

第 7 篇 IPv6 基础

第 22 章 IPv6 邻居发现

第 23 章 IPv6 路由协议

第 24 章 IPv6 过渡技术

第22章 IPv6 邻居发现

ND（Neighbor Discovery，邻居发现）协议是 IPv6 的一个关键协议，它综合了 IPv4 中的一些协议如 ARP、ICMP 路由器发现和 ICMP 重定向等，并对它们做了改进。本章介绍了 IPv6 邻居发现协议中的地址解析、无状态地址自动配置等重要功能，并对如何配置 ND 协议进行了讲解。

22.1 本章目标

课程目标

● 学习完本课程，您应该能够：

- 了解邻居发现协议的功能
- 掌握地址解析的功能和特点
- 了解邻居不可达检测的功能
- 掌握无状态地址自动配置的原理
- 掌握邻居发现协议的配置



www.h3c.com

22.2 邻居发现协议



ND (Neighbor Discovery, 邻居发现) 协议是 IPv6 中一个非常重要的基础协议。

IPv6 的 ND 协议实现了 IPv4 中的一些协议功能, 如 ARP、ICMP 路由器发现和 ICMP 重定向等, 并对这些功能进行了改进。同时, ND 协议还提供了其他许多非常重要的功能, 如前缀发现、邻居不可达检测、重复地址检测、无状态地址自动配置等。

- **地址解析:** 已知目的节点的网络层地址, 确定链路层地址的方法。ND 中的地址解析功能不仅替代了原 IPv4 中的 ARP 协议, 同时还用邻居不可达检测 (NUD) 来维护邻居节点之间的可达性状态信息。
- **邻居不可达检测:** 在获取到邻居节点的链路层地址后, 通过发送消息来验证邻居节点是否可达。
- **重复地址检测 (DAD):** 根据前缀信息生成 IPv6 地址或手工配置 IPv6 地址后, 为保证地址的唯一性, 在这个地址可以使用之前, 主机需要检验此 IPv6 地址是否已经被链路上其他节点所使用。
- **无状态地址自动配置:** 无状态地址自动配置指主机根据路由器发现/前缀发现所获取的信息, 自动配置 IPv6 地址。包括路由器发现/前缀发现、接口 ID 自动生成、重复地址检测等过程。通过无状态自动配置机制, 链路上的节点可以自动获得 IPv6 全球单播地址。

- 路由器重定向：当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当在本地链路上存在一个到达目的网络的更好的路由器时，缺省网关会向源主机发送 ICMPv6 重定向消息，通知主机选择更好的下一跳进行后续报文的发送。

ND协议报文类型

紫光集团
核心企业 | 数字化解决方案领导者

● ND协议使用ICMPv6报文

数据链路帧头	IPv6报文头	ICMPv6报文头	协议数据
--------	---------	-----------	------

● ND协议报文ICMPv6类型

ICMPv6类型	消息名称
Type = 133	RS - (Router Solicitation, 路由器请求)
Type = 134	RA - (Router Advertisement, 路由器公告)
Type = 135	NS - (Neighbor Solicitation, 邻居请求)
Type = 136	NA - (Neighbor Advertisement, 邻居公告)
Type = 137	Redirect - (重定向消息)

www.h3c.com

在 IPv4 中，ARP 报文直接封装在以太网帧中，其以太网协议类型为 0x0806。ARP 被看作是工作在 2.5 层的协议。而 ND 协议使用了 ICMPv6 报文，是在第 3 层上实现的。这样，ND 协议可以独立于数据链路层协议工作，不受下层的链路层协议的影响。

ND 协议使用了 RS、RA、NS、NA 和 Redirect 等 5 种报文，其所对应 ICMPv6 报文类型如表 22-1 所示。

表22-1 ICMPv6 报文类型

ICMPv6 类型	报文名称
Type = 133	RS (Router Solicitation, 路由器请求)
Type = 134	RA (Router Advertisement, 路由器公告)
Type = 135	NS (Neighbor Solicitation, 邻居请求)
Type = 136	NA (Neighbor Advertisement, 邻居公告)
Type = 137	Redirect (重定向报文)

上述报文中，NS/NA 报文主要用于地址解析，RS/RA 报文主要用于无状态地址自动配置，Redirect 报文用于路由器重定向。

22.3 IPv6地址解析

IPv6地址解析概述

- 与IPv4中的地址解析不同，IPv6地址解析包含了两个过程
 - 解析IPv6地址所对应的链路层地址过程
 - 邻居可达性状态的维护过程，即邻居不可达检测（NUD）
- IPv6地址解析的优点
 - 加强了解析协议与底层链路的独立性
 - 增强了安全性
 - 减小了报文传播范围

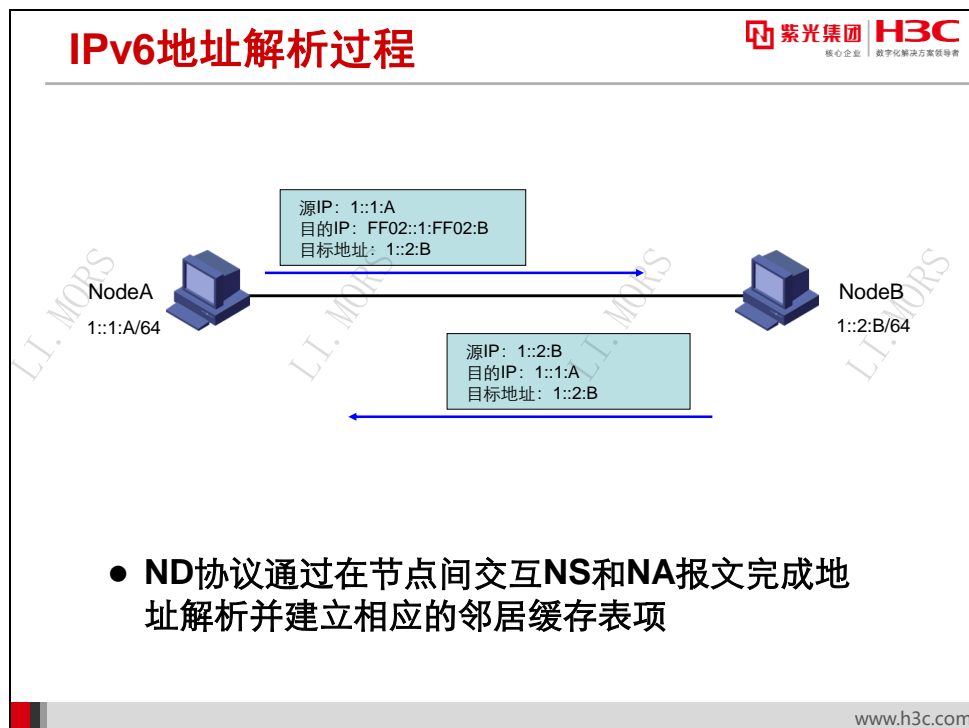
www.h3c.com

在报文转发过程中，当一个节点要得到同一链路上另外一个节点的链路层地址时，需要进行地址解析。IPv4 中使用 ARP 协议实现了这个功能。IPv6 使用 ND 协议实现了这个功能，但功能有所增强。

IPv6 的地址解析过程包括两部分，一部分解析了链路上目的 IP 地址所对应的链路层地址；另一部分是邻居可达性状态的维护过程，即邻居不可达检测。

相比于 IPv4 的 ARP，IPv6 地址解析工作在 OSI 模型的网络层，与链路层协议无关。这是一个很显著的优点，它的益处如下：

- 加强了地址解析协议与底层链路的独立性。对每一种链路层协议都使用相同的地址解析协议，无需再为每一种链路层协议定义一个新的地址解析协议。
- 增强了安全性。ARP 攻击、ARP 欺骗是 IPv4 中严重的安全问题。在第三层实现地址解析，可以利用三层标准的安全认证机制来防止这种 ARP 攻击和 ARP 欺骗。
- 减小了报文传播范围。在 IPv4 中，ARP 广播必须泛滥到二层网络中每台主机。IPv6 的地址解析利用三层组播寻址限制了报文的传播范围，通过将地址解析请求仅发送到待解析地址所属的被请求节点（Solicited-Node）组播组，减小了报文传播范围，节省了网络带宽。



ND 协议通过在节点间交互 NS 和 NA 报文完成地址解析,并使用得到的链路层地址和 IPv6 地址等信息来建立相应的邻居缓存表项。上图中, NodeA 的链路层地址为 00E0-FC00-0001, 全局地址 IPv6 为 1::1:A; NodeB 的链路层地址为 00E0-FC00-0002, 全局 IPv6 地址为 1::2:B。当 NodeA 要发送数据报文到 NodeB 时, 其地址解析过程如下:

- 1) NodeA 发送一个 NS 报文到链路上, 目的 IPv6 地址为 NodeB 对应的被请求节点组播地址(FF02::1:FF02:B), 选项字段中携带了 NodeA 的链路层地址 00E0-FC00-0001。
- 2) NodeB 接收到该 NS 报文后, 由于报文的目的地址 FF02::1:FF02:B 是 NodeB 的被请求节点组播地址, 所以 NodeB 会处理该报文; 同时, 根据 NS 报文中的源地址和源链路层地址选项更新自己的邻居缓存表项。
- 3) NodeB 发送一个 NA 报文来应答 NS, 同时在消息的目标链路层地址选项中携带自己的链路层地址 00E0-FC00-0002。
- 4) NodeA 接收到 NA 报文后, 根据报文中携带的 NodeB 链路层地址, 创建一个到目标节点 NodeB 的邻居缓存表项。

通过交互, 节点就获得了对方的链路层地址, 建立起到达对方的邻居缓存表项, 从而可以相互通信。

当一个节点的链路层地址发生改变时, 以所有节点组播地址 FF02::1 为目的地址发送 NA 报文, 通知链路上的其他节点更新邻居缓存表项。

邻居不可达检测概述

- **NUD (Neighbor Unreachability Detection, 邻居不可达检测)** 是节点确定邻居可达性的过程
- **邻居可达性状态机**用来描述邻居的可达性，共有五种状态，可互相迁移
 - INCOMPLETE (未完成)
 - REACHABLE (可达)
 - STALE (失效)
 - DEAY (延时)
 - PROBE (探测)

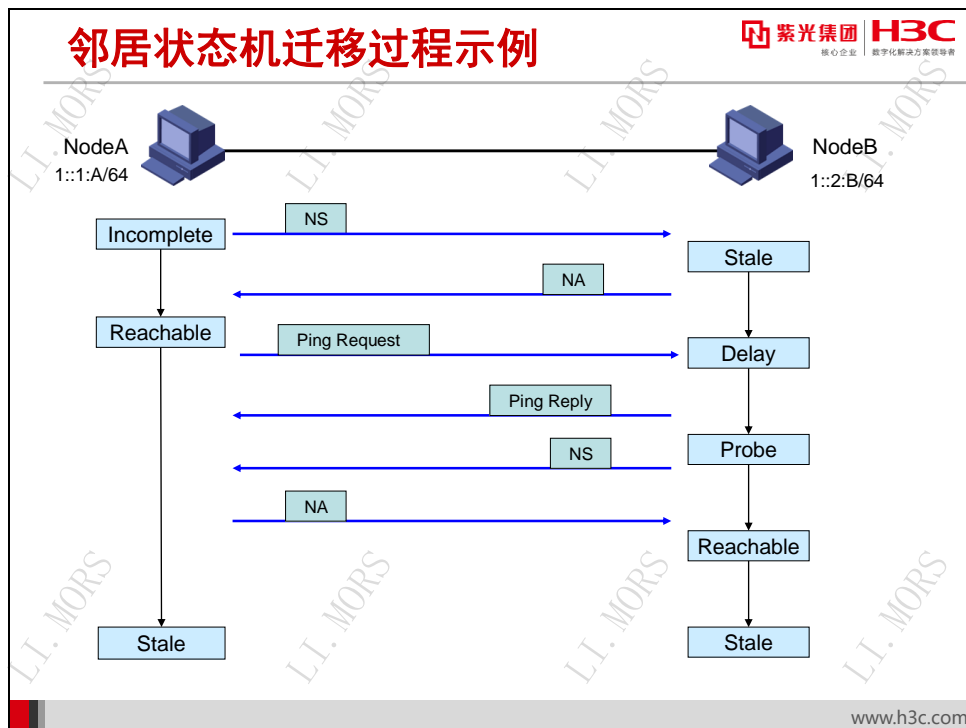
NUD (Neighbor Unreachability Detection, 邻居不可达检测) 是节点确定邻居可达性的过程。邻居不可达检测机制通过邻居可达性状态机来描述邻居的可达性。邻居可达性状态机之间满足一定的条件时，可相互迁移。

邻居可达性状态机保存在邻居缓存表中，共有五种：

- **INCOMPLETE (未完成) 状态**：表示正在解析地址，邻居的链路层地址尚未确定。当节点第一次发送 NS 报文到邻节点时，会同时在邻居缓存表中创建一个到此邻节点的新表项，此时表项状态就是 INCOMPLETE。
- **REACHABLE (可达) 状态**：表示地址解析成功，该邻居可达。节点可以与处于可达状态的邻节点互相通信。不过可达状态伴随有一个 REACHABLE_TIME 定时器，在定时器超时后，会转化到 STALE (失效) 状态。
- **STALE (失效) 状态**：表示未确定邻居是否可达。STALE 状态是一个稳定的状态。
- **DEAY (延迟) 状态**：表示未确定邻居是否可达。DEAY 状态也不是一个稳定的状态，而是一个延时等待状态。DEAY 状态下，节点需要收到“可达性证实信息”后，才能进入 REACHABLE 状态。
- **PROBE (探测) 状态**：同样表示未确定邻居是否可达。节点会向处于 PROBE 状态的邻居持续发送 NS 报文，直到接收到“可达性证实信息”后，才能进入可达状态。

