播网或者非广播、多访问网络。使用这个特性，你能灵活配置网络，可以将物理上的广播网络配置成非广播、多访问网络；也能配置非广播网络（X.25, Frame Relay, 与 SMDS）配置成为广播网络。这个特征也减少对邻居的配置，具体参见为非广播网络配置 OSPFv3 相关内容。

配置非广播、多访问网络为广播网络或者非广播网络，即假设从每一个路由器到其他路由器都存在虚链路，或假设为一个全网状网络。由于花费的限制，这常常是不现实的；或者有一个部分网状网。这种情形下，你可以配置成点到多点网络。不相邻的路由器之间可以通过虚链路交换路由信息。

OSPFv3 点到多点接口可以定义成多个点到点网络接口，它建立多个主机路由。OSPFv3 点到多点网络与非广播、多访问网络以及点到点网络相比，有以下优点：

- 点到多点网络容易配置，且不需产生 DR。
- 因为它不要求全网状拓扑，所以它的开销更小。
- 它更加可靠。即使在虚连路失败的情形下，也能保持连接。

交换机的网络类型是广播类型。

4.3.5 配置 OSPFv3 域参数

可以配置的区域参数有：认证、指定 Stub 区、为默认汇总路由指定权值。认证采用基于口令保护。

Stub 区域即不分发外部路由到该区的区域。取而代之的是，由 ABR 生成一条默认外部路由进入 stub 区域，使它能到达自治区域的外部网络。为了利用 OSPF Stub 支持的特性，在 Stub 区域必须使用默认路由，为了进一步减少发送进入 Stub 区域的 LSA 数，你能在 ABR 禁止汇总（No Summary）来减少发送汇总 LSA（类型 3）进入 Stub 区域。

在路由器的路由配置模式，使用下面的命令设定区域参数：

命令	目的
area *area-id* **stub** [no-summary]	定义一个stub区。
area *area-id* **default-cost** *cost*	为Stub区域的默认路由设定权值。

对于没有和骨干区域直接相连的非骨干区域，或者不连续的骨干区域，可以使用 OSPFv3 的虚链路建立逻辑上的连通性。为了建立一条虚链路， 必须在这个虚链路的两端都进行配置，如果只在一端配置，这个虚链路将无法工作。

在路由器的路由配置模式，使用下面的命令设定区域参数：

命令	目的
area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transdly** *dly-value*]	建立虚链路。

4.3.6 配置 OSPFv3 域内路由的汇总

这个特性使得 ABR 广播一条汇总路由到其他区域。在 OSPFv3 中，ABR 将广播每一个网络到其他区域。如果网络号按照某种方式分配，使得它们连续，你能配置 ABR 广播一条汇总路由到其他区。汇总路由能覆盖一定范围的所有网络。

在路由器的路由配置模式，使用下面的命令设定地址范围：

命令	目的
area *area-id* **range** *ipv6-prefix /prefix-length*	设定汇总路由的地址范围。

4.3.7 配置转发路由的汇总

当从其他路由区域分发路由到 OSPFv3 路由区域时，每条路由以外部 LSA 的方式进行单独广播。然而你能配置路由器广播一条路由，它能覆盖一定的地址范围。这种方式可以减少 OSPFv3 链路状态数据库的大小。

在路由器的路由配置模式，使用下面的命令，配置汇总路由：

命令	目的
summary-prefix *ipv6-prefix /prefix-length*	描述覆盖分发路由的地址与掩码，仅仅一条汇总路由被广播。

4.3.8 生成默认路由

能要求 ASBR 生成一条默认路由进入 OSPFv3 路由域。无论何时，你配置路由器分发路由进入 OSPFv3 路由域，该路由自动变成 ASBR。然而，ASBR 默认并不生成默认路由进入 OSPFv3 路由域。

4.3.9 由 LOOPBACK 接口选择路由 ID

OSPFv3 使用配置在接口的最大 IPv4 地址作为它的路由器 ID。如果与这个 IPv4 地址相连的接口变为 DOWN 状态，或者该 IPv4 地址被删除，OSPF 进程将重新计算新的路由器 ID 并且重新从所有接口发送路由信息。

如果一个 loopback 接口配置了 IPv4 地址，则路由器优先使用 loopback 的 IPv4 地址作为它的路由器 ID，由于 loopback 接口永远不会 Down，所以使得路由表具有较大的稳定性。

路由器优先选用 Loopback 接口作为路由器 ID，同时也选择所有 Loopback 接口中最大的 IPv4 地址作为路由器 ID。如果没有 Loopback 接口，则使用路由器的最大 IPv4 地址。你不能指定 OSPFv3 使用任何特定的接口。

在全局模式下，使用下面的命令，配置 IP Loopback 接口。

命令	目的
interface loopback *num*	创建一个loopback接口且进入接口配置模式。
ip address *ip-address mask*	为接口分配一个IPv4 地址。

4.3.10 配置 OSPFv3 的管理距离

管理距离是路由信息源的信任等级。一般来说，管理距离是 0－255 之间的整数，值越大，信任级别越低。如果管理距离为 255，则路由信息源不被信任且应当被忽略。

OSPFv3 使用三类不同的管理距离：域间、域内和外部。在一个区域内的路由是域内；到其他区域的路由是区域间；其他路由协议域分发来的路由为外部。每种类型路由的默认值为 110。

4.3.11 配置路由计算的计时器

你能配置 OSPFv3 收到拓扑变化消息与开始计算 SPF 之间的时延。也能配置连续两次 SPF 计算之间的间隔。在路由器的路由配置模式下，使用下面的命令进行配置：

命令	目的
timers delay *delaytime*	设定在一个域中路由计算的时间延迟。
timers hold *holdtime*	设定在一个域中路由计算的最小时间间隔。

4.3.12 监视和维护 OSPFv3

能显示网络的统计信息，如：IP 路由表的内容、缓冲和数据库等数据。这些信息能帮助你判断网络资源的利用，解决网络问题。能了解网络节点的可达性，发现网络数据包经过网络的路由。

使用下面的命令，可以显示各种路由统计信息：

命令	目的
show ipv6 ospf [*process-id*]	显示OSPFv3 路由进程的一般信息。
show ipv6 ospf [*process-id*] **database** **show ipv6 ospf** [*process-id*] **database [router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [network] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-prefix] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [external] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [link] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [intra-prefix] [adv-router** *router-id***]**	显示OSPFv3数据库的相关信息。
show ipv6 ospf interface	显示有关OSPFv3接口的信息。
show ipv6 ospf neighbor	显示OSPFv3的邻居信息。
show ipv6 ospf route	显示OSPFv3的路由信息。
show ipv6 ospf topology	显示OSPFv3的网络拓扑信息。
show ipv6 ospf virtual-links	显示OSPFv3的虚链路信息。
debug ipv6 ospf	监视OSPFv3的所有行为。
debug ipv6 ospf events	监视OSPFv3的事件。
debug ipv6 ospf ifsm	监视OSPFv3的接口状态机。
debug ipv6 ospf lsa	监视OSPFv3的LSA的相关行为。
debug ipv6 ospf nfsm	监视OSPFv3的邻居状态机。
debug ipv6 ospf nsm	监视路由管理模块通知OSPFv3的消息。
debug ipv6 ospf packet	监视OSPFv3的报文。
debug ipv6 ospf route	监视OSPFv3的路由信息。

4.4 OSPFv3配置举例

4.4.1 OSPFv3 路由学习配置举例

OSPFv3 要求在众多内部路由器、ABR 与 ASBR 间交换信息。在最小配置下，基于 OSPFv3 的路由器可以在默认参数下工作，没有认证要求。

下面是三个配置例子：

第一个例子演示基本的 OSPFv3 配置命令。

第二个例子演示在一台路由器上配置多个 OSPFv3 进程。

第三个例子演示一个比较复杂的利用 OSPFv3 学习路由的配置例子。

第四个例子演示 OSPFv3 虚链路的配置例子。

1. 基本 OSPFv3 配置例子

下面的例子说明一个简单的 OSPFv3 配置。激活路由进程 90，连接以太口 0 到区域 0.0.0.0。同时分发 RIPng 到 OSPFv3，OSPFv3 到 RIPng。

```
ipv6 unicast-routing
!
interface vlan 10
ipv6 address 2001::1/64
ipv6 enable
ipv6 rip aaa enable
ipv6 rip aaa split-horizon

ipv6 ospf 90 area 0
ipv6 ospf cost 1
!
router ospfv3 90
router-id 1.1.1.1
redistribute rip
!
router ripng aaa
redistribute ospf 90
```