在 STALE 和 PROBE 状态时，节点收到“可达性证实信息”后，才能进入可达状态。“可达性证实信息”的来源有 2 种：

- 来自上层连接协议的暗示。如果邻节点之间有 TCP 连接，且收到了对端节点发出的确认消息，则表明邻节点之间可达。
- 来自不可达探测回应。节点发送 NS 报文后，收到邻节点响应 NA 报文，则会认为邻节点可达。



上图是一个典型的邻居状态迁移过程示例。

假设管理员在 NodeA 上执行 Ping 操作，发送报文给 NodeB，则 NodeA 上有关 NodeB 的邻居状态变化过程如下：

- NodeA 第一次发送报文给 NodeB，所以它在邻居表中把 NodeB 的邻居状态置为 INCOMPLETE，同时发送 NS 报文以解析 NodeB 的链路层地址；
- 待 NodeB 返回 NA 报文应答后，它将 NodeB 的邻居状态置为 REACHABLE，同进发送 Echo Request 报文；
- 如果长时间不再发送报文，REACHABLE_TIME 定时器超时，NodeB 的邻居状态会进入 STALE 状态。

NodeB 上有关 NodeA 的邻居状态变化过程如下：

- NodeB 收到 NodeA 的 NS 报文后，将邻居表中的 NodeA 邻居状态置为 STALE；
- NodeB 向 NodeA 回应 NA 报文，并将邻居表中的 NodeA 邻居状态置为 DELAY，以等待收到“可达性证实信息”；
- 因为节点之间没有 TCP 连接，所以 NodeB 没有收到“可达性证实信息”，于是该表项进入 PROBE 状态，并向 NodeA 发送 NS 报文；


- 待 NodeA 返回 NA 报文应答后，它将 NodeA 的邻居状态置为 REACHABLE 状态；
- REACHABLE_TIME 定时器超时，NodeA 的邻居状态进入 STALE 状态。

由以上过程我们会发现，STALE 状态是一个稳定状态，表示邻居的地址解析结果未得到证实；而其它状态都是非稳定状态。

IPv6 采用状态机来表示邻居的状态，并设计了状态机之间的迁移转化，目的是为了使邻居之间能够建立一种双向可信的连接，来避免类似 IPv4 网络中的“ARP 欺骗”等网络攻击。

22.4 IPv6无状态地址自动配置

IPv6地址自动配置



紫光集团 H3C
核心企业 数字化解决方案领导者

- 有状态地址自动配置
 - 从DHCP服务器获取地址及相关信息
- 无状态地址配置
 - 根据路由器发布的信息而自动配置IPv6地址及相关信息
- 无状态地址自动配置的优点
 - 真正的即插即用
 - 网络迁移方便

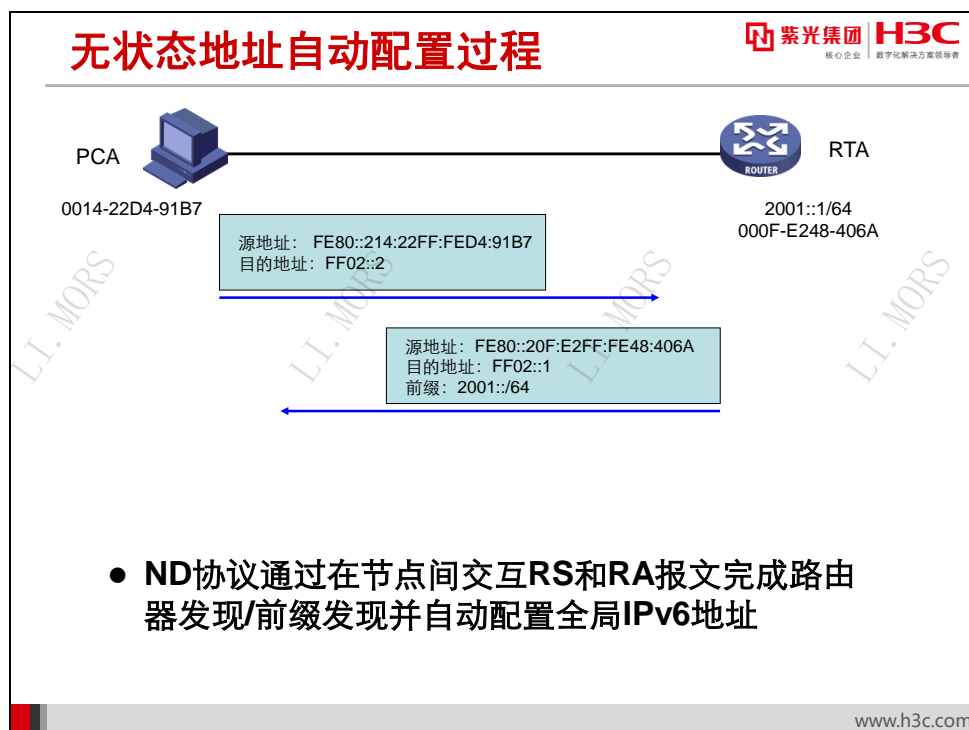
www.h3c.com

IPv6 同时定义了无状态与有状态地址自动配置机制。有状态地址自动配置使用 DHCPv6 协议来给主机动态分配 IPv6 地址，其工作机制与 IPv4 网络中的 DHCP 协议一样。而无状态地址自动配置是 IPv6 中独有的地址配置机制，其通过 ND 协议来实现。

在 IPv6 网络中，当一个节点连接到链路后，它首先使用 ND 协议发出 RS（Router Solicitation，路由器请求）报文，以请求链路上的路由器；路由器收到 RS 报文后，发送 RA（Router Advertisement，路由器公告）报文对其回应，内容包含了所在网络的前缀以及其他配置参数。节点收到 RA 报文后，根据其中的信息，结合接口的标识符来自动配置 IPv6 地址。

无状态地址自动配置的优点如下：

- 真正的即插即用。节点连接到没有 DHCP 服务器的网络时，无需手工配置地址等参数便可访问网络。
- 网络迁移方便。当主机连接到一个新的网络中时，路由器自动分配给主机新的网络前缀，主机根据前缀而进行重新编址，原有的地址仍旧保存一段时间，不会对原网络连接造成中断。



当主机启动时，主机会向本地链路范围内所有的路由器发送 RS 报文，触发链路上的路由器响应 RA 报文。主机接收到路由器发出的 RA 报文后，自动配置缺省路由器，建立缺省路由器列表、前缀列表和设置其它的配置参数。

上图显示了 RS 报文触发 RA 报文的过程。图中 PCA 的链路层地址为 0014-22D4-91B7，链路本地地址为 FE80::214:22FF:FED4:91B7；路由器 RTA 的链路层地址为 000F-E248-406A，链路本地地址为 FE80::20F:E2FF:FE48:406A。

PCA 以自己的链路本地地址作为源地址，发送一个 RS 报文到所有路由器的组播地址 FF02::2；路由器 RTA 收到该报文后，用它的链路本地地址作为源地址，发送 RA 报文到所有节点的组播地址 FF02::1，报文中携带了前缀、缺省路由器等有关地址配置的信息。

PCA 收到 RA 报文后，根据报文中携带的前缀，结合自己的接口 ID，生成全局地址；同时配置其它相关参数，如缺省路由器、跳数等。

节点通过 ND 协议自动获得缺省路由器时，缺省路由器被赋予了有效时间，表明缺省路由器能够被使用的时间。有效时间到期后，缺省路由器就失效了。为了保持缺省路由器有效，路由器需周期性发送路由器通告以刷新有效时间。

22.5 ND协议配置

配置IPv6邻居

- 配置静态邻居表项

```
[Router] ipv6 neighbor ipv6-address mac-address
```

- 配置接口上允许动态学习的邻居的最大个数

```
[Router-Ethernet0/0] ipv6 neighbors max-learning-num number
```

www.h3c.com

将邻居节点的 IPv6 地址解析为链路层地址，可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态实现，也可以通过手工配置实现。

在全局视图下配置 IPv6 邻居静态表项，命令如下：

```
ipv6 neighbor ipv6-address mac-address
```

设备可以通过 NS 消息和 NA 消息来动态获取邻居节点的链路层地址。如果动态获取的邻居表过大，将可能导致设备的转发性能下降。为此，可以通过设置接口上允许动态学习的邻居的最大个数来进行限制。如果接口上动态学习的邻居个数达到所设置的最大值时，该接口将不再学习邻居信息。

在接口视图下配置接口上允许动态学习的邻居的最大个数，命令如下：

```
ipv6 neighbors max-learning-num number
```

配置RA消息相关参数

- 取消对RA消息发布的抑制

```
[Router-Ethernet0/0] undo ipv6 nd ra halt
```

- 配置RA消息发布的时间间隔

```
[Router-Ethernet0/0] ipv6 nd ra interval max-  
interval-value min-interval-value
```

- 设置被管理地址配置标志位和其他配置标志位为1

```
[Router-Ethernet0/0] ipv6 nd autoconfig managed-  
address-flag | other-flag
```

www.h3c.com

用户可以根据实际情况，配置接口是否发送 RA 消息及发送 RA 消息的时间间隔，同时可以配置 RA 消息中的相关参数以通告给主机。当主机接收到 RA 消息后，就可以采用这些参数进行相应操作。

常见的 RA 消息中的参数及含义如下表所示：

表22-2 RA 消息中的常见参数及描述

参数	描述
跳数限制（Cur Hop Limit）	主机在发送IPv6报文时，将使用该参数值填充IPv6报文头中的Hop Limit字段。
前缀信息（Prefix Information）	在同一链路上的主机收到设备发布的前缀信息后，可以进行无状态自动配置等操作。
被管理地址配置标志位（M flag）	用于确定主机是否采用有状态自动配置获取IPv6地址。 如果设置该标志位为1，主机将通过有状态自动配置来获取IPv6地址；否则，将通过无状态自动配置获取IPv6地址。

参数	描述
其他配置标志位（Other flag）	用于确定主机是否采用有状态自动配置获取除IPv6地址外的其他信息。 如果设置其他配置标志位为1，主机将通过有状态自动配置（例如DHCP服务器）来获取除IPv6地址外的其他信息；否则，将通过无状态自动配置获取其他信息。
路由器生存时间（Router Lifetime）	用于设置发布RA消息的路由器作为主机的默认路由器的时间。

可以在接口视图下配置取消对 RA 消息发布的抑制，命令如下：

undo ipv6 nd ra halt

可以在接口视图下配置 RA 消息发布的时间间隔，命令如下：

ipv6 nd ra interval *max-interval-value min-interval-value*

max-interval-value 表示 RA 消息的最大时间间隔；*min-interval-value* 表示 RA 消息的最小时间间隔。

为了避免链路上的突发流量，RA 消息周期性发布时，相邻两次的时间间隔是在最大时间间隔与最小时间间隔之间随机选取一个值作为周期性发布 RA 消息的时间间隔。


可以在接口视图下配置被管理地址标志位为 1，命令如下：

ipv6 nd autoconfig managed-address-flag

可以在接口视图下配置其他标志位为 1，命令如下：

ipv6 nd autoconfig other-flag

ND显示与维护



紫光集团 H3C
核心企业 数字化转型领导者

- 显示邻居信息

[Router] display ipv6 neighbors

- 显示可以配置IPv6地址的接口的IPv6信息

[Router] display ipv6 interface

- 清除IPv6邻居信息

<Router> reset ipv6 neighbors

www.h3c.com

在完成 ND 配置后，在任意视图下执行 **display** 命令可以显示 IPv6 配置后的运行情况，以查看显示信息验证配置的效果。在用户视图下，执行 **reset** 命令可以清除相应的统计信息。

下表列出了常见的几个 IPv6 显示和维护命令。

表22-3 IPv6 显示和维护

操作	命令
显示邻居信息	display ipv6 neighbors
显示可以配置IPv6地址的接口的IPv6信息	display ipv6 interface
清除IPv6邻居信息	reset ipv6 neighbors

display ipv6 neighbors信息详解

紫光集团 H3C
核心企业 数字化转型领导者

```

[RTB]dis ipv6 neighbors all
Type: S-Static      D-Dynamic      O-Openflow      R-Rule      I-Invalid
IPv6 address      Link layer      VID      Interface      State      T      Age
2001::1           90a7-7292-0105      N/A      GE0/0          REACH      D      4
  
```

链路层地址

邻居的状态

邻居信息的类型

www.h3c.com

使用 `display ipv6 neighbors` 命令可查看设备上 IPv6 邻居信息。以下是输出示例：

```

[RTB]dis ipv6 neighbors all
Type: S-Static      D-Dynamic      O-Openflow      R-Rule      I-Invalid
IPv6 address      Link layer      VID      Interface      State      T      Age
2001::1           90a7-7292-0105      N/A      GE0/0          REACH      D      4
  
```

输出命令中各参数描述如下表：

表22-4 display ipv6 neighbors 命令显示信息描述表

字段	描述
IPv6 Address	邻居的IPv6地址
Link-layer	链路层地址（邻居的MAC地址）
VID	与邻居相连的接口所属的VLAN
Interface	与邻居相连的接口
State	邻居的状态，包括： <ul style="list-style-type: none"> • INCMP：正在解析地址，邻居的链路层地址尚未确定； • REACH：邻居可达； • STALE：未确定邻居是否可达； • DELAY：未确定邻居是否可达，延迟一段时间发送邻居请求报文； • PROBE：未确定邻居是否可达，发送邻居请求报文来验证邻居的可达性。

字段	描述
T	邻居信息的类型，S表示静态配置，D表示动态获取，O表示从OpenFlow特性获取，I表示无效
Age	静态项显示“-”，动态项显示上次可达以来经过的时间（单位为秒），如果始终不可达则显示“#”（只适用于动态项）

22.6 本章总结

本章总结

- 邻居发现协议是IPv6中的基础协议
- 邻居发现协议包括了地址解析、无状态地址自动配置等重要功能
- 通过交互NS和NA报文完成地址解析
- 通过交互RS和RA报文完成地址自动配置
- ND协议的配置和显示