2. 配置多个 OSPFv3 进程例子

下面的例子创建了两个 OSPFv3 进程。

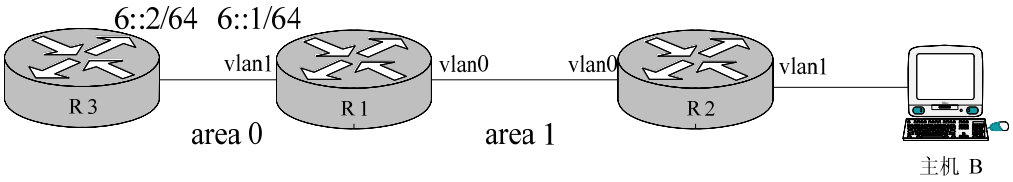
```
ipv6 unicast-routing
!
!
interface vlan 10
  ipv6 address 2001::1/64
   ipv6 enable

   ipv6 ospf 109 area 0 instance 1
   ipv6 ospf 110 area 0 instance 2
!
!
interface vlan 11
  ip address 2002::1/64
   ipv6 enable

 ipv6 ospf 109 area 1 instance 1
 ipv6 ospf 110 area 1 instance 2
!
!
router ospfv3 109
```

```
  router-id 1.1.1.1
   redistribute static
!
router ospfv3 110
  router-id 2.2.2.2
!
```

每个接口可以属于多个 OSPFv3 进程，但是当一个接口属于多个 OSPFv3 进程时，每个 OSPFv3 进程对应的 instance 必须不同。

3. 比较复杂的配置例子

下面的例子演示了在单个 OSPFv3 自治系统内，多个路由器的配置。下图是配置例子的网络拓扑图。



按照上图配置路由器。

```
R1:
interface vlan 0
     ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
     ipv6 enable

    ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 1.1.1.1
    redistribute static
!

R2:
interface vlan 0
     ipv6 enable

    ipv6 ospf 1 area 1
!
!
router ospfv3 1
   router-id 2.2.2.2
!
```

查看 R2 的路由表信息:

```
R2#show ipv6 route
O        6::/64[1]
          [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
O        2001::/64[1] （转发路由）
          [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C        fe80::/10[1]
          is directly connected, L,Null0
C        fe80::/64[1]
          is directly connected, C, VLAN0
C        fe80::2e0:fff:fe26:a8/128[1]
          is directly connected, L, VLAN0
C        ff00::/8[1]
          is directly connected, L,Null0
```

可以看出路由器 R2 学习到了转发路由。

配置 area 1 为 stub 区域:

R1:

```
interface vlan 0
    ipv6 enable

   ipv6 ospf 1 area 1
!
interface vlan 1
    ipv6 enable

   ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 1.1.1.1
   area 1 stub
    redistribute static
!
```

R2:

```
interface vlan 0
    ipv6 enable

   ipv6 ospf 1 area 1
!
!
router ospfv3 1
   router-id 2.2.2.2
   area 1 stub
!
```

查看 R2 的路由表信息

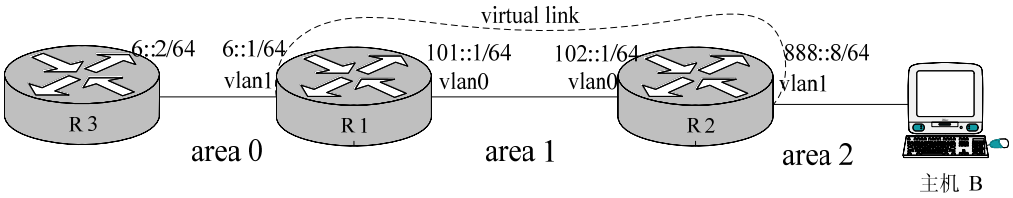
```
R2#show ipv6 route
O        ::/0[1]
          [110,11] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
```

```
O        6::/64[1]
          [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C        fe80::/10[1]
          is directly connected, L,Null0
C        fe80::/64[1]
          is directly connected, C, VLAN0
C        fe80::2e0:fff:fe26:a8/128[1]
          is directly connected, L, VLAN0
C        ff00::/8[1]
          is directly connected, L,Null0
```

可以看出 stub 区中的 abr 能正常产生一个默认路由，并通知区中其它路由器，而且 stub 区域中没有引入 ASE LSA。

4. 虚链路的配置例子

下面的例子演示了在单个 OSPFv3 自治系统内，虚链路的配置。下图是配置例子的网络拓扑图。



按照上图配置路由器。

```
R1:
interface vlan 0
    ipv6 address 101::1/64
     ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
    ipv6 address 6::1/64
     ipv6 enable

    ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 200.200.200.1
   area 1 virtual-link 200.200.200.2
   redistribute static
!

R2:
interface vlan 0
    ipv6 address 101::2/64
```

```
    ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
    ipv6 address 888::8/64
    ipv6 enable

    ipv6 ospf 1 area 2
!
!
router ospfv3 1
  router-id 200.200.200.2
  area 1 virtual-link 200.200.200.1
!
```

查看 OSPFv3 邻居状态:

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri    State          Dead Time    Interface    Instance ID
200.200.200.2     1     Full/DR        00:00:35     VLAN0        0
200.200.200.2     1     Full/ -        00:00:36     VLINK1       0

R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
OSPFv3 Process (1)
Neighbor ID      Pri    State          Dead Time    Interface    Instance ID
200.200.200.1     1     Full/Backup    00:00:36     VLAN0        0
200.200.200.1     1     Full/ -        00:00:37     VLINK1       0
```

查看路由表信息

```
R1#show ipv6 route
C        6::/64[1]
          is directly connected, C,VLAN1
C        6::1/128[1]
          is directly connected, L, VLAN1
C        101::/64[2]
          is directly connected, C, VLAN0
C        101::1/128[2]
          is directly connected, L, VLAN0
O        101::2/128[2]
          [110,10] via fe80:4::2e0:fff:fe26:a8(on VLAN0)
O        888::/64[2]
          [110,20] via fe80:4::2e0:fff:fe26:a8(on VLAN0)
S        2001::/64[1]
          [1,0] via 6::2(on VLAN1)
C        fe80::/10[2]
          is directly connected, L,Null0
C        fe80::/64[2]
          is directly connected, C, VLAN0
C        fe80::2e0:fff:fe26:2d98/128[2]
          is directly connected, L, VLAN0
C        fe80::/64[1]
          is directly connected, C, VLAN1
```

```
C        fe80::2e0:fff:fe26:2d99/128[1]
          is directly connected, L, VLAN1
C        ff00::/8[2]
          is directly connected, L,Null0

R2#show ipv6 route
O        6::/64[1]
          [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C        101::/64[1]
          is directly connected, C, VLAN0
O        101::1/128[1]
          [110,10] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C        101::2/128[1]
          is directly connected, L, VLAN0
C        888::/64[1]
          is directly connected, C, VLAN1
C        888::8/128[1]
          is directly connected, L, VLAN1
O        2001::/64[1]
          [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C        fe80::/10[1]
          is directly connected, L,Null0
C        fe80::/64[1]
          is directly connected, C, VLAN0
C        fe80::2e0:fff:fe26:a8/128[1]
          is directly connected, L, VLAN0
C        fe80::/64[1]
          is directly connected, C, VLAN1
C        fe80::2e0:fff:fe26:a9/128[1]
          is directly connected, L, VLAN1
C        ff00::/8[1]
          is directly connected, L,Null0
```

第5章　路由管理模块配置

5.1　概述

这一章描述怎样配置路由管理模块的相关内容，包括静态路由的相关配置，以及一些路由表属性的配置，本节中涉及的命令的详细描述，请参考“网络协议命令参考”中的“路由管理模块命令”一章。如果想查找本节中出现其它命令的文档，请使用命令参考主索引或在线查询。

静态路由是一种特殊的路由，由管理员手工配置；配置静态路由后，去往指定目的地的数据报文将按照管理员指定的路径进行转发。

在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由的缺点在于：不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

如果到达某个指定网络的数据报文在设备的路由表里找不到对应的表项，那么该报文将被设备丢弃。

通过给当前设备配置一条缺省路由，那些在路由表里找不到匹配路由表入口项的数据报文将会转发给另外一台设备（如果这台设备的路由能力比较强，包括到达大部分所有网络的路由信息），由另外一台设备进行报文的转发。

缺省路由是在设备没有找到匹配的路由表入口项时才使用的路由：

如果报文的目的地址不能与路由表的任何入口项相匹配，那么该报文将选取缺省路由；

如果没有缺省路由且报文的目的地不在路由表中，那么该报文将被丢弃，将向源端返回一个 ICMPv6 报文报告该目的地址或网络不可达。

缺省路由有两种生成方式：

第一种是通过网络管理员在设备上配置到网络 0::0/0 的静态路由，对于一个到来的数据报文，如果在当前设备里找不到匹配的路由表项，将会把报文发给在配置的静态路由里指定的下一跳端口；

第二种是通过动态路由协议生成（如 OSPFv6、IS-Isv6 和 RIPng），由路由能力比较强的设备将缺省路由发布给其它设备，其它设备在自己的路由表里生成指向那台设备的缺省路由。

5.2　路由管理模块配置任务列表

路由管理模块包括以下几个配置任务。

- 配置静态路由
- 配置路由表路由总数限制
- 检测静态路由下一跳是否可达

5.3 路由管理模块配置任务

5.3.1 配置静态路由

要配置静态路由，需要进入全局配置模式，使用以下命令进行：

命令	目的
Ipv6 route *prefix / prefixlen* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*distance*]	配置静态路由

在配置静态路由时，可指定出接口 *interface-type interface-number*，也可指定下一跳地址。指定出接口还是指定下一跳地址要视具体情况而定，下一跳地址不能为本地接口 Ipv6 地址，否则路由不会生效。

在使用 **ipv6 route** 配置静态路由时，如果将目的地址与掩码配置为全零（0::0/0），则表示配置的是缺省路由。配置的 prefix 的 prefixlen 应该少于等于 64，或者等于 128（主机路由）

对于不同的静态路由，可以为它们配置不同的管理距离，从而更灵活地应用路由管理策略。例如：配置到达相同目的地的多条路由，如果指定相同管理距离，则可实现负载分担，如果指定不同管理距离，则可实现路由备份。

配置的静态路由的下一跳必须是激活的，否则静态路由将不能被激活：当下一跳为 interface 或者 interface vlan 的时候，这个接口须是 v6 接口；当配置的下一跳为网关时，这个网关须在直连网段内

5.3.2 配置路由表路由总数限制

要对路由表的最大路由条目数限制，需要进入全局配置模式，使用以下命令进行：

命令	目的
Ipv6 route max-number *<64-640000>*	设定总的路由数，合理分配系统资源，提供设置出来速度。

5.3.3 监视和维护路由表状态

在管理态输入命令，使用下面的命令，可以显示各种路由统计信息。

命令	目的
show ipv6 route	显示主路由表信息
show ipv6 route [*protocol*]	显示路由表中对应路由协议的路由信息
show ipv6 route summary	显示主路由表统计信息
show ipv6 fib route	显示主转发表fib中条目信息
show ipv6 fib summary	显示转发表相关统计信息

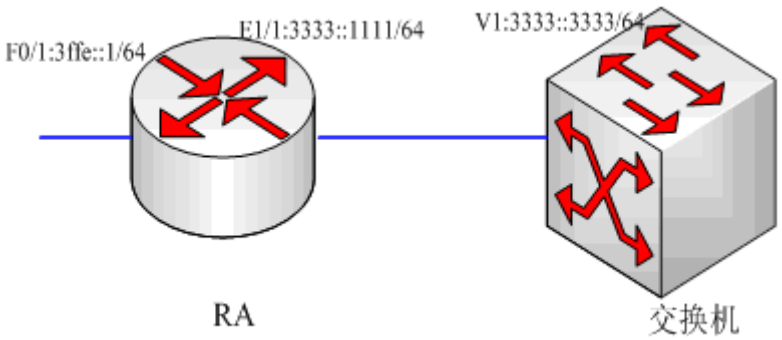
Show ipv6 route summary (line card)	显示线卡上路由表相关统计信息
Show ipv6 route information (line card)	显示线卡上当前状态信息
Show ipv6 route [delete | stale | un-lpm | no-lla | ipv6-address] (line card)	显示线卡上各种路由信息

在管理态，使用下面的命令，可以跟踪路由管理模块发生的相关事件和信息。

命令	目的
debug ipv6 routing message	跟踪rtv6消息的接收和发送
debug ipv6 routing search	跟踪路由查找
debug ipv6 routing timer	跟踪rtv6时钟信息
Debug ipv6 routing redis	跟踪rtv6 redistribute信息
debug ipv6 fib cache	跟踪rtv6 cache信息
Debug ipv6 fib message	跟踪rtv6 转发表消息信息
Debug ipv6 routing exf (line card)	跟踪线卡上添加exf信息
Debug ipv6 routing packet (line card)	跟踪线卡主控线卡间报文交互信息
Debug ipv6 routing message (line card)	跟踪线卡上和主控交互信息
Debug ipv6 routing cache (line card)	跟踪线卡上cache相关信息
Debug ipv6 routing route (line card)	跟踪线卡上路由变化相关信息
Debug ipv6 routing search (line card)	跟踪线卡上查找路由信息

5.4 静态路由配置举例

如下图所示，路由器 RA 和一台 85 路由器直接相连。



RA 的配置：

```
interface FastEthernet0/1
  no ip address
```

```
 no ip directed-broadcast
 ipv6 address 3FFE::1/64
!
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
 duplex half
 ipv6 address 3333::1111/64
!
```

S 的配置：

```
interface VLAN1
 no ip address
 no ip directed-broadcast
 ipv6 address 3333::3333/64
!
!
```

查看 RA 的 local link 地址：

```
RA_config#show ipv6 route
Codes: C - Connected, L - Local, S - Static, R - Ripng, B - BGP
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type
VRF ID: 0
C      3333::/64[1]
        is directly connected, C,Ethernet1/1
C      3333::1111/128[1]
        is directly connected, L,Ethernet1/1
C      3ffe::/64[1]
        is directly connected, C,FastEthernet0/1
C      3ffe::1/128[1]
        is directly connected, L,FastEthernet0/1
C      fe80::/10[1]
        is directly connected, L,Null0
C      fe80::/64[1]
        is directly connected, C,FastEthernet0/1
C      fe80::a00:3eff:fed5:effc/128[1]
        is directly connected, L,FastEthernet0/1
C      fe80::/64[1]
        is directly connected, C,Ethernet1/1
C      fe80::a00:3eff:fed5:effd/128[1]
        is directly connected, L,Ethernet1/1
C      ff00::/8[1]
        is directly connected, L,Null0
!
```

在 S 上配置到 3ffe::/64 子网的静态路由：

```
!
ipv6 route 3ffe::/64 3333::1111
!
```

或者：

```
!
```

```
ipv6 route 3ffe::/64 VLAN1 fe80::a00:3eff:fed5:effd
!
```

第6章　配置物理端口 IPv6 访问列表

6.1　配置基于物理端口IPv6访问列表

6.1.1　过滤 IPv6 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，本公司路由路由器提供了访问列表。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 IPv6 访问列表以及如何应用它们。

IPv6 访问列表是应用 IPv6 地址的允许和禁止条件的有序集合。本公司路由路由器的 ROS 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。

6.1.2　建立 IPv6 访问列表

用一个字符串建立 IPv6 访问列表。

为了建立 IPv6 访问列表，在全局配置态执行下列命令。

命令	目的
Ipv6 access-list *name*	使用名字定义一个标准的IPv6访问列表。
{**deny** | **permit**} *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**sequence** *value*] {**deny | permit**} *protocol* **any any**	在IPv6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。

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。

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。

6.1.3 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。

在端口配置态使用以下命令。

命令	目的
ipv6 access-group *name in/out*	将ipv6访问列表应用到端口。

访问列表用在入接口。在接收到包之后，对照访问列表检查包的源地址以及目的地址。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。

如果指定的访问列表不存在，所有的包允许通过。

6.1.4 访问列表示例

在以下例子中，第一行允许新来的 TCP 与主机 2001:1::2E0:FFF:FE8E:700B 的 TELNET 端口连接。