22.7 习题和解答

22.7.1 习题

1. 以下哪些是邻居发现协议所提供的功能？（ ）
A. 地址解析 B. 邻居不可达检测
C. 重复地址检测 D. 无状态地址自动配置
2. IPv6 地址解析功能由 ND 协议的哪些报文完成？（ ）
A. RS B. RA C. NS D. NA E. Redirect
3. IPv6 无状态地址自动配置功能由 ND 协议的哪些报文完成？（ ）
A. RS B. RA C. NS D. NA E. Redirect
4. 在邻居不可达检测过程中，邻居的哪些状态是稳定状态？（ ）
A. INCOMPLETE（未完成）状态 B. REACHABLE（可达）状态
C. STALE（失效）状态 D. DELAY（延迟）状态
E. PROBE（探测）状态
5. 下列哪一条命令用来配置取消对 RA 消息发布的抑制？（ ）
A. [Router] ipv6 nd ra halt B. [Router] undo ipv6 nd ra halt
C. [Router-Serial2/0] ipv6 nd ra halt D. [Router-Serial2/0] undo ipv6 nd ra halt

22.7.2 习题答案

1. ABCD
2. CD
3. AB
4. C
5. D

第23章 IPv6 路由协议

由于 IP 地址的缺乏，最终 IPv4 必将过渡到 IPv6，而 IPv6 路由协议也将会取代 IPv4 的路由协议。本章介绍了 IPv6 路由协议分类，静态路由、RIPng、OSPFv3 等常用 IPv6 路由协议的原理及配置。

23.1 本章目标

课程目标

● 学习完本课程，您应该能够：

- 掌握IPv6路由协议分类
- 掌握IPv6路由表显示与查看
- 掌握RIPng协议的配置
- 掌握OSPFv3协议的配置



www.h3c.com

23.2 IPv6路由协议概述

IPv6路由分类



路由协议	协议算法	IGP/EGP
RIPng	距离矢量	IGP
OSPFv3	链路状态	IGP
IPv6-IS-IS	链路状态	IGP
BGP4+	路径矢量	EGP

- 与IPv4相同，路由的来源包括直连、静态、动态

www.h3c.com

与 IPv4 路由相同，IPv6 路由可以通过三种方式生成，分别是通过链路层协议直接发现生成的直连路由，通过手工配置生成的静态路由和通过路由协议计算生成的动态路由。

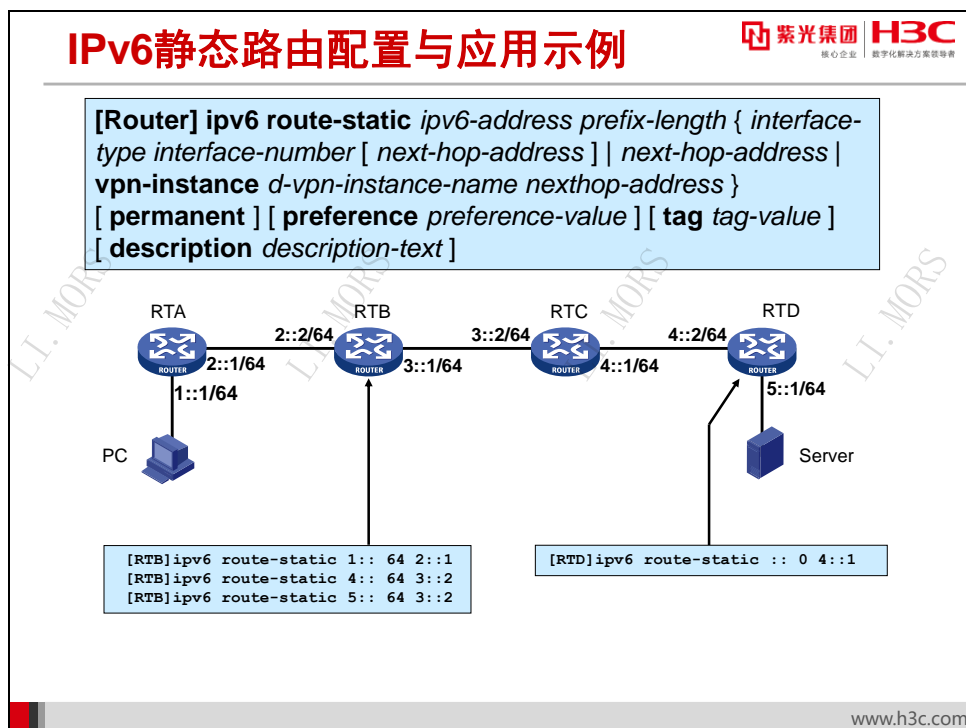
IPv6 路由协议共有 4 种，为 RIPng、OSPFv3、IPv6-IS-IS 和 BGP4+。

IPv6 路由协议根据作用的范围，可分为：

- 在一个自治系统内部运行的内部网关协议，包括 RIPng、OSPFv3 和 IPv6-IS-IS。
- 运行于不同自治系统之间的外部网关协议，包括 BGP4+。

根据使用的算法，又可分为：

- 距离矢量协议，包括 RIPng 和 BGP4+。其中 BGP 也被称为路径矢量协议。
- 链路状态协议，包括 OSPFv3 和 IPv6-IS-IS。



IPv6 静态路由与 IPv4 静态路由类似，适合于一些结构比较简单的 IPv6 网络。

它们之间的主要区别是目的地址和下一跳地址有所不同，IPv6 静态路由使用的是 IPv6 地址，而 IPv4 静态路由使用 IPv4 地址。

在配置 IPv6 静态路由时，如果指定的目的地址为::/0（前缀长度为 0），则表示配置了一条 IPv6 缺省路由。

在系统视图下配置 IPv6 静态路由的命令如下所示：

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number
[ next-hop-address ] | next-hop-address | vpn-instance d-vpn-instance-name
nexthop-address } [ permanent ] [ preference preference-value ] [ tag tag-value ]
[ description description-text ]
```

在上图所示网络中，RTA 和 RTB 配置为 IPv6 缺省路由，RTB 和 RTC 配置了 IPv6 静态路由。

RTA 的配置：

```
[RTA] ipv6 route-static :: 0 2::2
```

RTB 的配置：

```
[RTB]ipv6 route-static 1:: 64 2::1
[RTB]ipv6 route-static 4:: 64 3::2
[RTB]ipv6 route-static 5:: 64 3::2
```

RTC 的配置：

```
[RTC]ipv6 route-static 1:: 64 3::1
```

```
[RTC]ipv6 route-static 2:: 64 3::1
[RTC]ipv6 route-static 5:: 64 4::2
```

RTD 的配置:

```
[RTD] ipv6 route-static :: 0 4::1
```

配置完成后, PC 可以通过 IPv6 来访问服务器。

IPv6路由表显示

紫光集团 核心企业 数字化转型与智能领导者

```
[RTA]display ipv6 routing-table

Routing Table :
    Destinations : 5          Routes : 5

Destination: 3::/64
NextHop    : FE80::20F:E2FF:FE43:1136      Protocol : RIPng
Interface  : GE0/0                          Preference: 100
                                              Cost      : 1

Destination: 4::1/128
NextHop    : FE80::20F:E2FF:FE50:4430      Protocol : O_INTRA
Interface  : GE0/0                          Preference: 10
                                              Cost      : 10

Destination: 2::/64
NextHop    : 1::2                          Protocol : Static
Interface  : GE0/0                          Preference: 80
                                              Cost      : 0

Destination: FE80::/10
NextHop    : ::                             Protocol : Direct
Interface  : InLoop0                         Preference: 0
                                              Cost      : 0
```

● 路由下一跳可以是链路本地地址

www.h3c.com

在任意视图下使用命令 **display ipv6 routing-table** 可查看设备上 ipv6 路由表的信息。

```
[RTA]display ipv6 routing-table
```

```
Routing Table :
    Destinations : 5          Routes : 5

Destination: 3::/64
NextHop    : FE80::20F:E2FF:FE43:1136      Protocol : RIPng
Interface  : GE0/0                          Preference: 100
                                              Cost      : 1

Destination: 4::1/128
NextHop    : FE80::20F:E2FF:FE50:4430      Protocol : O_INTRA
Interface  : GE0/0                          Preference: 10
                                              Cost      : 1

Destination: 2::/64
NextHop    : 1::2                          Protocol : Static
Interface  : GE0/0                          Preference: 80
                                              Cost      : 0

Destination: FE80::/10
NextHop    : ::                             Protocol : Direct
Interface  : InLoop0                         Preference: 0
                                              Cost      : 0
```

命令输出中各字段的含义如下表所示:

表23-1 display ipv6 routing-table 命令显示信息描述


字段	描述
Destination	目的网络/主机的IPv6地址和前缀
NextHop	下一跳地址
Preference	路由优先级
Interface	出接口，即到该目的地址的数据包将从此接口发出

在路由表输出中可以看到，IPv6 动态路由的下一跳是链路本地地址。这样做的好处是有利于保持路由表的稳定。因为链路本地地址是由接口的 MAC 地址经过 EUI-64 算法得出，其地址是固定的。路由器上接口全局 IP 的变化不会导致邻居路由器路由表中下一跳地址的变化。

23.3 RIPng协议

RIPng概述

- **RIPng是对原来的IPv4网络中RIPv2协议的扩展，工作机制与RIPv2基本相同。**
- **同样是基于D-V算法的路由协议，具有距离矢量路由协议的所有特点。**
- **针对IPv6应用环境，RIPng协议报文进行了如下修改**
 - 使用UDP的521端口收发报文
 - 组播地址是FF02::9
 - 源地址是链路本地地址



核心企业 | 数字化解决方案领导者

www.h3c.com

RIPng（RIP next generation，下一代 RIP 协议）是 RIP 协议针对 IPv6 网络而做的修改和增强。它与 RIPv2 同样是基于 D-V（Distance Vector，距离矢量）算法的路由协议，具有距离矢量路由协议的所有特点。为了在 IPv6 网络中应用，RIPng 对原有的 RIP 协议进行了如下修改：

- **UDP 端口号：**使用 UDP 的 521 端口发送和接收路由信息。
- **组播地址：**使用 FF02::9 作为链路本地范围内的 RIPng 路由器组播地址。
- **前缀长度：**目的地址使用 128 比特的前缀长度。
- **下一跳地址：**使用 128 比特的 IPv6 地址。
- **源地址：**使用链路本地地址 FE80::/10 作为源地址发送 RIPng 路由信息更新报文。

RIPng 的工作机制与 RIPv2 基本相同。

RIPng基本配置

 紫光集团 H3C
核心企业 数字化转型领导者

- 创建RIPng进程并进入RIPng视图

```
[Router] ripng [ process-id ]
```

- 在指定的网络接口上使能RIPng协议

```
[Router-Serial2/0] ripng process-id enable
```

www.h3c.com

在配置 RIPng 基本功能之前，需要在路由器上启动 IPv6 报文转发功能，并配置接口的网络层地址，使相邻节点的网络层可达。

配置 RIPng 的基本功能步骤如下：

第1步：在系统视图下创建 RIPng 进程并进入 RIPng 视图。

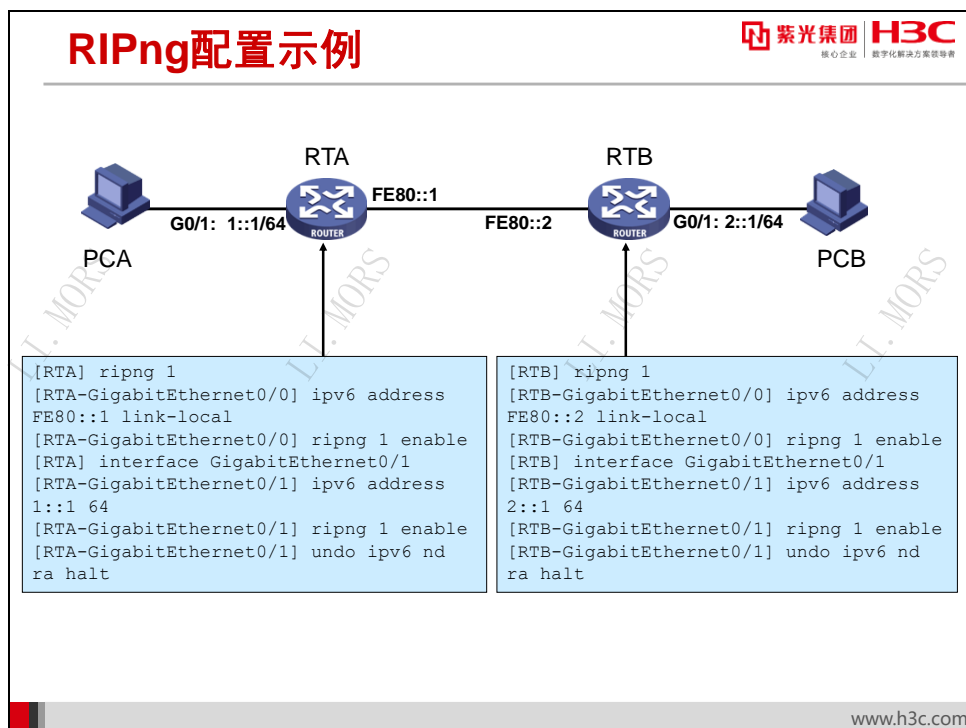
```
ripng [ process-id ]
```

缺省情况下，没有 RIPng 进程在运行。所以，必须手工创建 RIPng 进程。如果没有指定进程 ID，系统的缺省进程 ID 为 1。

第2步：在接口视图下在指定的网络接口上使能 RIPng 。

```
ripng process-id enable
```

此命令的作用是使 RIPng 进程在接口上收发 RIPng 路由。如果接口没有使能 RIPng，那么 RIPng 进程在该接口上既不发送也不接收 RIPng 路由。



在上图所示网络中，RTA 和 RTB 运行 RIPng 协议来交换路由信息；同时，RTA 和 RTB 连接有 PC，作为 PC 的网关。

因为 RIPng 协议使用链路本地地址作为源地址发送路由更新报文，所以路由器间的互联地址可配置为链路本地地址。这样做的好处是减少不必要的全局地址，并有利于网络维护。

RTA 的配置如下：

```
[RTA] ripng 1
[RTA-GigabitEthernet0/0] ipv6 address FE80::1 link-local
[RTA-GigabitEthernet0/0] ripng 1 enable
[RTA] interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1] ipv6 address 1::1 64
[RTA-GigabitEthernet0/1] ripng 1 enable
[RTA-GigabitEthernet0/1] undo ipv6 nd ra halt
```

RTB 的配置如下：

```
[RTB] ripng 1
[RTB-GigabitEthernet0/0] ipv6 address FE80::2 link-local
[RTB-GigabitEthernet0/0] ripng 1 enable
[RTB] interface GigabitEthernet0/1
[RTB-GigabitEthernet0/1] ipv6 address 2::1 64
[RTB-GigabitEthernet0/1] ripng 1 enable
[RTB-GigabitEthernet0/1] undo ipv6 nd ra halt
```

说明：

因为网络中 PC 需要自动获得 IPv6 全局地址，所以在接口视图下使用命令 `undo ipv6 nd ra halt` 来取消对 RA 消息发布的抑制。

RIPng显示与维护



● 显示RIPng进程的配置信息

```
[Router] display ripng [ process-id ]
```

● 显示指定RIPng进程的路由信息

```
[Router] display ripng process-id route
```

● 显示RIPng的接口信息

```
[Router] display ripng process-id interface  
[ interface-type interface-number ]
```

www.h3c.com

在任意视图下执行 **display** 命令可以显示配置后 RIPng 的运行情况，通过查看显示信息验证配置的效果。

display ripng 命令用来显示指定 RIPng 进程的当前运行状态及配置信息。以下是输出示例：

```
<Router> display ripng
```

```
Public VPN-instance name:
```

```
RIPng process: 1
```

```
Preference: 100
```

```
Checkzero: Enabled
```

```
Default cost: 0
```

```
Maximum number of load balanced routes: 6
```

```
Update time : 30 secs Timeout time : 180 secs
```

```
Suppress time : 120 secs Garbage-collect time : 120 secs
```

```
Update output delay: 20(ms) Output count: 3
```

```
Graceful-restart interval: 60 secs
```

```
Triggered Interval : 5 50 200
```

```
Number of periodic updates sent: 0
```

Number of trigger updates sent: 0 其中重要的参数含义如下表所示：

表23-2 display ripng 命令显示说明

字段	描述
RIPng Process	RIPng进程号
Preference	RIPng路由优先级
Update time	Update定时器的值，单位为秒
Timeout time	Timeout定时器的值，单位为秒

字段	描述
Suppress time	Suppress定时器的值，单位为秒
Garbage-Collect time	Garbage-Collect定时器的值，单位为秒

display ripng route 命令用来显示指定 RIPng 进程的路由信息。

display ripng interface 命令用来显示指定 RIPng 进程的接口信息。以下是输出示例：

```
<Router> display ripng 1 interface
Interface: GigabitEthernet0/0
  Link-local address: FE80::1
  Split-horizon: On           Poison-reverse: Off
  MetricIn: 0                 MetricOut: 1
  Default route: Off
  Update output delay: 20 (ms) Output count: 3
```

其中重要的参数含义如下表所示：


表23-3 display ripng interface 命令显示信息解释

字段	描述
Interface	运行RIPng协议的接口的名称
Link Local Address	运行RIPng协议的接口的链路本地地址
Split-horizon	是否使能了水平分割（on表示使能，off表示关闭）
Poison-reverse	是否使能了毒性逆转（on表示使能，off表示关闭）

23.4 OSPFv3 协议

OSPFv3 概述

- **OSPFv3 是 OSPF（Open Shortest Path First，开放式最短路径优先）版本 3**
- **相对于 OSPFv2，OSPFv3 进行了如下修改：**
 - 运行机制变化
 - 功能有所扩展
 - 报文格式变化
 - LSA 格式变化



紫光集团 H3C
核心企业 数字化解决方案领导者

www.h3c.com

OSPFv2（Open Shortest Path First version 2，开放式最短路径优先协议版本 2）在报文格式、运行机制等方面与 IPv4 地址联系紧密，这大大制约了它的可扩展性。为了使 OSPF 能够很好的应用于 IPv6 同时保留其众多优点，IETF 制定了应用于 IPv6 的 OSPF 即 OSPFv3（Open Shortest Path First version 3，开放式最短路径优先协议版本 3）。

OSPFv3 沿袭了 OSPFv2 的协议框架，其网络类型、邻居发现和邻接建立机制、协议状态机、协议报文类型和 OSPFv2 基本一致。为了更好的支持 IPv6 且增强可扩展性，OSPFv3 在以下方面有所修改：

- 运行机制变化

主要是针对 IPv6 的特点进行了相应的修订，并将拓扑描述与 IP 网络描述分开。

- 功能有所扩展

增加了单链路运行多 OSPF 实例的能力；增加了对不识别的 LSA 的处理能力，协议具备了更好的适用性。

- 报文格式变化

针对 IPv6 进行相应的报文修改，取消 OSPFv2 中的验证字段，增加了 Instance ID 字段用于区分同一链路上的不同 OSPF 实例。

- LSA 格式变化

新增加两种 LSA，并对 Type-3 LSA 和 Type-4 LSA 的名称进行了修改。

OSPFv3与OSPFv2运行机制比较

紫光集团 H3C
核心企业 数字化解决方案领导者

- **OSPFv3与OSPFv2的相同点**
 - 相同的SPF算法
 - 区域和Router ID的概念没有变化
 - 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的不同点**
 - OSPFv3是基于链路（Link）运行，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
 - OSPFv3是通过Router ID来标识邻接的邻居，OSPFv2则是通过IP地址来标识邻接的邻居
 - OSPFv3取消了报文中的验证

www.h3c.com

在运行机制方面，OSPFv3 和 OSPFv2 在很多方面是相同的：

- 使用相同的 SPF 算法，根据开销来决定最佳路径；
- 区域和 Router ID 的概念没有变化。OSPFv3 中的 Router ID，Area ID 与仍然是 32 位，与 OSPFv2 完全相同。
- 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。

但同时，它们也有很多不同之处：

- OSPFv3 是基于链路（Link）运行，OSPFv2 是基于网段（Network）运行。

在 OSPFv2 中，协议的运行是基于子网的，路由器之间形成邻居关系的条件之一就是两端接口的 IP 地址必须属于同一网段。

OSPFv3 基于链路运行，同一个链路上可以有多个 IPv6 子网。OSPFv2 中的网段、子网等概念在 OSPFv3 中都被链路所取代。由于 OSPFv3 不受网段的限制，所以两个具有不同 IPv6 前缀的节点可以在同一条链路上建立邻居关系。

- OSPFv3 在同一条链路上可以运行多个实例。

OSPFv3 在协议报文中增加了“instance ID”字段，用于标识不同的实例。路由器在报文接收时对该字段进行判断，只有报文中的实例号和接口配置的实例号相匹配时报文才会处理，否则丢弃。这样，一条链路可以运行多个 OSPF 实例，且各实例独立运行，互相之间不受影响。

- OSPFv3 是通过 Router ID 来标识邻接的邻居，OSPFv2 则是通过 IP 地址来标识邻接的邻居。

OSPFv3 中，Router ID、Area ID 和 Link State ID 仍保留为 32 位，不以 IPv6 地址形式赋值；DR 和 BDR 也只通过 Router ID 来标识，不通过 IPv6 地址进行标识。这样做的好处是，OSPFv3 可以独立于网络层协议运行，大大提高了协议的扩展性。

- OSPFv3 取消了报文中的验证。

OSPFv3 取消了报文中的验证字段，改为使用 IPv6 中的扩展头 AH 和 ESP 来保证报文的完整性和机密性。这在一定程度上简化了 OSPF 协议的处理。

OSPFv3与OSPFv2中的LSA比较	
OSPFv3	OSPFv2
Router-LSA	Router-LSA (Type-1 LSA)
Network-LSA	Network-LSA (Type-2 LSA)
Inter-Area-Prefix-LSA	Network-Summary-LSA (Type-3 LSA)
Inter-Area-Router-LSA	ASBR-Summary-LSA (Type-4 LSA)
AS-external-LSA	AS-external-LSA (Type-5 LSA)
Link-LSA	-
Intra-Area-Prefix-LSA	-

OSPFv3 中，IPv6 地址信息仅包含在部分 LSA 的载荷中。其中 Router-LSA 和 Network-LSA 中不再包含地址信息，仅用来描述网络拓扑。增加了一种新的 LSA——Intra-Area-Prefix-LSA 来携带 IPv6 地址前缀，用于发布区域内的路由。

OSPFv3 还新增了另一种 LSA——Link-LSA，用于路由器向链路上其他路由器通告自己的链路本地地址以及本链路上的所有 IPv6 地址前缀。Link-LSA 只在本地链路范围内传播。

除了新增加两种 LSA 外，OSPFv3 还对 Type-3 LSA 和 Type-4 LSA 的名称进行了修改。在 OSPFv3 中 Type-3 LSA 更名为 Inter-Area-Prefix-LSA，Type-4 LSA 更名为 Inter-Area-Rouer-LSA。

下表列出了 OSPFv3 中 7 类 LSA 的名称和描述。

表23-4 OSPFv3 中 LSA 名称和描述

LSA 名称	作用描述
Router-LSA	由每个路由器生成，描述本路由器的链路状态和开销，只在路由器所处区域内传播。
Network-LSA	由广播网络和NBMA网络的DR生成，描述本网段接口的链路状态，只在DR所处区域内传播。
Inter-Area-Prefix-LSA	和OSPFv2中的Type-3 LSA类似，该LSA由区域边界路由器ABR生成，在与该LSA相关的区域内传播。每一条Inter-Area-Prefix-LSA描述了一条到达本自治系统内其他区域的IPv6地址前缀（IPv6 Address Prefix）的路由。
Inter-Area-Router-LSA	和OSPFv2中的Type-4 LSA类似，该LSA由区域边界路由器ABR生成，在与该LSA相关的区域内传播。每一条Inter-Area-Router-LSA描述了一条到达本自治系统内的自治系统边界路由器ASBR的路由。
AS-external-LSA	由自治系统边界路由器ASBR生成，描述到达其它AS（Autonomous System，自治系统）的路由，传播到整个AS（Stub区域除外）。
Link-LSA	路由器为每一条链路生成一个Link-LSA，在本地链路范围内传播。每一个Link-LSA描述了该链路上所连接的IPv6地址前缀及路由器的Link-local地址。
Intra-Area-Prefix-LSA	每个Intra-Area-Prefix-LSA包含路由器上的IPv6前缀信息，Stub区域信息或穿越区域（Transit Area）的网段信息，该LSA在区域内传播。

OSPFv3与OSPFv2中的协议报文比较

紫光集团 H3C
核心企业 数字化转型领导者

- OSPFv3保留了与OSPFv2相同的5类协议报文，Hello、DD、LSR、LSU和LSAck，但其细节有所不同

协议报文	OSPFv3	OSPFv2
版本号	3	2
协议端口号	89	89
源地址	链路本地地址	接口IP地址
AllSPFRouters组播地址	FF02::5	224.0.0.5

www.h3c.com

OSPF 有五种协议报文，分别为 Hello、Database Description、LSR、LSU 和 LSAck。这五种报文都以一个 16 字节的头部作为报文的开始。

OSPFv3 取消了 OSPFv2 中的验证字段，增加了 Instance ID 字段用于区分同一链路上的不同 OSPF 实例。此外，OSPFv3 的 Version 字段的值为 3，表示该报文是一个 OSPFv3 报文，其他字段和 OSPFv2 中的对应字段保持一致。

OSPFv3 协议号为 89，对应 IPv6 报文的 Next Header 字段为 0x59。OSPFv3 协议报文的源 IPv6 地址除了虚连接外，一律使用链路本地地址。虚连接使用全球单播地址作为协议报文的源地址。

目的 IPv6 地址则是根据不同应用场合选择 AllSPFRouters、AllDRouters 以及邻居路由器 IPv6 地址这三种地址中的一种。AllSPFRouters 为 IPv6 组播地址 FF02::5，所有运行 OSPFv3 的路由器都需要接收目的地址为该地址的 OSPFv3 协议报文，如 Hello 报文。AllDRouters 为 IPv6 组播地址 FF02::6，DR 和 BDR 都需要接收目的地址为该地址的 OSPFv3 协议报文，如由于链路发生变化导致 DR-Other 发送的 LSU 报文。

OSPFv3基本配置



- 启动OSPFv3进程

```
[Router] ospfv3 [ process-id ]
```

- 配置路由器的ID

```
[Router-ospfv3-1] router-id router-id
```

- 在接口上使能OSPFv3协议

```
[Router-Serial2/0] ospfv3 process-id area area-id  
[ instance instance-id ]
```

www.h3c.com

配置 OSPFv3 的基本功能步骤如下：

第1步：在系统视图下创建 OSPFv3 进程并进入 OSPFv3 视图。

```
ospfv3 [ process-id ]
```

OSPFv3 进程号在启动 OSPFv3 时进行设置，它只在本地有效，不影响与其它路由器之间的报文交换。如果没有指定进程 ID，则系统缺省的进程 ID 为 1。

第2步：在 OSPFv3 视图配置路由器的 ID。