```
ipv6 access-list aaa
    permit tcp any host 2001:1::2E0:FFF:FE8E:700B eq 23

interface   g1/10
    ipv6 access-group aaa in
```

第7章 DHCPv6 配置

7.1 DHCPv6 client PD前缀配置

在端口配置模式下进行下列配置：

命令	目的
Ipv6 dhcp pd *prefix_name* [rapid-commit]	开启DHCPv6 pd client功能。
no ipv6 dhcp pd *prefix_name*	恢复缺省设置。

该命令是启动 DHCPv6 pd client 功能的控制命令。配置该命令，则设备侦听所有 DHCPv6 前缀代理请求。

其中 prefix_name 可以被当做前缀来使用，譬如在配置 ipv6 端口地址的时候。

7.2 开启dhcpv6 中继功能

在端口配置模式下进行下列配置：

命令	目的
ipv6 dhcp relay destination *ipv6_address*	开启DHCPv6 relay功能。
no ipv6 dhcp relay destination *ipv6_address*	恢复缺省设置。

ipv6 dhcp relay destination 命令用于配置 relay 的目的地址。可以是另外的 relay agent 的地址也可以是服务器的地址。

如果需要配置多个目的地址，可以多次配置该命令。

DHCPv6 的 client、relay、server 功能在一个接口上是互斥的，也就是说在一个接口上只能配置成一种模式。

7.3 配置dhcpv6 服务器功能

7.3.1 配置 ipv6 前缀池

在全局配置模式下进行下列配置：

命令	目的
ipv6 local pool *poolname prefixlprefix-length assigned-length*	配置ipv6前缀池。

no ipv6 local pool poolname	删除ipv6前缀池。

配置前缀池是为了让 dhcpv6 的地址池调用，来分配前缀地址。

7.3.2 配置 dhcpv6 前缀服务器功能

此功能打开需要先配置一个 ipv6 前缀池，例如：

ipv6 local pool *pd1 100::1/56 64*

在全局配置模式下进行下列配置，进入 dhcpv6 池特殊配置模式：

ipv6 dhcp pool *dhpool1*

在 dhcpv6 特殊配置下进行下列配置：

命令	目的
prefix-delegation pool *poolname*	指定ipv6前缀池。
no prefix-delegation pool	删除ipv6前缀池。

或者进行配置

命令	目的
prefix-delegation *ipv6_prefix/prefix_length client_DUID* [**iaid** *IAID*]	指定ipv6前缀。
no prefix-delegation *ipv6_prefix/prefix_length client_DUID* [**iaid** *IAID*]	删除ipv6前缀

在端口配置态下启用 dhcpv6 server 功能，在端口配置态下进行下列配置：

命令	目的
ipv6 dhcp server *poolname* [allow-hint | preference *num*| rapid-commit]	打开dhcpv6 server功能。
no ipv6 dhcp server *name*	关闭dhcpv6 server功能

7.3.3 配置 dhcpv6 地址服务器功能

在 dhcpv6 池特殊配置模式态下进行下列配置：

命令	目的
non-temporary-address block	配置ipv6地址。

ipv6_address_start ipv6_address_end	
no non-temporary-address block *ipv6_address_start ipv6_address_end*	删除ipv6地址

为了方便地址划分，提供了块地址配置：

命令	目的
non-temporary-address block *ipv6_address/len*	配置ipv6地址。
no non-temporary-address block *ipv6_address/len*	删除ipv6地址

Len 可以看做是掩码，地址数量是 2^len-1 个。

配置完地址池以后，需要在端口上启用 dhcpv6 功能。

相关命令：

ipv6 dhcp server *poolname* [allow-hint | preference *num*| rapid-commit]

7.3.4 配置 DNS 服务器

在 dhcpv6 池特殊配置模式态下进行下列配置：

命令	目的
Dns-server *ipv6_address*	配置分配给client的dns服务器地址。
no dns-server*s*	删除dns服务器

此命令主要是为了将 DNS 地址分配给客户端。

7.3.5 配置 DNS IPv6 域名

在 dhcpv6 池特殊配置模式态下进行下列配置：

命令	目的
Domain-name *domain*	配置分配给client的dns域名。
no domain-name	删除域名

7.3.6 配置租约时间

在 dhcpv6 池特殊配置模式态下进行下列配置：

命令	目的
Lifetime *valid-time preferred-time*	配置分配给client的租约时间。
no lifetime	恢复默认租约时间

Valid-time 缺省 43200（30 天)

Preferred-time 缺省 10080（7 天）

第8章 IPv6 Tunnel 配置

IPv6 Tunnel 是由 IPv6 报文作为 IPv4 的载荷，并跨越 IPv4 网络以连接各个 IPv6 孤岛。其配置必须在 tunnel 类型的端口下进行。配置的基本流程：

- 配置隧道接口
- 配置隧道接口 IPv6 地址
- 配置隧道源 IPv4 地址
- 配置隧道目的 IPv4 地址（可选）
- 配置封装 ipv6 隧道协议
- 配置路由

IPv6 隧道协议分为手工配置隧道、6to4 隧道、ISATAP 隧道。

8.1 IPv6手工配置隧道

8.1.1 配置条件

IPv6 手工配置隧道需要在一个拥有 IPv6 地址的 tunnel 端口下运行。并且，该端口必须手动配置源端和目的端的 IPv4 地址。手工配置隧道的两端都必须同时支持 IPv4 和 IPv6 协议栈。由于这种隧道方式需要明确配置隧道端点，所以通常用在路由器到路由器之间建立隧道的情况。

8.1.2 配置流程

interface tunnel *tunnel-num*	配置隧道接口
ipv6 address { ipv6-address/prefix-length | prefix-name sub-bits/prefix-length }	配置隧道接口IPv6地址
tunnel source {ip-address | interface-type interface-number}	配置隧道源源IPv4地址
tunnel destination ip-address	配置隧道目的IPv4地址
tunnel mode ipv6ip	配置封装ipv6手工隧道协议

8.2 IPv6 6to4隧道

8.2.1 配置条件

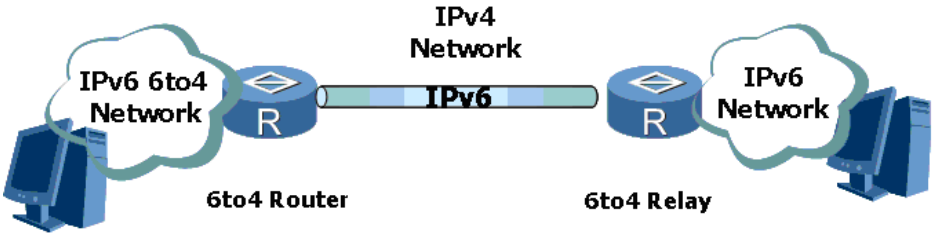
IPv6 6to4 隧道用来为 IPv4 网络中的 IPv6 孤岛提供互通的手段，并且使配置隧道的工作尽量少。这种方式要求每个 IPv6 孤岛至少有一个全网唯一的 IPv4 地址，该地址被 IPv6

孤岛的边缘路由器作为 6to4 隧道的源 ipv4 地址，并由此构造自己的 IPv6 地址前缀 2002:border-router-IPv4-address::/48，因此该前缀也是全网唯一的。6to4 隧道的目的 IPv4 地址不需要手动配置，而是由 IPv6 目的地址中提取出隧道末端的 IPv4 地址，隧道的构造过程可以自动进行。6to4 隧道的两端都必须同时支持 IPv4 和 IPv6 协议栈。

8.2.2 配置流程

interface tunnel *tunnel-num*	配置隧道接口
ipv6 address { *ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length* **}**	配置隧道接口IPv6地址（其前缀必须于隧道源地址匹配）