```
router-id router-id
```

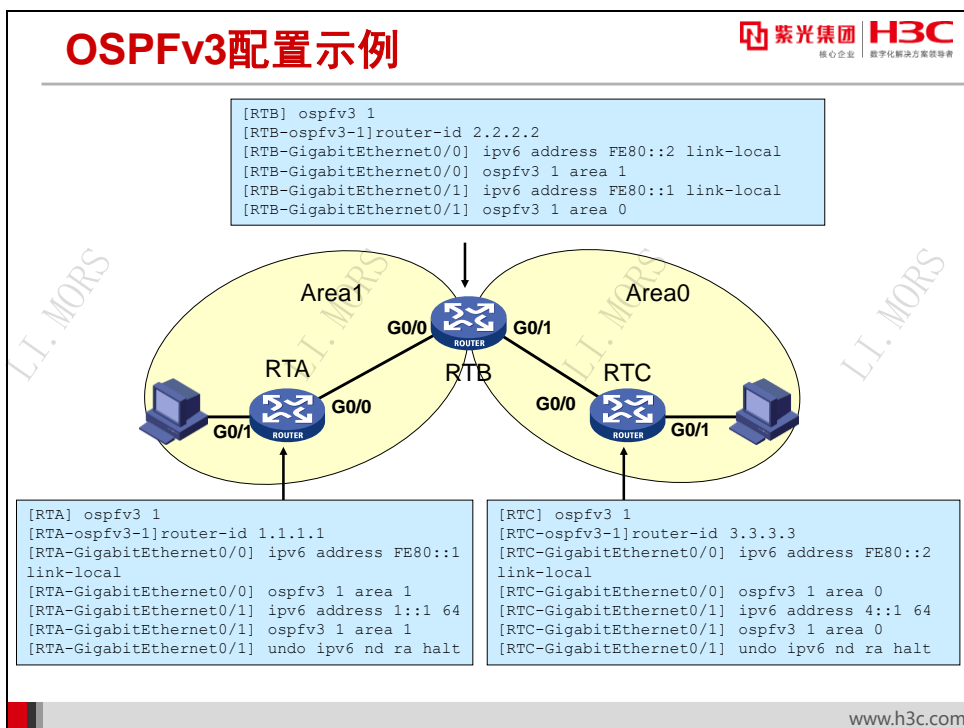
与 OSPFv2 不同，OSPFv3 的 Router ID 必须手工配置，如果没有配置 Router ID，OSPFv3 无法正常运行。

配置 Router ID 时，必须保证自治系统中任意两台路由器的 Router ID 都不相同。如果在同一台路由器上运行了多个 OSPFv3 进程，必须为不同的进程指定不同的 Router ID。

第3步：在接口视图下在指定的网络接口上使能 OSPFv3。

```
ospfv3 process-id area area-id [ instance instance-id ]
```

配置此命令后，相应的接口将属于指定的区域，并能够与邻居路由器收发 OSPFv3 路由。同时，此命令也可以指定接口的实例 ID。



在上图所示的网络中，整个自治系统划分为 2 个区域。其中 RTA 属于区域 1，RTC 属于区域 0，RTB 作为 ABR 来转发区域之间的路由。

OSPFv3 基于链路运行，其协议报文源地址是链路本地地址。所以，路由器间的互联地址可配置为链路本地地址。

RTA 配置如下：

```

[RTA] ospfv3 1
[RTA-ospfv3-1]router-id 1.1.1.1
[RTA-GigabitEthernet0/0] ipv6 address FE80::1 link-local
[RTA-GigabitEthernet0/0] ospfv3 1 area 1
[RTA-GigabitEthernet0/1] ipv6 address 1::1 64
[RTA-GigabitEthernet0/1] ospfv3 1 area 1
[RTA-GigabitEthernet0/1] undo ipv6 nd ra halt
  
```

RTB 配置如下：

```

[RTB] ospfv3 1
[RTB-ospfv3-1]router-id 2.2.2.2
[RTB-GigabitEthernet0/0] ipv6 address FE80::2 link-local
[RTB-GigabitEthernet0/0] ospfv3 1 area 1
[RTB-GigabitEthernet0/1] ipv6 address FE80::1 link-local
[RTB-GigabitEthernet0/1] ospfv3 1 area 0
  
```

RTC 配置如下：

```

[RTC] ospfv3 1
[RTC-ospfv3-1]router-id 3.3.3.3
[RTC-GigabitEthernet0/0] ipv6 address FE80::2 link-local
[RTC-GigabitEthernet0/0] ospfv3 1 area 0
[RTC-GigabitEthernet0/1] ipv6 address 4::1 64
[RTC-GigabitEthernet0/1] ospfv3 1 area 0
[RTC-GigabitEthernet0/1] undo ipv6 nd ra halt
  
```

OSPFv3显示与维护

- 显示OSPFv3进程的概要信息

```
[Router] display ospfv3 [ process-id ]
```

- 显示OSPFv3路由表信息

```
[Router] display ospfv3 [ process-id ] routing
```

- 显示OSPFv3邻居信息

```
[Router] display ospfv3 [ process-id ] peer
```

- 显示OSPFv3的LSDB信息

```
[Router] display ospfv3 [ process-id ] lsdb
```

www.h3c.com

在任意视图下执行 **display** 命令可以显示配置后 OSPFv3 的运行情况，通过查看显示信息验证配置的效果。

display ospfv3 命令用来查看 OSPFv3 进程的概要信息。其输出如下所示：

```
<Router> display ospfv3
OSPFv3 Process 1 with Router ID 1.1.1.1

RouterID: 1.1.1.1          Router type:
Route tag: 0
Route tag check: Disabled
Multi-VPN-Instance: Disabled
Type value of extended community attributes:
  Domain ID : 0x0005
  Route type: 0x0306
  Router ID : 0x0107
Domain-id: 0.0.0.0
DN-bit check: Enabled
DN-bit set: Enabled
SPF-schedule-interval: 5 50 200
LSA generation interval: 5
LSA arrival interval: 1000
Transmit pacing: Interval: 20 Count: 3
Default ASE parameters: Tag: 1
Route preference: 10
ASE route preference: 150
SPF calculation count: 25
External LSA count: 0
LSA originated count: 10
LSA received count: 5
SNMP trap rate limit interval: 10 Count: 7
Area count: 1 Stub area count: 0 NSSA area count: 0
ExChange/Loading neighbors: 0
```

```

Area: 0.0.0.1
Area flag: Normal
SPF scheduled count: 5
ExChange/Loading neighbors: 0
LSA count: 5

```

以上信息表明，路由器的 OSPFv3 进程 ID 是 1，Router ID 是 1.1.1.1。

display ospfv3 routing 命令用来显示 OSPFv3 路由表的信息。其输出如下所示：

```

<Router> display ospfv3 routing

                OSPFv3 Process 1 with Router ID 2.2.2.2
-----
I - Intra area route, E1 - Type 1 external route, N1 - Type 1 NSSA route
IA - Inter area route, E2 - Type 2 external route, N2 - Type 2 NSSA route
* - Selected route

*Destination: 1::1/128
Type      : I                      Cost      : 1
Nexthop    : FE80::1                Interface: GE0/0
AdvRouter   : 1.1.1.1                Area       : 0.0.0.1
Preference : 10

Total: 1
Intra area: 1      Inter area: 0      ASE: 0      NSSA: 0

```

以上信息表明，路由表中有一条区域内路由由 1: 1/128，出接口为 GE0/0，其开销为 1。

display ospfv3 peer 命令用来显示 OSPFv3 邻居的信息。其输出如下所示：

```

<Router>
dis ospfv3 peer

                OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.1
-----
Router ID      Pri State          Dead-Time InstID Interface
2.2.2.2        1 Full/DR          00:00:32  0      GE0/0

```

以上信息表明，路由器在接口 GE0/0 上与 ID 为 2.2.2.2 的路由器建立了邻居关系，其状态为 Full。

display ospfv3 lsdb 命令用来显示 OSPFv3 的链路状态数据库信息。

23.5 本章总结

本章总结

- IPv6路由协议包括RIPng、OSPFv3、IPv6-IS-IS和BGP4+
- RIPng的工作机制与RIPv2基本相同
- OSPFv3针对IPv6进行了修改，并增加了2类LSA
- RIPng的配置与维护
- OSPFv3的配置与维护

www.h3c.com

23.6 习题和解答

23.6.1 习题

1. 以下哪些是链路状态型的 IPv6 路由协议？（ ）
A. RIPng B. OSPF C. OSPFv3 D. BGP4+
2. 关于 RIPng 路由协议的描述，以下哪些是正确的？（ ）
A. 使用 UDP 的 521 端口发送和接收路由信息
B. 使用 FF02::9 作为 RIPng 路由器组播地址
C. 使用链路本地地址 FE80::/10 作为源地址发送路由更新报文
D. 是一种距离矢量型的路由协议
3. 下列哪些是 OSPFv3 和 OSPFv2 之间的相同点？（ ）
A. OSPFv3 和 OSPFv2 具有相同的 LSA 类型
B. OSPFv3 和 OSPFv2 使用相同的 SPF 算法
C. OSPFv3 和 OSPFv2 使用相同的 Router ID 和 Area ID
D. OSPFv3 和 OSPFv2 具有相同的邻居发现机制和邻接形成机制
4. 下列哪一条命令用来配置在接口上使能 RIPng 进程 1？（ ）
A. [RTA] ripng enable B. [RTA] ripng 1 enable
C. [RTA-Ethernet0/0] ripng enable D. [RTA-Ethernet0/0] ripng 1 enable
5. 假定路由 RTA 的接口 Ethernet0/1 的 IPv6 地址为 2001::1/64，则下列哪一条命令用来配置在接口 Ethernet0/1 上使能 OSPFv3 并划分到区域 1？（ ）
A. [RTA] ospfv3 1 area 1 B. [RTA-ospfv3-0.0.0.1] Interface Ethernet0/1
C. [RTA-ospfv3-0.0.0.1] network 2001::0 64
D. [RTA-Ethernet0/1] ospfv3 1 area 1

23.6.2 习题答案

1. C 2. ABCD 3. BCD 4. D 5. D

第24章 IPv6 过渡技术

现阶段，绝大多数网络仍然是 IPv4，过渡到 IPv6 还要相当长的一段时间。在这段时间里，IPv4 和 IPv6 是共同存在的。本章介绍了常用的 IPv6 过渡技术如隧道、NAT-PT 等的原理和配置。

24.1 本章目标

课程目标

○ 学习完本课程，您应该能够：


- 了解过渡技术的分类
- 掌握6to4隧道技术的原理和配置
- 掌握ISATAP隧道技术的原理和配置
- 掌握NAT-PT的原理和配置



www.h3c.com

24.2 IPv6过渡技术概述

IPv6过渡技术概述



- 双协议栈技术
 - 节点同时启用IPv4与IPv6协议栈
- 隧道技术
 - IPv6报文封装在IPv4中
 - 目前的主流技术
- 网络地址转换/协议转换
 - NAT-PT

www.h3c.com

IPv6 过渡技术大体上可以分为以下三类：

- 双协议栈技术
- 隧道技术
- 网络地址转换/协议转换技术

双协议栈技术是指在设备上同时启用 IPv4 和 IPv6 协议栈。IPv6 和 IPv4 是功能相近的网络层协议，两者都基于相同的下层平台。如果网络中的一个节点同时支持 IPv6 和 IPv4 两种协议，那么该节点既能与支持 IPv4 协议的节点通信，又能与支持 IPv6 协议的节点通信，这就是双协议栈技术的工作机理。

双协议栈技术是 IPv6 过渡技术中应用最广泛的一种过渡技术。同时，它也是所有其它过渡技术的基础。

隧道是一种封装技术，它利用一种网络协议来传输另一种网络协议，即利用一种网络传输协议，将其他协议产生的数据报文封装在它自己的报文中，然后在网络中传输。IPv6 隧道是将 IPv6 报文封装在 IPv4 报文中，这样 IPv6 协议报文就可以穿越 IPv4 网络进行通信。对于采用隧道技术的设备来说，在起始端（隧道的入口处），将 IPv6 的数据报文封装入 IPv4 报文中，IPv4 报文的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。在隧道的出口处，再将 IPv6 报文取出转发给目的站点。它的特点是要求隧道两端的网络设备能够支持隧道及双栈技术，而对

网络中其它设备没有要求，因而非常容易实现。但是隧道技术不能实现 IPv4 主机与 IPv6 主机的直接通信。

NAT-PT (Network Address Translation-Protocol Translation) 是指带协议转换功能的网络地址转换器，通过修改协议报文头来转换网络地址，使它们能够互通。NAT-PT 用于 IPv6 网络和 IPv4 网络之间。另外，NAT-PT 通过与应用层网关 (ALG) 相结合，实现了 IPv6 节点和 IPv4 节点间大部分应用的相互通信。

双协议栈技术

紫光集团 H3C
核心企业 数字化转型解决方案领导者

- 双栈的工作原理
 - 同时支持IPv6和IPv4协议
 - 应用程序根据DNS解析地址类型选择使用IPv6或IPv4协议
- 特点
 - 互通性好，实现简单，允许应用逐渐从IPv4过渡到IPv6
 - 只适用双栈节点本身
 - 对每个IPv4节点都要升级，成本较大，没有解决IPv4地址紧缺问题

www.h3c.com

具有双协议栈的节点称作“IPv6/v4 节点”，这些节点既可以收发 IPv4 报文，也可以收发 IPv6 报文。它们可以使用 IPv4 协议与 IPv4 节点互通，也可以使用 IPv6 协议与 IPv6 节点互通。

绝大多数情况下，用户给应用层提供的只是对端通信设备的名字而不是地址，这就要求系统提供名字与地址之间的映射。无论是在 IPv4 中还是在 IPv6 中，这个任务都是由 DNS 完成的。对于 IPv6 地址，定义了新的记录类型“A6”和“AAAA”。由于 IPv4/v6 节点要能够直接与 IPv4 和 IPv6 节点通信，因此 DNS 必须能够同时支持对 IPv4 和 IPv6 的记录类型的解析。

另外，在查询到 IP 地址之后，解析库向应用层返回的 IP 地址可能是 IPv6 地址，也可能是 IPv4 地址，或者是同时返回 IPv6 和 IPv4 地址。所以，应用层必须做出选择使用哪个地址，即使用哪个 IP 协议。具体选择哪一个地址的结果是与应用的环境有关的（也就是与操作系统和应用程序相关）。

双栈技术的优点是互通性好，并且实现简单。其缺点是双栈节点需要维护两个协议栈，系统开销比原来增加了；且每个 IPv6 节点都需要使用一个 IPv4 地址，实际上并没有解决 IPv4 地址紧缺问题，所以只能作为一种临时过渡技术。

24.3 IPv6隧道技术

IPv6隧道技术分类

- 手工隧道技术
 - IPv6手动隧道
- 自动隧道技术
 - IPv4兼容IPv6自动隧道（简称自动隧道）
 - 6to4隧道
 - ISATAP隧道
 - 6PE隧道

www.h3c.com

IPv6 隧道可以建立在主机-主机、主机-设备、设备-主机、设备-设备之间。隧道的终点可能是 IPv6 报文的最终目的地，也可能需要进一步转发。如果隧道的终点不是 IPv6 报文的最终目的地，当 IPv6 报文通过隧道到达隧道终点后，隧道终点设备（通常为路由器）会对封装的 IPv6 报文进行解封装，并转发 IPv6 报文到最终目的地。

根据隧道终点的 IPv4 地址的获取方式不同，隧道分为以下 2 种：

● 手工隧道

如果设备不能从 IPv6 报文的目的地址中自动获取到隧道终点的 IPv4 地址，就需要对隧道终点进行手工配置。这种需要对隧道终点进行配置的隧道称为手工隧道。

手工隧道是点到点之间的链路，一条链路就是一个单独的隧道，通常应用于路由器之间的稳定连接。

● 自动隧道

如果隧道的终点能够从 IPv6 报文的目的地址中自动获取，也就是说隧道终点不需要手工配置，则这种隧道就是自动隧道。通常，自动隧道的实现需要采用内嵌 IPv4 地址的特殊 IPv6 地址形式。

常见的自动隧道包括 IPv4 兼容 IPv6 自动隧道、6to4 隧道、ISATAP 隧道及 6PE 隧道。

6PE 隧道是建立在 MPLS/VPN 网络上的隧道技术。

6to4自动隧道

紫光集团 H3C
核心企业 数字化转型先锋

- 必须使用6to4地址
- 6to4地址格式为2002:abcd:efgh:子网号::接口ID，其中abcd:efgh对应的32位全球唯一的IPv4地址，用16进制表示
- 不需要为每条隧道预先配置目的IPv4地址，由系统从6to4地址中读取
- 维护方便、扩展性强
- 节省系统资源
- 适应于站点间互连

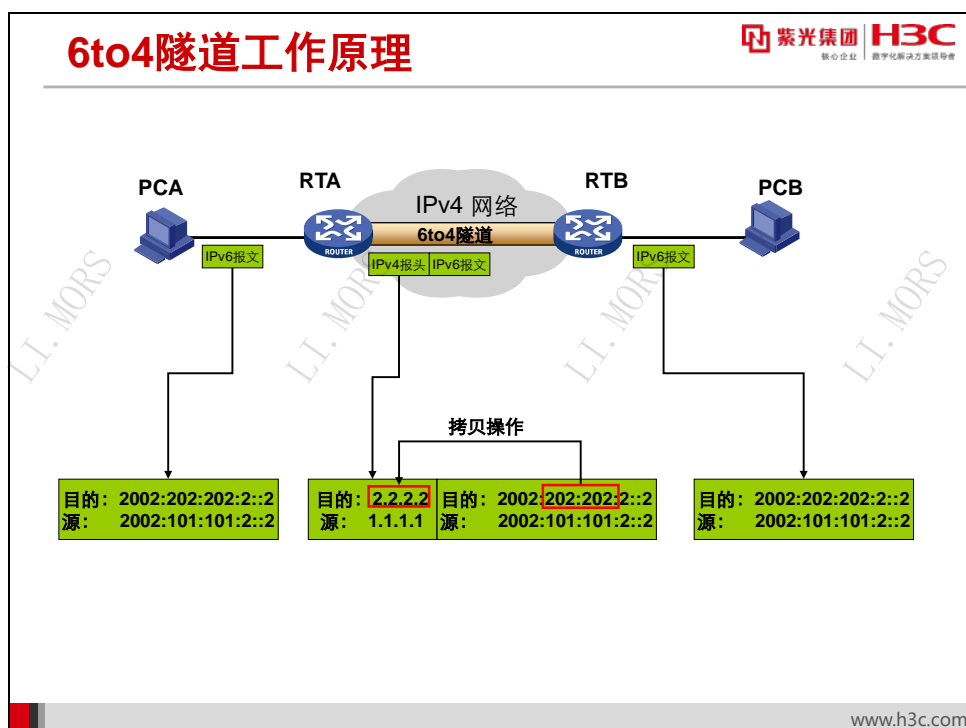
www.h3c.com

6to4 隧道是点到多点的自动隧道，主要用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。6to4 隧道通过 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

6to4 隧道必须采用特殊的 6to4 地址，其格式为 2002:abcd:efgh:子网号::接口 ID，其中 2002 表示固定的 IPv6 地址前缀，abcd:efgh 为用 16 进制表示的 IPv4 地址（如 1.1.1.1 可以表示为 0101:0101），用来唯一标识一个 6to4 网络。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

6to4 地址的网络前缀有 64 位长，其中前 48 位(2002:abcd:efgh)被分配给路由器上的 IPv4 地址决定了，用户不能改变，而后 16 位是由用户自己定义的。这样，6to4 隧道可以实现 IPv6 网络的互连。

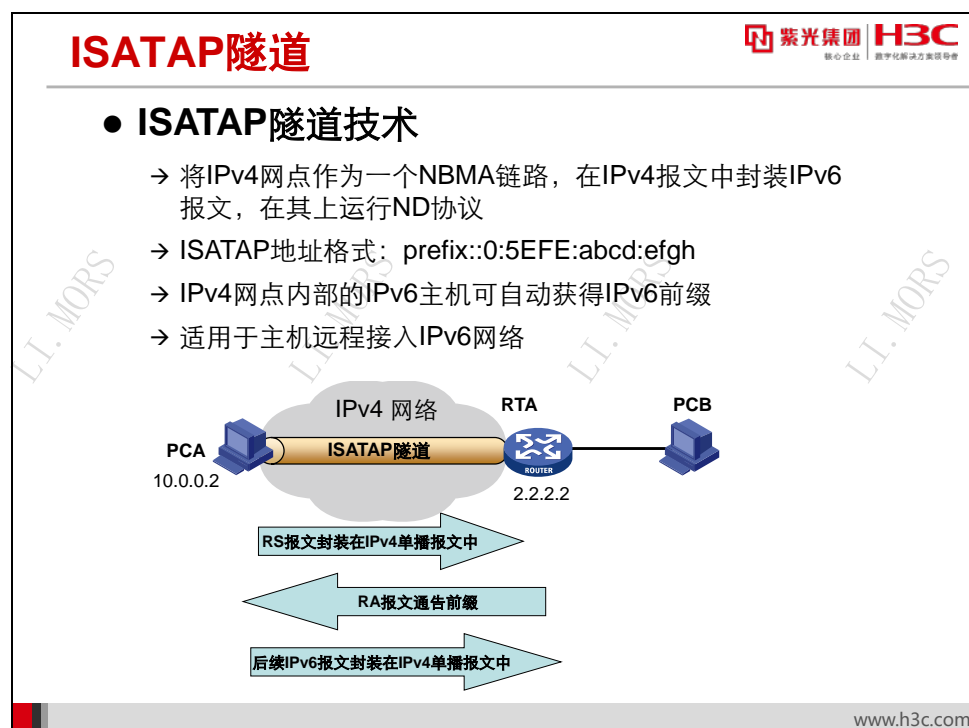
6to4 隧道是随报文建立的隧道，并不需要事先建立；并且，无论要和多少个对端设备建立隧道，本端只需要一个隧道接口。这样可以节省路由器资源，方便路由器的维护，并且易于扩展。



上图显示了 6to4 隧道的工作原理。两台路由器 RTA 和 RTB 通过 6to4 隧道相连。PCA 的 IPv6 地址为 2002:101:101:2::2，PCB 的 IPv6 地址为 2002:202:202:2::2。

当 PCA 发出的 IPv6 报文到达 RTA 后，RTA 查找路由表，发现报文所匹配的路由表项下一跳指向 6to4 隧道接口，于是对其进行报文封装。封装时的源地址就是物理接口的 IPv4 地址 1.1.1.1；目的地址是从 IPv6 报文目的地址 2002:202:202:2::2 中把 IPv4 的部分 202:202 提取出来，就是 2.2.2.2，作为 IPv4 报文的目的地址。封装后从 IPv4 网络转发到 RTB。

RTB 收到此 IPv4 报文后，进行解封装操作，将其中的 IPv6 报文取出，查找路由表后发送至 PCB。



ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) 不但是一种自动隧道技术，同时它可以进行地址自动配置。在 ISATAP 隧道的两端设备之间可以运行 ND 协议。配置了 ISATAP 隧道以后，IPv6 网络将底层的 IPv4 网络看作一个非广播的点到多点的链路(NBMA)。

ISATAP 隧道的地址也有特定的格式，ISATAP 地址格式为：

Prefix:0:5EFE:abcd:efgh/64:

在这里，64 位的 Prefix 为任何合法的 IPv6 单播地址前缀，0:5EFE 是 IANA 规定的格式。abcd:efgh 为用 16 进制表示的 32 位 IPv4 地址（如 1.1.1.1 可以表示为 0101:0101）。ISATAP 地址的前 64 位前缀是通过向 ISATAP 路由器发送请求来得到的。

如上图所示，双栈主机 PCA 与路由器 RTA 通过 ISATAP 隧道相连。PCA 作为一个 ISATAP 主机，配置有 IPv4 地址 10.0.0.2，IPv6 地址由 ISATAP 路由器 RTA 自动分配。路由器 RTA 连接有 IPv4 网络和 IPv6 网络，IPv4 地址是 2.2.2.2，并配置有相应的 ISATAP 隧道接口，负责给 PCA 分配前缀，其前缀为 1::。PCB 是一个 IPv6 主机。

默认情况下，主机会生成链路本地 ISATAP 地址。它的生成方法如下：首先按照前面讲述的方法生成::0:5EFE:A00:2 的接口 ID，然后加上一个前缀 FE80，生成的链路本地 ISATAP 地址就是 FE80::5EFE:A00:2。生成链路本地 ISATAP 地址以后，PCA 就有了 IPv6 连接功能，就可以与路由器进行 ND 协议的交互了。

PCA 与 RTA 之间的交互包括以下几个步骤：

- PCA 发出 RS 报文

按照 ND 协议, PCA 要想获得全局 IPv6 地址, 它首先需要向 ISATAP 路由器发出 RS 报文。RS 报文的源 IPv6 地址就是它自己预先生成的链路本地 ISATAP 地址 FE80::5EFE:A00:2, 目的 IPv6 地址是路由器的组播地址 FF02 ::2。在封装时, 源 IPv4 地址是自己网络接口卡的地址 10.0.0.2, 目的 IPv4 地址是路由器 RTA 的地址 2.2.2.2。

- RTA 回应 RA 报文


RTA 收到 RS 报文后, 需要回复 RA 报文给主机。RA 报文的源 IPv6 地址是 PCA 的链路本地 ISATAP 地址 FE80::5EFE:A00:2。在封装时, 源 IPv4 地址为 2.2.2.2, 目的 IPv4 地址就是从目的 IPv6 地址中内嵌的 IPv4 地址得来的 (A00:2→10.0.0.2), 即为 10.0.0.2。

- 主机得到全局 IPv6 地址

ISATAP 路由器回应的 RA 报文中告诉主机 PCA 前缀为 1::。PCA 把此前缀加上接口 ID: ::0:5EFE: A00:2, 得到一个全局 IPv6 地址 1:: 5EFE:A00:2。

PCA 得到全局 IPv6 地址后, 就可以向 PCB 发起通信了。此时源地址就是自己的全局地址 1:: 5EFE:A00:2。

隧道配置命令



- 创建Tunnel接口

```
[Router] interface tunnel number mode { ds-lite-  
aftr | gre [ ipv6 ] | ipv4-ipv4 | ipv6 | ipv6-ipv4 [ 6to4 |  
auto-tunnel | isatap ] | mpls-te }
```

- 设置Tunnel接口的IPv6单播地址

```
[Router-Tunnel0] ipv6 address { ipv6-address prefix-  
length | ipv6-address/prefix-length }
```

- 设置Tunnel接口的源端地址或接口

```
[Router-Tunnel0] source { ip-address | ipv6-address |  
interface-type interface-number }
```

www.h3c.com

在路由器上配置隧道的基本步骤如下:

第1步: 在系统视图下创建 Tunnel 接口, 指定隧道模式, 并进入 Tunnel 接口视图。