tunnel source {ip-address | interface-type interface-number}	配置隧道源源IPv4地址
tunnel mode ipv6ip 6to4	配置封装ipv6 6to4隧道协议

8.2.3 6to4 中继



在 6to4 隧道技术中 IPv6 网络之间互联要求网络前缀必须是 2002 开头的，即 6to4 网络必须使用 6to4 地址。但是，6to4 网络作为整个网络的一部分，还可能需要和其它的纯 IPv6 网络互连。为了解决这个问题，需要采用 6to4 中继。

在一个 6to4 域和一个纯 IPv6 域中间，需要至少一个 6to4 中继以保证连通性。如上图，6to4 中继一般位于 IPv4 因特网和 IPv6 因特网的交界。6to4 路由器在它的连接到 IPv6 因特网的接口上广播 2002::/16 的网络前缀加入 IPv6 单播路由网络。要使用 6to4 中继，必须在 6to4 边缘路由器上配置一条缺省路由指向 6to4 中继。需要注意，目前 8000 系列路由器中只支持 6to4 的流量通过 6to4 中继被发送到 IPv6 因特网中，即 6to4 边缘路由器下连的 IPv6 网络中，只有那些 IPv6 地址是 6to4 地址的主机才能够通过隧道与另一端的主机通信。

8.3 IPv6 ISATAP隧道

8.3.1 配置条件

IPv6 ISATAP 隧道主要用于在 IPv4 网络中将一些孤立的 IPv6 主机与 IPv6 网络进行连接。这种连接的一端是支持 ISATAP 的 IPv6 IPv4 双栈主机，另一端是 ISATAP 路由器。使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的地址：ISATAP 地址。ISATAP 地址格式为：Prefix（64bit）:0:5EFE:IPv4ADDR（IPv4ADDR 即隧道端口的 IPv4 源地址。通过这个嵌入的 IPv4 地址就可以自动建立隧道，完成 IPv6 报文的传送。因此，ISATAP 隧道的 IPv6 地址必须是一个 modified EUI-64 地址。

需要注意，目前 8000 系列路由器只能作为 ISATAP 路由器使用，而不能作为 ISATAP 主机。

8.3.2 配置流程

interface tunnel *tunnel-num*	配置隧道接口
ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]	配置隧道接口IPv6地址
tunnel source {ip-address | interface-type interface-number}	配置隧道源源IPv4地址
tunnel mode ipv6ip isatap	配置封装ipv6 isatap隧道协议

8.3.3 ISATAP 主机

ISATAP 隧道的一端为主机，其 ipv6 地址一般为无状态配置。ISATAP 主机通过源端 ipv4 地址自动生成 ipv6 本地链路地址，然后通过 ISATAP 隧道向 ISATAP 路由器发送路由器请求（RS），随后 ISATAP 路由器会发送一个路由器通告消息（RA），包含有 ISATAP 前缀。收到 ISATAP 前缀后，ISATAP 主机获得全局 ipv6 地址，并将该 ISATAP 路由器加入到潜在路由表中。

由于 ISATAP 路由器无法主动向隧道另一端的主机发送路由器通告（RA）报文，所以路由器端配置的 RA 存活时间必须大于主机端发送 RS 的时间间隔。

isatap 主机配置：

在命令行窗口下依次输入

ipv6 install

netsh

interface ipv6 isatap

set router *ipv4-addr* (*ipv4-addr 为 isatap 路由器的隧道源端 ipv4 地址*)

第9章　NATPT 协议配置

9.1　NATPT协议配置

NATPT 协议在默认状态下未启用。如需使用 NATPT 协议对报文进行 v4 和 v6 域的转换，应在端口配置态下使能 NATPT 协议，并且执行配置服务设置正确的配置转换规则。IPv6 协议的使能通过在需要收发报文的端口上配置 ipv6 nat 命令实现。

为了使能 NATPT 协议，需至少完成下列任务：

- 在至少一个 IPv4 端口和至少一个 IPv6 端口的端口配置态下配置 ipv6 nat 命令

9.2　NATPT协议使能

9.2.1　端口下配置 ipv6 nat 命令

在希望接收和发送 IPv4、IPv6 报文的端口上配置 ipv6 nat 命令，否则即使在配置中找到了匹配的转换规则也不会成功地将转换后的报文发出去。

第10章　配置 NATPT 服务

10.1　配置NATPT服务

要想使用 NATPT 对报文进行 v4 和 v6 域的转换，除了使能协议，还需要配置相应的规则。目前提供的 NATPT 服务主要包括：

- 转换规则的管理
- 地址池的管理
- 由转换规则生成的转换映射管理

10.1.1　转换规则的管理

转换规则包括两种：静态转换规则和动态转换规则。静态转换规则优先级高于动态转换规则，即对报文进行转换时会优先匹配静态转换规则。主要提供的服务也分为两种：

- 静态转换规则的管理
- 动态转换规则的管理
- IPv6 匹配地址前缀的管理

1. 静态转换规则的管理

要向路由器中添加一条静态转换规则，在全局配置态下使用下列命令：

命令	目的
ipv6 nat v4v6 source *ipv4-address ipv6-address*	设置一条从v4域到v6域的源地址静态转换规则，当IPv4报文源地址为*ipv4-address*时，转换成的IPv6报文源地址为*ipv6-address*。
ipv6 nat v6v4 source *ipv6-address ipv4-address*	设置一条从v6域到v4域的源地址静态转换规则，当IPv6报文源地址为*ipv6-address*时，转换成的IPv4报文源地址为*ipv4-address*。

在命令前面加 no 删除一条配置的静态转换规则。

需要注意的是，静态转换规则的双向性。以 ipv6 nat v4v6 source 1.1.1.1 2001::1 为例，一方面报文 IPv4 转换为 IPv6 时进行源地址的替换，另一方面，反过来，当一个目的地址为 2001::1 的 IPv6 报文进行转换时也会被转换成目的地址为 1.1.1.1 的 IPv4 报文。

2. 动态转换规则的管理

要向路由器中添加一条动态转换规则，在全局配置态下使用下列命令：

命令	目的
ipv6 nat v4v6 source list *access- name* **pool** *name*	设置一条从v4域到v6域的源地址动态转换规则，当IPv4报文通过了IPv4访问列表access-name检查时，从IPv6地址池name中分配一个IPv6地址用作转

	换后的IPv6报文的源地址。
ipv6 nat v6v4 source list *access- name* **pool** *name* **[overload]**	设置一条从v6域到v4域的源地址动态转换规则，当IPv6报文通过了IPv6访问列表access-name检查时，从IPv4地址池name中分配一个IPv4地址用作转换后的IPv4报文的源地址。overload是可选命令参数，它允许来自不同IPv6源地址的TCP、UDP和ICMP报文转换成IPv4报文后复用同一个IPv4源地址。
ipv6 nat v6v4 source list *access- name* **interface** interface-*name* **overload**	设置一条从v6域到v4域的源地址动态转换规则，当IPv6报文通过了IPv6访问列表access-name检查时，自动使用转发IPv4报文端口的主IPv4地址作为转换后报文的源地址。在这种情况下，总是允许来自不同IPv6源地址的TCP、UDP和ICMP报文转换成IPv4报文后复用同一个IPv4源地址。

在命令前面加 no 删除一条配置的动态转换规则。

和静态转换规则的双向性不同，动态转换规则只具有单向性，即只能对报文源地址进行转换，不能反过来对报文目的地址进行转换。

3. IPv6 匹配地址前缀的管理

报文在从 v6 域转换到 v4 域时，只有目的地址匹配指定 IPv6 地址前缀的 IPv6 报文才会被转换。反过来，当报文从 v4 域转换到 v6 域时，转换后的 IPv6 报文源地址也应当同指定的 IPv6 地址前缀匹配，否则将不能被转换。

要设置全局的 IPv6 匹配地址前缀，在全局配置态下使用下列命令；要在特定端口设置 IPv6 匹配地址前缀，在端口配置态使用下列命令：

命令	目的