```
interface tunnel number [ mode { ds-lite-aftr | gre [ ipv6 ] | ipv4-ipv4 | ipv6 |  
ipv6-ipv4 [ 6to4 | auto-tunnel | isatap ] | mpls-te } ]
```

缺省情况下设备上没有 Tunnel 接口, 所以必须先创建 Tunnel 接口。

第2步：在接口视图设置 Tunnel 接口的 IPv6 单播地址。

ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }

如果隧道接口是 6to4 隧道或 ISATAP 隧道时，要注意单播地址的格式要符合 6to4 地址或 ISATAP 地址格式。

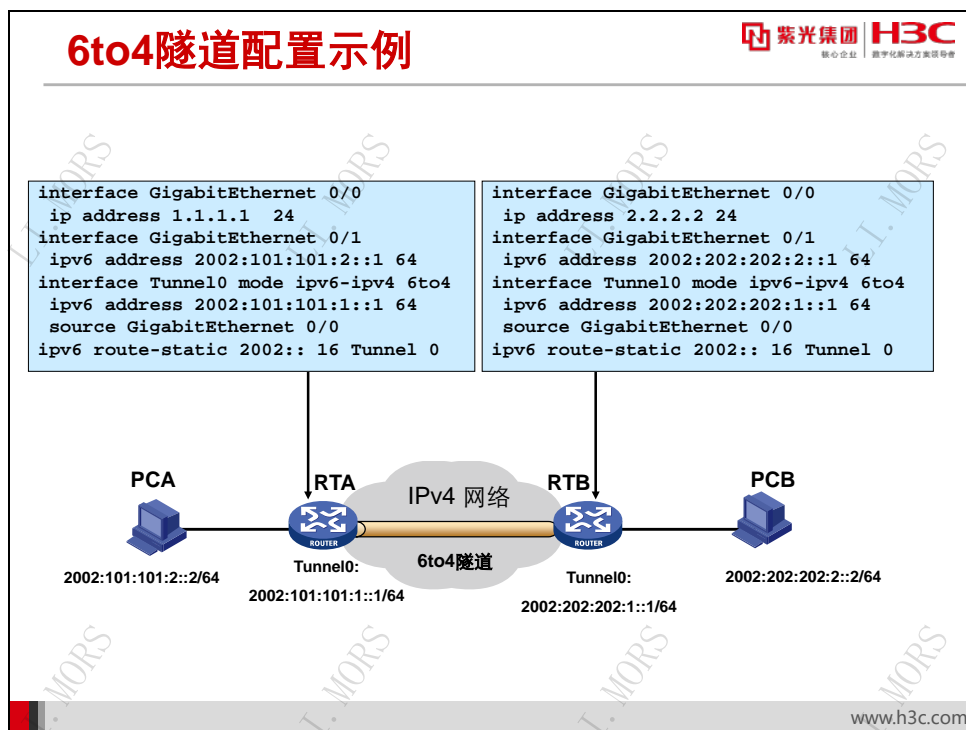
一般情况下，隧道两端 Tunnel 接口的地址需要配置为同一个网段。如果是不同网段，则必须配置通过隧道到达对端的转发路由。

第3步：在隧道接口视图下设置 Tunnel 接口的源端地址或接口。

source { ip-address | ipv6-address | interface-type interface-number }

配置 Tunnel 接口的源端接口后，封装的报文的源地址就是源端接口的地址。

对于 6to4 隧道和 ISATAP 隧道等自动隧道来说，不需要配置 Tunnel 接口的目的端地址，由系统根据 IPv6 报文中的内嵌地址得来；而对于 GRE 等手工隧道来说，需要配置 Tunnel 接口的目的端地址。



在上图所示网络中，PCA 和 PCB 是 IPv6 主机，RTA 和 RTB 是双栈路由器，之间通过 IPv4 网络进行连接。通过在路由器上配置 6to4 隧道接口，使路由器间通过 6to4 隧道而互连起来。

RTA 的配置如下：

```

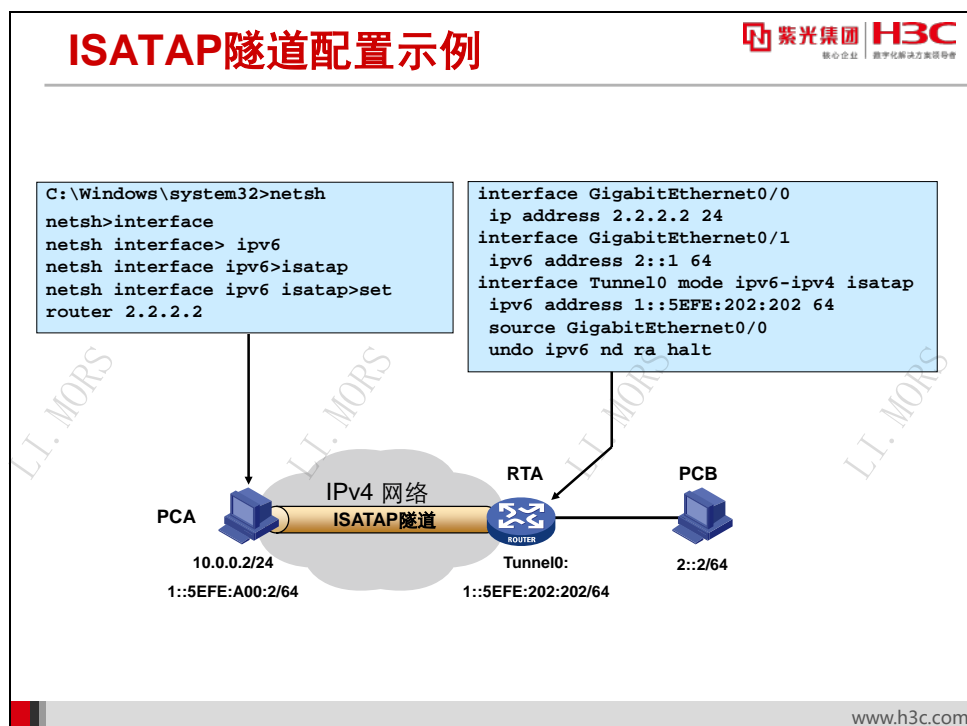
[RTA] interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0] ip address 1.1.1.1 24
[RTA] interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1] ipv6 address 2002:101:101:2::1 64
[RTA] interface Tunnel0 mode ipv6-ipv4 6to4
[RTA-Tunnel0] ipv6 address 2002:101:101:1::1 64
        
```

```
[RTA-Tunnel0] source GigabitEthernet0/0
[RTA] ipv6 route-static 2002:: 16 Tunnel 0
```

RTB 的配置如下:

```
[RTB] interface GigabitEthernet0/0
[RTB-GigabitEthernet0/0] ip address 2.2.2.2 24
[RTB] interface GigabitEthernet0/1[RTB- GigabitEthernet0/1] ipv6 address
2002:202:202:2::1 64
[RTB] interface Tunnel0 mode ipv6-ipv4 6to4
[RTB-Tunnel0] ipv6 address 2002:202:202:1::1 64
[RTB-Tunnel0] source GigabitEthernet0/0
[RTB] ipv6 route-static 2002:: 16 Tunnel 0
```

在以上配置中, 在路由器间配置了 IPv6 静态路由, 以使两端的 IPv6 路由可达。



在上图所示网络中, PCA 位于 IPv4 网络中, IP 地址为 10.0.0.2/24; PCB 位于 IPv6 网络中, 地址为 2::2/64。RTA 是一个双栈路由器, 配置 ISATAP 隧道, 通过 ND 协议给 PCA 分配 ISATAP 地址。

假设主机 PCA 的操作系统是 Windows 7。则在命令行视图使用管理员权限进行如下配置:

```
C:\Windows\system32>>netsh interface ipv6 isatap set router 2.2.2.2
确定。
```

一般情况下, 在 Windows 7 操作系统命令行视图下配置如下命令获取管理员权限:

```
C:\>runas /noprofile /user:Administrator cmd.exe
```

以上配置完成后, PCA 发出的 IPv6 报文进行封装时, 其目的 IPv4 地址就是路由器 RTA 的地址 2.2.2.2。


RTA 的配置如下:

```
[RTA] interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0] ip address 2.2.2.2 24
[RTA] interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1] ipv6 address 2::1 64
[RTA] interface Tunnel0 mode ipv6-ipv4 isatap
[RTA-Tunnel0] ipv6 address 1::5EFE:202:202: 1 64
[RTA-Tunnel0] GigabitEthernet0/0
[RTA-Tunnel0] undo ipv6 nd ra halt
```

配置完成后，如果 PCA 与 RTA 之间进行 ND 协议的交互，RTA 将会给 PCA 分配 1::/64 的前缀。PCA 得到前缀后，与自己的接口 ID 结合起来，生成全局 IPv6 地址 1:: 5EFE:A00:2/64。

24.4 NAT-PT

NAT-PT概述



紫光集团 H3C
核心企业 数字化转型方案领导者

- NAT-PT把协议转换技术和IPv4网络中地址转换技术（NAT）相结合。
- NAT-PT的工作原理
 - 协议转换的目的是实现IPv4和IPv6协议头之间的转换
 - 地址转换是为了使IPv6和IPv4网络中的主机能够识别对方
 - IPv4网络中的主机用IPv4地址标识IPv6网络中的主机
 - IPv6网络中的主机用IPv6地址标识IPv4网络中的主机
- NAT-PT的特点
 - 所有转换都在NAT-PT上实现，对原有网络无影响
 - 报文中有些信息无法转换，且缺少端到端的安全性

www.h3c.com

Pv6 的应用是个循序渐进的过程，在很长时间内，IPv4 网络和 IPv6 网络会同时存在且需要相互通信。通过 NAT-PT（Network Address Translation-Protocol Translation，附带协议转换的网络地址转换）所提供的 IPv4 和 IPv6 地址之间的相互转换功能可以实现这个需求。

NAT-PT 是把协议转换技术与 IPv4 网络中动态地址翻译技术（NAT）相结合的一种技术。

NAT-PT 处于 IPv6 和 IPv4 网络的交界处，可以实现 IPv6 主机与 IPv4 主机之间的互通。协议转换的目的是实现 IPv4 和 IPv6 协议头之间的转换；地址转换则是为了让 IPv6 和 IPv4 网络中的主机能够识别对方，也就是说，IPv4 网络中的主机用 IPv4 地址标识 IPv6 网络中的主机，反过来，IPv6 网络中的主机用 IPv6 地址标识 IPv4 网络中的主机。

NAT-PT 有如下特点：

- 所有转换都在 NAT-PT 上实现，对原有网络无影响

NAT-PT 作用于 IPv4 和 IPv6 网络边缘的设备上，所有的地址转换过程都在该设备上实现，对 IPv4 和 IPv6 网络来说是透明的，用户不必改变目前的 IPv4 网络就可实现 IPv6 网络与 IPv4 网络的通信。

- 报文中有些信息无法转换，且缺少端到端的安全性

由于 IPv6 协议和 IPv4 协议报文头中某些字段不同，所以在进行协议转换时，某些信息会丢失。例如 IPv4 报文头的可选项部分无法转换到 IPv6 报文中，而 IPv6 报文中的目的选项头、路由头、逐跳选项头也无法转换到 IPv4 报文中去。

NAT 转换破坏了 IP 协议端到端的安全性。

NAT-PT种类

- **静态NAT-PT**
 - NAT-PT服务器提供一对一的IPv6地址和IPv4地址的映射
- **动态NAT-PT**
 - 根据需要从地址池中选取空闲地址来完成IPv6地址与IPv4地址的映射
- **NAPT-PT**
 - “地址 + 端口号” 的映射方式，不同的IPv6地址转换时，可以对应同一个IPv4地址

www.h3c.com

有三种 NAT-PT 机制可实现 IPv4 和 IPv6 地址之间的相互转换：

- 静态映射的 NAT-PT 机制

静态映射的 NAT-PT 机制是指采用手工配置的 IPv6 地址与 IPv4 地址的一一对应关系来实现 IPv6 地址与 IPv4 地址的转换。

- 动态映射的 NAT-PT 机制

和静态映射不同，动态映射没有 IPv6 和 IPv4 地址之间的一一对应关系。动态映射要求先创建一个地址池，然后根据需要从地址池中选取空闲地址来完成 IPv6 地址与 IPv4 地址的映射。

- NAPT-PT 机制

NAPT-PT 是在 IP 地址动态转换的基础上对 TCP、UDP 的端口号也进行 IPv6 到 IPv4 的转换。采用这种“地址+端口号”的映射方式，不同的 IPv6 地址转换时，可以对应同一个 IPv4 地址，通过端口号来区分不同的 IPv6 主机，从而使多个 IPv6 主机能共享一个 IPv4 地址完成转换。

静态 NAT-PT 基本配置

紫光集团 H3C
核心企业 数字化转型集团导师

- 使能 NAT-PT 功能

```
[Router-Ethernet0/0] natpt enable
```

- 配置 IPv4 侧报文的静态映射

```
[Router] natpt v4bound static ipv4-address ipv6-address
```

- 配置 IPv6 侧报文的静态映射

```
[Router] natpt v6bound static ipv6-address ipv4-address
```

www.h3c.com

在路由器上配置静态 NAT-PT 的基本步骤如下：

第1步：在接口视图下使能 NAT-PT 功能。

natpt enable

缺省情况下 NAT-PT 功能处于关闭状态，所以必须先使能 NAT-PT 功能，以使接口能够转换报文。

第2步：在系统视图下配置 IPv4 侧报文的静态映射。

natpt v4bound static ipv4-address ipv6-address

IPv4 侧报文映射是指从 IPv4 到 IPv6 的报文转换。当报文从 IPv4 网络发送到 IPv6 网络时，源 IPv4 地址将会按照配置的映射关系转换为 IPv6 地址；静态映射是指设备根据所配置的 IPv4 地址与 IPv6 地址的一一对应关系，把源 IPv4 地址转换为相应的 IPv6 地址。

第3步：在系统视图下配置 IPv6 侧报文的静态映射。

natpt v6bound static ipv6-address ipv4-address

与 IPv4 侧报文的静态映射相反，IPv6 侧静态报文映射是指当报文从 IPv6 网络发送到 IPv4 网络时，源 IPv6 地址将会按照配置的一一映射关系转换为相应的 IPv4 地址。

动态NAT-PT基本配置



- 配置NAT-PT地址池

```
[Router] natpt address-group group-number start-  
ipv4-address end-ipv4-address
```

- 配置NAT-PT前缀

```
[Router] natpt prefix natpt-prefix
```

- 配置IPv4侧报文的动态映射

```
[Router] natpt v4bound dynamic acl number acl-  
number prefix natpt-prefix
```

- 配置IPv6侧报文的动态映射