ipv6 nat prefix *ipv6-prefix/prefix-length*	设置IPv6匹配地址前缀，*ipv6-prefix*的格式应符合RFC2373的要求，prefix-length为前缀的长度，以十进制数表示，其值只能为96.
ipv6 nat prefix *ipv6-prefix/prefix-length* **v4-mapped** *access-list-name*	设置IPv6匹配地址前缀，并且目的地址满足这个地址前缀IPv6报文，其目的地址的低32bit就是转换后的IPv4报文目的地址。在转换前，IPv6报文应通过IPv6访问控制列表access-list-name的检查，否则将不能被转换。

在命令前面加 no 删除一个配置的 IPv6 地址前缀。

10.1.2 地址池的管理

地址池分为两种，一种提供 IPv6 地址，另一种提供 IPv4 地址，两种地址池的配置命令相似。地址池的管理提供的服务：

- IPv4 地址池的管理
- IPv6 地址池的管理

1. IPv4 地址池的管理

要向路由器中添加一个 IPv4 地址池，在全局配置态下使用下列命令：

命令	目的
ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length*	设置一个IPv4地址池，地址池名为name， 地址池起始和结束地址分别为start-ipv4和end-ipv4，起始地址和结束地址应当符合prefix-length指定的范围（1-32）

在命令前面加 no 删除地址池。

IPv4 地址池在报文从 v6 转到 v4 域时使用，为转换后的 IPv4 报文分配一个动态的 IPv4 源地址。

2. IPv6 地址池的管理

要向路由器中添加一个 IPv6 地址池，在全局配置态下使用下列命令：

命令	目的
ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length*	设置一个IPv6地址池，地址池名为name， 地址池起始和结束地址分别为start-ipv6和end-ipv6，起始地址和结束地址应当符合prefix-length指定的范围（1-128）

在命令前面加 no 删除地址池。

IPv6 地址池在报文从 v4 转到 v6 域时使用，为转换后的 IPv6 报文分配一个动态的 IPv6 源地址。

10.1.3 转换映射管理

转换映射是由报文根据转换规则生成的。静态转换规则生成的转换映射具有无限的有效时间，除非规则被改变或删除；动态转换规则生成的转换映射如果在一定时间内未被使用将会变为无效，其使用的地址若是从地址池中分配的也将被归还到地址池中。转换映射管理提供的服务：

- 转换映射的显示
- 清除动态转换映射

1. 转换映射的显示

在全局执行态或配置态下执行下列命令显示当前已经生成的转换映射：

命令	目的
show ipv6 nat translationss [icmp | tcp | udp] [verbose]	可选参数用来指定只显示某些关注协议的转换映射情况，verbose可选参数能显示更多的额外信息，如转换映射的生成时间和使用时间等。

2. 清除动态转换映射

要清除路由器中缓存的动态转换映射，在全局执行态或配置态下使用下列命令：

命令	目的

clear ipv6 nat translations *	清除所有的动态转换映射

这条命令只会清除动态转换映射，不会删除静态转换映射。

第11章 VRRP 配置

11.1 概述

虚拟路由冗余协议(Virtual Router Redundancy Protocol) 消除了在静态缺省路由环境下的单点服务失败的风险。VRRP 可避免静态指定网关的缺陷。通过 VRRP，一组路由交换机可以一起协同工作，共同组成一台虚拟路由交换机。该虚拟路由交换机对外配有一个虚拟 IP 地址和虚拟 MAC 地址，VRRP 从路由交换机组中选出一台作为 master，负责转发数据包。当主路由交换机发生故障时，备份路由交换机会迅速接管主路由交换机，主机不必改变缺省网关地址，且此过程对于终端系统是透明的。这样就提供了在故障发生时更快、更有效的解决方法。

11.2 VRRP IPv6配置任务列表

- 端口开启/关闭 VRRP
- 配置 VRRP 的验证方式
- 配置 VRRP 优先级抢占
- 配置 VRRP 的优先级
- 配置 VRRP 的时钟值
- VRRP 的监控与维护

11.3 VRRP IPv6配置任务

11.3.1 端口开启/关闭 VRRP

在端口配置模式下进行下列配置：

命令	操作
vrrp *vrid* **associate** *virtual-address* **[secondary]**	端口配置VRRP虚拟地址。
no vrrp *vrid* **associate** *virtual-address* **[secondary]**	端口清除VRRP虚拟地址。

配置 VRRP 的主虚拟地址后就开启了该虚拟路由。可选配最多 32 个备用虚拟地址。只有配置了主虚拟地址后虚拟路由才会离开 Init 状态。

缺省关闭 VRRP 功能。

11.3.2 配置 VRRP 说明信息

在端口配置模式下进行下列配置。

命令	操作
vrrp *vrid* **description** *WORD*	配置VRRP说明信息。

no vrrp *vrid* **description**	删除VRRP说明信息。

可配置的说明信息不超过 64 个字符。

11.3.3 配置 VRRP 优先级抢占

在端口配置模式下进行下列配置。

命令	操作
vrrp *vrid* **preempt**	配置VRRP优先级抢占。
no vrrp *vrid* **preempt**	关闭VRRP优先级抢占。

优先级抢占只对处于 Backup 下的路由器有效，当收到由 master 路由器发送来的 announce 报文后，当检测到 master 的优先级没有本地配置的优先级高时，如果 Backup 路由器配置了优先级抢占，Backup 路由器将从 Backup 状态跃迁到 master 状态，并向外发送 announce 报文。反之，则继续停留在 Backup 状态。

缺省方式是优先级抢占。

11.3.4 配置 VRRP 优先级抢占延迟

在端口配置模式下进行下列配置。

命令	操作
vrrp *vrid* **preempt delay** *seconds*	配置VRRP优先级抢占延迟。
no vrrp *vrid* **preempt deley** *seconds*	恢复缺省VRRP优先级抢占延迟。

对于开启了优先级抢占的 Backup 路由器，收到由 master 路由器发送来的 announce 报文后，当检测到 master 的优先级没有本地配置的优先级高时，需推迟抢占动作直至抢占延迟过后。

缺省优先级抢占延迟为 0。

11.3.5 配置 VRRP 优先级

在端口配置模式下进行下列配置。

命令	操作
vrrp *vrid* **priority** *value* **(1~254)**	配置VRRP优先级。
no *vrid* **priority**	恢复VRRP优先级为缺省值。

当虚拟地址和端口地址一致时，VRRP 会自动提升优先级为 255，当虚拟地址或者端口地址发生变化后，优先级值会自动恢复到原来配置的值。

缺省值为 100。

11.3.6 配置 VRRP 时钟值

在端口配置模式下进行下列配置。

命令	操作
vrrp *vrid* **timer advertisement {***second* **| dsec** *decisecond* **| csec** *centisecond***}**	配置VRRP时钟值。
no vrrp *vrid* **timer advertisement**	恢复VRRP时钟值为缺省值。

时钟值将决定虚拟路由器从故障中恢复的最短时间，当 master 路由器 down 了后，Backup 路由器将在 3*advertisement + skew_time 间隔后跃迁为 master 路由器，asvertisement 时钟太长显然不利于故障恢复，推荐采用缺省值。

提供了 3 种时钟精度：秒级精度、0.1 秒级精度和 0.01 秒级精度。

缺省值为 1 second。

11.3.7 VRRP 的监控与维护

在管理配置模式下进行下列配置。

命令	操作
show vrrp *vrid* **{brief | detail | interface** *intf-id***}**	显示VRRP信息。
[no] debug vrrp {errors | event | packets | interface *intf-id* **| all}**	开启/关闭VRRP调试开关。

显示 VRRP 信息：