```
[Router] natpt v6bound dynamic prefix natpt-prefix  
address-group address-group [ no-pat ]
```

www.h3c.com

在路由器上配置动态 NAT-PT 与 NAPT-PT 时，除了要在接口上使能 NAT-PT 功能之外，还要做如下配置：

第1步：在系统视图下配置 NAT-PT 地址池。

```
natpt address-group group-number start-ipv4-address end-ipv4-address
```

NAT-PT 地址池中包含了若干 IPv4 地址。当符合条件的 IPv6 报文通过 NAT-PT 时，NAT-PT 将报文中的源 IPv6 地址转换为地址池中的 IPv4 地址。

第2步：在系统视图下配置 NAT-PT 前缀。

```
natpt prefix natpt-prefix
```

当报文要从 IPv6 网络发送到 IPv4 网络时，接收到该报文的具有 NAT-PT 功能的设备会检测报文 IPv6 目的地址的前缀，只有与所配置的 NAT-PT 前缀相同的报文才允许进行 IPv6 到 IPv4 的转换。

第3步：在系统视图下配置 IPv4 侧报文的动态映射。

```
natpt v4bound dynamic acl number acl-number prefix natpt-prefix
```

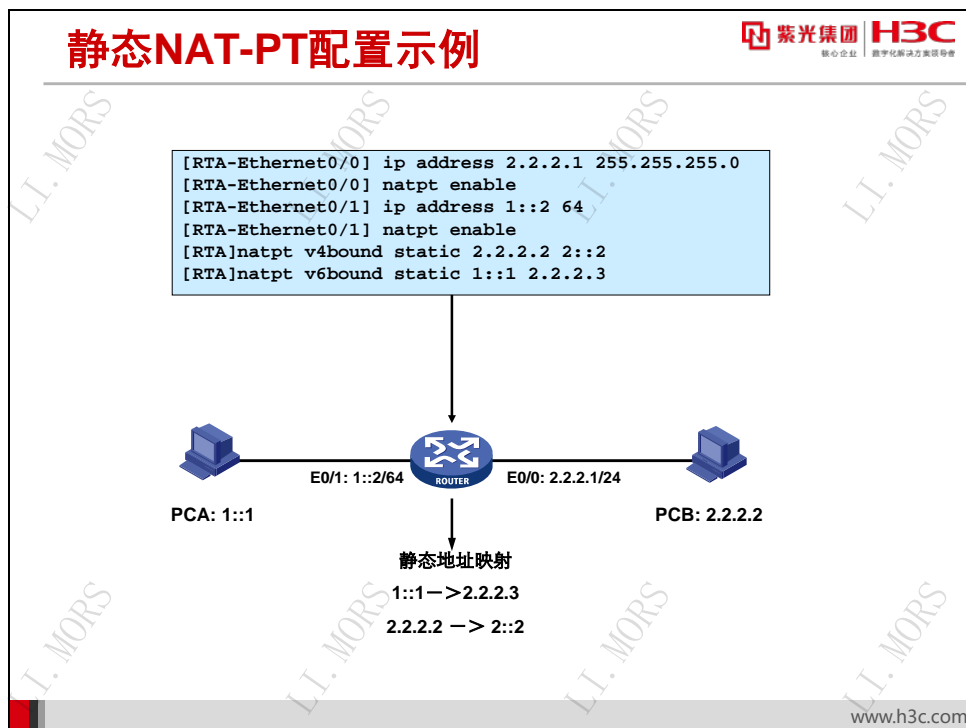
配置 IPv4 侧报文的动态映射后，对于从 IPv4 侧到 IPv6 侧的报文，如果 IPv4 源地址符合指定的 ACL 规则，则会在源 IPv4 地址前面添加 NAT-PT 前缀，转换为 IPv6 地址。

第4步：在系统视图下配置 IPv6 侧报文的动态映射。

```
natpt v6bound dynamic prefix natpt-prefix address-group address-group  
[ no-pat ]
```

配置 IPv6 侧报文的动态映射后，对于从 IPv6 侧到 IPv4 侧的报文，如果目的地址 IPv6 地址符合 NAT-PT 前缀，则源 IPv6 地址会转换为指定 NAT-PT 地址池中的 IPv4 地址。

如果配置了 no-pat 参数，则 NAT-PT 不进行端口转换，即不是 NAPT-PT 方式。



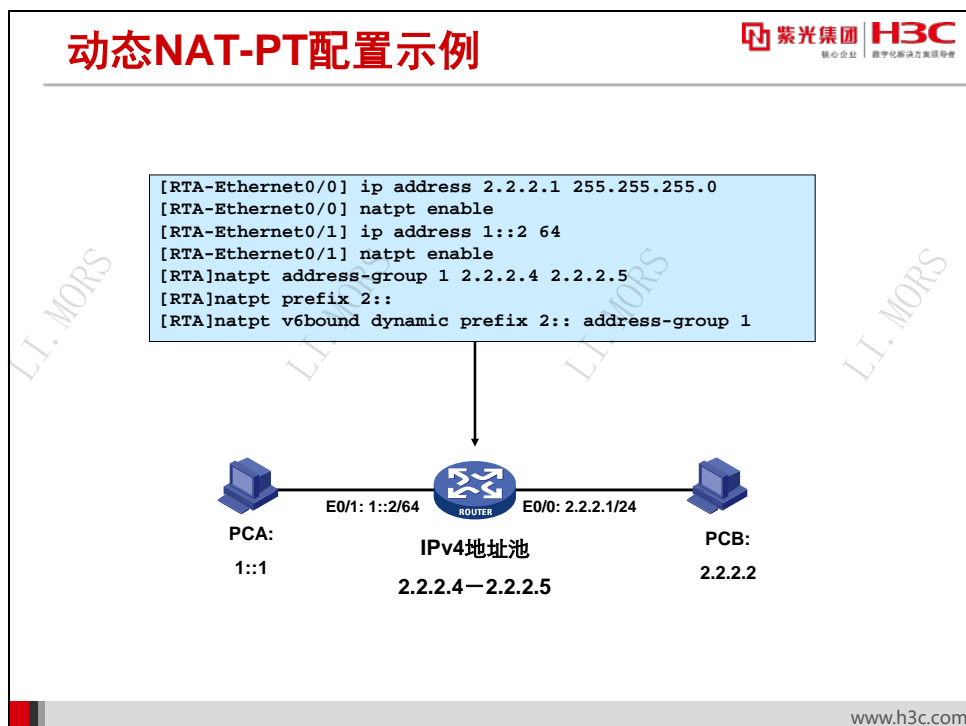
在上图所示网络中，IPv4 网络与 IPv6 网络通过 NAT-PT 设备 RTA 相连。在 RTA 上配置 IPv4 侧报文静态映射和 IPv6 侧报文静态映射，使 IPv4 网络和 IPv6 网络之间可以互相访问。

RTA 的配置：

```

[RTA-Ethernet0/0] ip address 2.2.2.1 255.255.255.0
[RTA-Ethernet0/0] natpt enable
[RTA-Ethernet0/1] ip address 1::2 64
[RTA-Ethernet0/1] natpt enable
[RTA]natpt v4bound static 2.2.2.2 2::2
[RTA]natpt v6bound static 1::1 2.2.2.3
  
```

配置完成后，如果 PCA 想访问 PCB，它需要发出目的地址为 2::2 的 IPv6 报文。报文经过 NAT-PT 转换后，变成源地址为 2.2.2.3，目的地址为 2.2.2.2 的 IPv4 报文。PCB 返回的报文也经过类似转换。



在上图所示网络中，IPv4 网络与 IPv6 网络通过 NAT-PT 设备 RTA 相连。在 RTA 上配置 IPv6 侧报文动态映射，使 IPv6 网络中的主机可以主动访问 IPv4 网络中的主机，而 IPv4 网络中的主机不能主动访问 IPv6 网络中的主机。

RTA 的配置：

```

[RTA-Ethernet0/0] ip address 2.2.2.1 255.255.255.0
[RTA-Ethernet0/0] natpt enable
[RTA-Ethernet0/1] ip address 1::2 64
[RTA-Ethernet0/1] natpt enable
[RTA]natpt address-group 1 2.2.2.4 2.2.2.5
[RTA]natpt prefix 2::
[RTA]natpt v6bound dynamic prefix 2:: address-group 1
    
```

配置完成后，如果 PCA 想访问 PCB，它需要发出目的地址为 2::2.2.2.2 的 IPv6 报文。报文经过 NAT-PT 转换后，变成源地址为 2.2.2.4，目的地址为 2.2.2.2 的 IPv4 报文；同时在 RTA 的 NAT-PT 会话表中建立 2.2.2.4—>1::1，2.2.2.2—>2::2.2.2.2 的动态映射表项。当 PCB 返回报文时，RTA 根据已建立的表项，经过相应的转换后发到 PCA。

NAT-PT显示与维护



- 显示所有NAT-PT配置信息

```
[Router] display natpt all
```

- 显示NAT-PT地址池配置信息

```
[Router] display natpt address-group
```

- 显示NAT-PT的静态和动态映射信息

```
[Router] display natpt address-mapping
```

- 显示NAT-PT动态会话信息

```
[Router] display natpt session { all | icmp | tcp |  
udp }
```

www.h3c.com

在系统视图下用 `display natpt all` 命令可以显示所有 NAT-PT 配置信息，包括 NAT-PT 地址池、静态和动态映射信息，所建立的 NAT-PT 会话等。

`display natpt address-group` 命令用来显示 NAT-PT 地址池配置信息。其输出如下所示：

```
<Router> display natpt address-group  
NATPT IPv4 Address Pool Information:  
1: from 1.1.1.1 to 1.1.1.4
```

以上输出表明，地址池编号为 1，池内地址是从 1.1.1.1 到 1.1.1.4。

`display natpt address-mapping` 命令用来显示 NAT-PT 的静态和动态映射信息。其输出如下所示：

```
<Sysname> display natpt address-mapping  
NATPT address mapping(v6bound view):  
IPv4 Address      IPv6 Address      Type  
1.1.1.1           3001::0001        SOURCE  
2.2.2.2           3001::0002        DESTINATION  
  
NATPT V6Server static mapping:  
IPv4Address      IPv6 Address      Pro  
1.1.1.1^ 6       3001::0003^ 1270  TCP
```

以上输出的重要参数说明见下表。

表24-1 display natpt address-mapping 命令显示信息描述表

字段	描述
NATPT address mapping(v6bound view)	显示IPv6侧NAT-PT的静态和动态映射信息

字段	描述
Type	IPv6侧是作为发起连接方（这时IPv6地址是源地址（SOURCE））还是IPv4侧作为发起连接方（这时IPv6地址作为目的地址（DESTINATION）），在本例中是3001::0001是源地址，2.2.2.2是目的地址。
NATPT V6Server static mapping:	显示NAT-PT的地址加端口的映射关系
IPv4Address	IPv4地址及端口号
IPv6 Address	对应的IPv6地址及端口号
Pro	协议类型

display natpt session 命令用来显示 NAT-PT 动态会话信息。其输出如下所示：

```
[RouterB] display natpt session all
```

```
NATPT Session Info:
```

No	IPv6Source	IPv4Source	Pro
	IPv6Destination	IPv4Destination	
1	2001::0002^20140	8.0.0.19^12290	ICMP
	3001::0800:0002^ 0	8.0.0.2^ 0	

由以上输出可知，目前设备上存在一条 NAT-PT 动态会话。会话的 IPv6 源地址为 2001::0002，端口号为 20140，IPv6 目的地址为 3001::0800:0002，端口号为 0；会话的 IPv4 源地址为 8.0.0.19，端口号为 12290，IPv4 目的地址为 8.0.0.2，端口号为 0。此条会话是 ICMP 协议类型。

24.5 本章总结

本章总结

- IPv6过渡技术包括双栈、隧道和NAPT-PT
- 6to4隧道和ISATAP隧道是自动隧道技术
- 6to4隧道和ISATAP隧道的配置与维护
- NAT-PT结合了地址转换和协议转换
- NAT-PT分为静态、动态和NAPT-PT
- NAT-PT的配置与维护

24.6 习题和解答

24.6.1 习题

1. 以下哪些描述是双协议栈技术的特点？（ ）
 - A. 既能与支持 IPv4 协议的节点通信，又能与支持 IPv6 协议的节点通信
 - B. 节点需要维护两个协议栈
 - C. 解决了 IPv4 地址紧缺问题
 - D. 将 IPv6 报文封装在 IPv4 报文中穿越 IPv4 网络
2. 6to4 自动隧道地址格式是（ ）
 - A. 2001:a.b.c.d:xxxx:xxxx:xxxx:xxxx:xxxx
 - B. 2001::0:5EFE:w.x.y.z
 - C. 2002:a.b.c.d:xxxx:xxxx:xxxx:xxxx:xxxx
 - D. 2002::0:5EFE:w.x.y.z
3. 以下哪些是 ISATAP 隧道的优点？（ ）
 - A. 隧道终点不需要手工配置
 - B. 无须使用特定格式的地址
 - C. 可将 IPv4 报文转换成 IPv6 报文
 - D. 隧道两端设备之间可以运行 ND 协议从而实现地址自动配置
4. 配置将 IPv4 报文的源地址 2.2.2.2 转换到 IPv6 报文的源地址 2::2 的命令是（ ）
 - A. [RTA]natpt v4bound static 2.2.2.2 2::2
 - B. [RTA]natpt v6bound static 2::2 2.2.2.2
 - C. [RTA-Ethernet0/0]natpt v4bound static 2.2.2.2 2::2
 - D. [RTA-Ethernet0/0]natpt v6bound static 2::2 2.2.2.2
5. 下列哪些命令用来查看 NAT-PT 的静态映射信息？（ ）
 - A. display natpt all
 - B. display natpt address-group
 - C. display natpt address-mapping
 - D. display natpt session

24.6.2 习题答案

1. AB

2. C

3. AD

4. A

5. AC