```
Switch(config)# show vrrp detail
VLAN1 - Group 1
   VRRP State is Master
   Virtual IP address : 1.1.1.100/24
   Virtual Mac address : 0000.5e00.0101
   Current Priority : 100     (Config 100)
   VRRP timer : Advertise 1.0 s (default)     master_down 3.6 s
   VRRP current timer : Advertise 0.2 s master_down 0.0 s preempt after 0.0 s
   Authentication string is not set
   Preempt is set    (delay : 0    s)
   Learn Advertise Interval is not set
   Master Router IP : 1.1.1.1, priority : 100, advertisment :    1.0 s
```

11.3.8 VRRP 配置示例

示例网络连接如图 11-1所示：

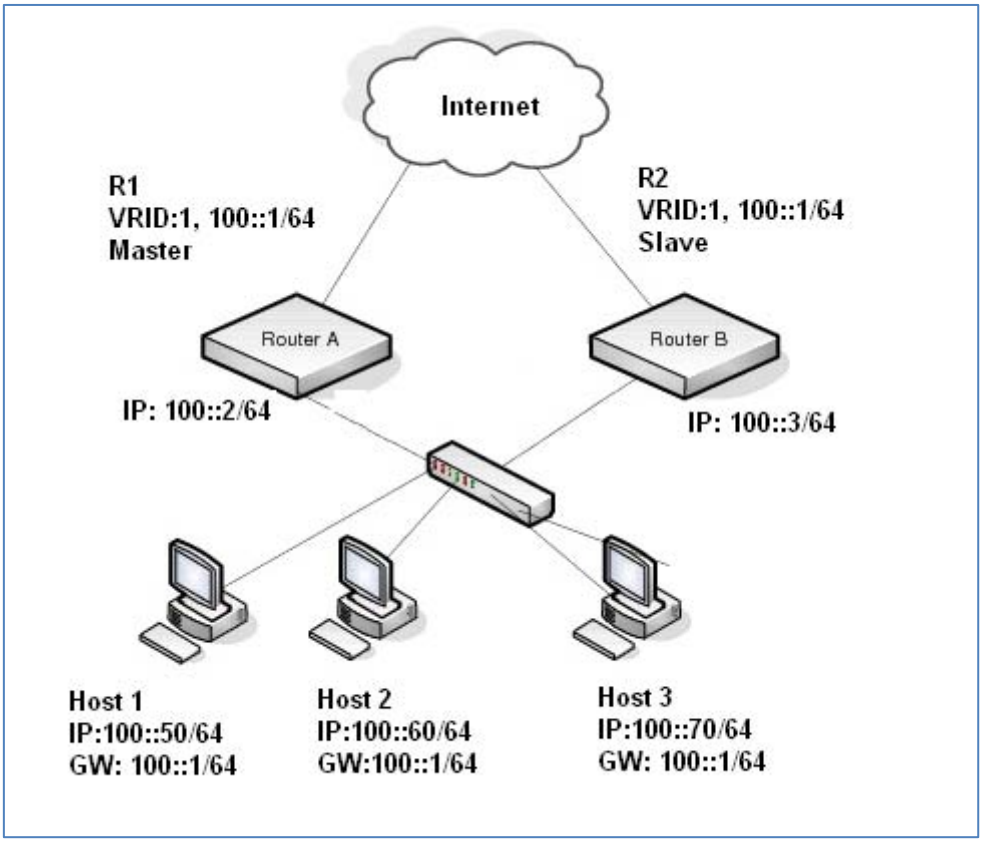


图 11-1 网络连接示例

1. 配置路由器 Router A

(3) 配置 Private Network 接口地址

```
Router_config_g0/0# ipv6 address 100::2/64
```

(4) 在 Private Network 接口上配置虚拟路由 1，虚拟地址为 100::1，优先级为 120

```
Router_config_g0/0#vrrp 1 associate 100::1/64
Router_config_g0/0#vrrp 1 priority 120
```

(5) 显示虚拟路由交换机信息

```
Router_config_g0/0#show vrrp
GigaEthernet0/0 - Group 1
  VRRP State is Master
  Configured version: 3, actual version: 3
  Virtual IP address : 100::1
  Virtual Mac address : 0000.5e00.0201
  Current Priority : 120     (Config 120)
  VRRP timer : Advertise 1.000s (default)     master_down 3.060s
  VRRP current timer : Advertise 0.550s master_down 0.000s preempt after 0.0 s
  Preempt is set   (delay : 0   s)
  Learn Advertise Interval is not set
  Master Router IP : FE80::2E0:FFF:FE87:0, priority : 120, advertisment : 1.000
```

2. 配置路由器 Router B

(1) 配置 Private Network 接口地址

```
Router_config_g0/0# ipv6 address 100::3/64
```

(6) 在 Private Network 接口上配置虚拟路由 1，虚拟地址为 100::1，优先级采用默认值

```
Router_config_g0/0#vrrp 1 associate 100::1/64
```

(7) 显示虚拟路由交换机信息

```
Router_config_g0/0#show vrrp
GigaEthernet0/0 - Group 1
  VRRP State is BACKUP
  Configured version: 3, actual version: 3
  Virtual IP address : 100::1
  Virtual Mac address : 0000.5e00.0201
  Current Priority : 100     (Config 100)
  VRRP timer : Advertise 1.000s (default)     master_down 3.060s
  VRRP current timer : Advertise 0.000s master_down 3.050s preempt after 0.0 s
  Preempt is set   (delay : 0   s)
  Learn Advertise Interval is not set
  Master Router IP : FE80::2E0:FFF:FE87:0, priority : 120, advertisment : 1.000
```

3. 配置 Private Network 的 PC 和 Server：

配置 Private Network 内每台 PC 和 Server 的 Default Gateway 为 100::1。

第12章 RADIUS 配置

12.1 概述

RADIUS 是一种 C/S 结构的协议。用户接入 NAS，NAS 向 RADIUS 服务器使用 Access-Require 数据包提交用户信息，包括用户名、密码等相关信息，其中用户密码是经过 MD5 加密的，双方使用共享密钥，这个密钥不经过网络传播；RADIUS 服务器对用户名和密码的合法性进行检验，必要时可以提出一个 Challenge，要求进一步对用户认证，也可以对 NAS 进行类似的认证；如果合法，给 NAS 返回 Access-Accept 数据包，允许用户进行下一步工作，否则返回 Access-Reject 数据包，拒绝用户访问；如果允许访问，NAS 向 RADIUS 服务器提出计费请求 Account-Require，RADIUS 服务器响应 Account-Accept，对用户的计费开始，同时用户可以进行自己的相关操作。

RADIUS 服务器和 NAS 服务器通过 UDP 协议进行通信，RADIUS 服务器的 1812 端口负责认证，1813 端口负责计费工作。RADIUS 协议还规定了重传机制。如果 NAS 向某个 RADIUS 服务器提交请求没有收到返回信息，那么可以要求备份 RADIUS 服务器重传。由于有多个备份 RADIUS 服务器，因此 NAS 进行重传的时候，可以采用轮询的方法。如果备份 RADIUS 服务器的密钥和以前 RADIUS 服务器的密钥不同，则需要重新进行认证。

本文说的是在 NAS 上进行的相关配置。

12.2 RADIUS IPv6配置任务列表

- 配置 NAS 的 Identifier
- 配置 NAS 的 ipv4 地址
- 配置 NAS 的 ipv6 地址
- 配置在 Access-Challenge 方式下用户数据不显示
- 配置 RADIUS 服务器不回应时的停止时间
- 配置允许用户以“@server”格式来指定 RADIUS 服务器
- 配置 RADIUS 服务器
- 配置 RADIUS 服务器密匙
- 配置初始 RADIUS 请求无需密码
- 配置 RADIUS 重发次数
- 配置等待 RAIDUS 服务器回答超时值
- 配置 RADIUS 附加属性等
- 配置 radius 服务器组的名称
- 在服务器组中增加服务器
- 指明 RADIUS 数据包的源 IP 地址
- 开启 debug 信息

12.3 RADIUS IPv6配置任务

12.3.1 配置 NAS 的 Identifier

在配置模式下进行下列配置：

命令	操作
radius-server attribute 32 in-access-req	在访问请求中发送属性 32
no radius-server attribute 32 in-access-req	在访问请求中不发送属性 32
radius-server attribute 32 in-account-req	在记帐请求中发送属性 32
no radius-server attribute 32 in-account-req	在记帐请求中不发送属性 32
radius-server attribute 32 identifier WORD	设置 32 号属性的字符串，即 NAS 的 Identifier 属性
no radius-server attribute 32 identifier WORD	清除所设 32 号属性的字符串，即 NAS 的 Identifier 属性

NAS 的 Identifier 属性的字符串长度不超过 32 字节

12.3.2 配置 NAS 的 ipv4 地址

在配置模式下进行下列配置：

命令	操作
radius-server attribute 4 x.x.x.x	设置 NAS 的 ipv4 地址
No radius-server attribute 4	删除 NAS 的 ipv4 地址

12.3.3 配置 NAS 的 ipv6 地址

在配置模式下进行下列配置：

命令	操作
radius-server attribute 95 x:x:x:x::x	设置 NAS 的 ipv6 地址
no radius-server attribute 95	删除 NAS 的 ipv6 地址

12.3.4 配置在 Access-Challenge 方式下用户数据不显示

在配置模式下进行下列配置：

命令	操作

radius-server challenge-noecho	在 Access-Challenge 方式下用户数据不显示
No dius-server challenge-noecho	在 Access-Challenge 方式下用户数据显示

12.3.5 配置 RADIUS 服务器不回应时的停止时间

在配置模式下进行下列配置：

命令	操作
radius-server deadtime <0-1440>	配置 RADIUS 服务器不回应时的停止时间
no radius-server deadtime <0-1440>	恢复缺省配置

12.3.6 配置允许用户以“@server”格式来指定 RADIUS 服务器

在配置模式下进行下列配置：

命令	操作
Radius-server directed-request	允许用户以“@server”格式来指定 RADIUS 服务器
no radius-server directed-request	不允许用户以“@server”格式来指定 RADIUS 服务器
Radius-server directed-request restricted	允许用户以“@server”格式来指定 RADIUS 服务器，但限定只查询直接请求的 RADIUS 服务器
no radius-server directed-request restricted	不允许用户以“@server”格式来指定 RADIUS 服务器

12.3.7 配置 RADIUS 服务器

在配置模式下进行下列配置：

命令	操作
radius-server host ADDR x.x.x..x [acct-port <0-65536>][auth-port <0-65536>]	配置 ipv4 的 RADIUS 服务器，记账和认证 UDP 端口配置为可选
no radius-server host ADDR x.x.x..x	删除所配置的 ipv4 的 RADIUS 服务器
radius-server host ADDR x:x:x:x::x [acct-port <0-65536>][auth-port <0-65536>]	配置 ipv6 的 RADIUS 服务器，记账和认证 UDP 端口配置为可选
no radius-server host ADDR x:x:x:x::x	删除所配置的 ipv6 的 RADIUS 服务器

12.3.8 配置 RADIUS 服务器密匙

在配置模式下进行下列配置：

命令	操作
radius-server key string WORD	配置 RADIUS 服务器密匙
no radius-server key	删除 RADIUS 服务器密匙

这是一个全局的密匙配置，所有的单独的服务器和没有配置密匙的服务器组都用该配置密匙。

12.3.9 配置初始 RADIUS 请求无需密码

在配置模式下进行下列配置：

命令	操作
radius-server optional-passwords	设置初始 RADIUS 请求无需密码
no radius-server optional-passwords	恢复缺省值

12.3.10 配置 RADIUS 重发次数

在配置模式下进行下列配置：

命令	操作
radius-server retransmit <0-100>	配置 RADIUS 重发次数
no radius-server retransmit	恢复缺省值

12.3.11 配置等待 RAIDUS 服务器回答超时值

在配置模式下进行下列配置：

命令	操作
radius-server timeout <1-1000>	配置等待 RAIDUS 服务器回答超时值
no radius-server timeout	恢复缺省值

12.3.12 配置 RADIUS 附加属性等

在配置模式下进行下列配置：

命令	操作
radius-server vsa	在认证和记账请求中发送附加属性

no radius-server vsa	在认证和记账请求中都不发送附加属性
radius-server vsa authentication	在认证请求中发送附加属性
no radius-server vsa authentication	在认证请求中不发送附加属性

12.3.13 配置 radius 服务器组的名称

在配置模式下进行下列配置：

命令	操作
aaa group server radius WORD	配置 radius 服务器组，名称为 WORD
no aaa group server radius WORD	删除 radius 服务器组，名称为 WORD

12.3.14 在服务器组中增加服务器

在配置模式下进行下列配置：

命令	操作
server ADDR x.x.x.x [key WORD][retransmit <0-100>][timeout <1-1000>][privilege <1-15>][acct-port <0-65536>][auth-port <0-65536>][DUMMYSTR]	在服务器组中增加ipv4的服务器
no server ADDR x.x.x.x	在服务器组中删除ipv4的服务器
server ADDR x:x:x:x::x [key WORD][retransmit <0-100>][timeout <1-1000>][privilege <1-15>][acct-port <0-65536>][auth-port <0-65536>][DUMMYSTR]	在服务器组中增加ipv6的服务器
no server ADDR x:x:x:x::x	在服务器组中增加ipv6的服务器

在服务器组中增加的服务器，可以配置其 key（密匙）、retransmit（重传次数）、timeout（回应超时值）、privilege（优先级）、acct-port（记账 UDP 端口）、auth-port（认证 UDP 端口）。

12.3.15 指明 RADIUS 数据包的源 IP 地址

在配置模式下进行下列配置：

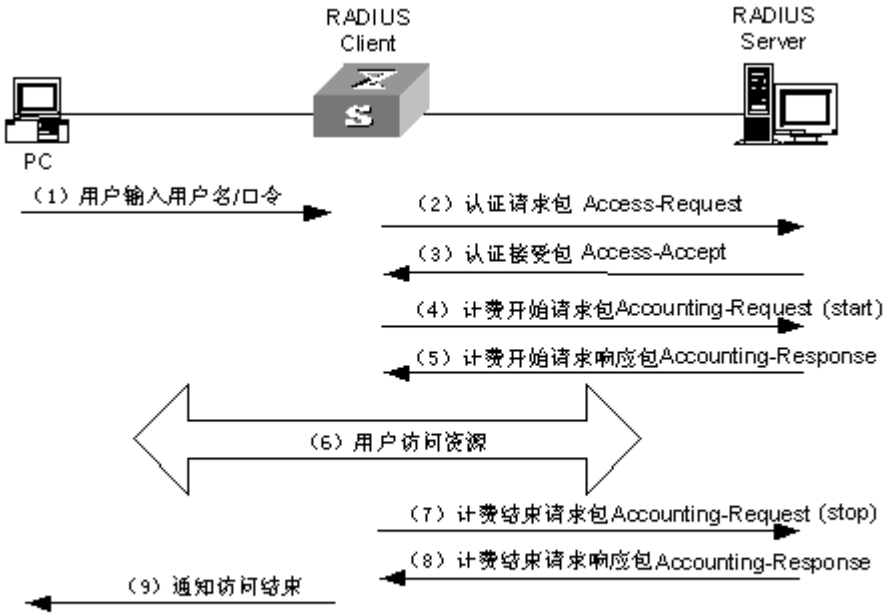
命令	操作
radius source-interface dv_id	指明 RADIUS 数据包的源 IP 地址
no radius source-interface	取消指明 RADIUS 数据包的源 IP 地址

12.3.16 开启 debug 信息

在配置模式下进行下列配置：

命令	操作
debug radius event	开启 RAIDUS 的 event debug
no debug radius event	关闭 RAIDUS 的 event debug
debug radius packet	开启 RAIDUS 的 packet debug
no debug radius packet	关闭 RAIDUS 的 packet debug

12.3.17 配置示例



上图是一个简单的拓扑连接，PC 为 ipv4 , RADIUS Server 为 ipv6 服务器。图中 RADIUS Client 就是我们所要配置的 NAS。以下以**服务器**和**服务器组**两种方式进行配置。

1. 对 NAS 进行本身的一些配置

（1）配置 NAS 的 Identifier

Router_config# radius-server attribute 32 identifie bdcom

Router_config# radius-server attribute 32 in-access-req

Router_config# radius-server attribute 32 in-account-req

（2）配置 NAS 的 ip 地址，要配一个 ipv4 地址和一个 ipv6 地址

Router_config# radius-server attribute 4 192.168.1.1

Router_config# radius-server attribute 95 2001::224

（3）配置允许用户以“@server”格式来指定 RADIUS 服务器

Router_config# radius-server directed-request

2. 配置 RADIUS 服务器

（1）配置 RADIUS 服务器

Router_config# radius-server host ADDR 2001::224

（2）配置 RADIUS 服务器密匙，服务器组的密匙也可以配置在这里，注意，这里只能存储一个密匙，后面配置的会覆盖前面配置的。

Router_config# radius-server key string bdcom

3. 配置 RADIUS 服务器组

（1）配置 RADIUS 服务器组名称

Router_config# aaa group server radius bdcom_radius1

（2）在服务器组中增加服务器

Router_config_sg_radius_bdcom_radius1# server ADDR 2001::224 key bdcom privilege 1