

目 录

IPv6 基础	1
IPv6 协议特点.....	1
IPv6 地址介绍.....	2
IPv6 邻居发现协议介绍	5
IPv6 PMTU发现	8
IPv6 DNS简介	9

IPv6 基础

IPv6 (Internet Protocol Version 6, 因特网协议版本 6) 是网络层协议的第二代标准协议, 也被称为 IPng (IP Next Generation, 下一代因特网), 它是 IETF (Internet Engineering Task Force, Internet 工程任务组) 设计的一套规范, 是 IPv4 的升级版。IPv6 和 IPv4 之间最显著的区别为: IP 地址的长度从 32 比特增加到 128 比特。

IPv6 协议特点

1. 简化的报文头格式

通过将 IPv4 报文头中的某些字段裁减或移入到扩展报文头, 减小了 IPv6 基本报文头的长度。IPv6 使用固定长度的基本报文头, 从而简化了转发设备对 IPv6 报文的处理, 提高了转发效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍, 但 IPv6 基本报文头的长度只有 40 字节, 为 IPv4 报文头长度 (不包括选项字段) 的两倍。

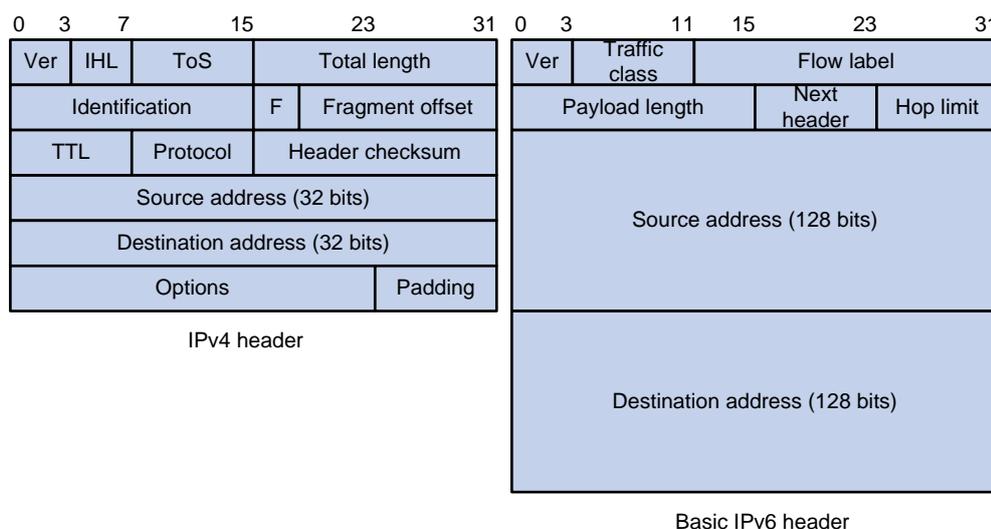


图1 IPv4 报文头和 IPv6 基本报文头格式比较

2. 充足的地址空间

IPv6 的源地址与目的地址长度都是 128 比特 (16 字节)。它可以提供超过 3.4×10^{38} 种可能的地址空间, 完全可以满足多层次的地址划分需要, 以及公有网络和机构内部私有网络的地址分配。

3. 层次化的地址结构

IPv6 的地址空间采用了层次化的地址结构, 有利于路由快速查找, 同时可以借助路由聚合, 有效减少 IPv6 路由表占用的系统资源。

4. 地址自动配置

为了简化主机配置，IPv6 支持有状态地址配置和无状态地址配置：

- 有状态地址配置是指从服务器（如 DHCP 服务器）获取 IPv6 地址及相关信息；
- 无状态地址配置是指主机根据自己的链路层地址及路由器发布的前缀信息自动配置 IPv6 地址及相关信息。

同时，主机也可根据自己的链路层地址及默认前缀（FE80::/10）形成链路本地地址，实现与本链路上其他主机的通信。

5. 内置安全性

IPv6 将 IPsec 作为它的标准扩展头，可以提供端到端的安全特性。这一特性也为解决网络安全问题提供了标准，并提高了不同 IPv6 应用之间的互操作性。

6. 支持 QoS

IPv6 报文头的流标签（Flow Label）字段实现流量的标识，允许设备对某一流中的报文进行识别并提供特殊处理。

7. 增强的邻居发现机制

IPv6 的邻居发现协议是通过一组 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 的因特网控制报文协议）消息实现的，管理着邻居节点间（即同一链路上的节点）信息的交互。它代替了 ARP（Address Resolution Protocol，地址解析协议）、ICMPv4 路由器发现和 ICMPv4 重定向消息，并提供了一系列其他功能。

8. 灵活的扩展报文头

IPv6 取消了 IPv4 报文头中的选项字段，并引入了多种扩展报文头，在提高处理效率的同时还大大增强了 IPv6 的灵活性，为 IP 协议提供了良好的扩展能力。IPv4 报文头中的选项字段最多只有 40 字节，而 IPv6 扩展报文头的大小只受到 IPv6 报文大小的限制。

IPv6 地址介绍

1. IPv6 地址表示方式

IPv6 地址被表示为以冒号（:）分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，每组的 16 比特用 4 个十六进制数来表示，组和组之间用冒号隔开，比如：2001:0000:130F:0000:0000:09C0:876A:130B。

为了简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0”可以省略，即上述地址可写为 2001:0:130F:0:0:9C0:876A:130B。

- 如果地址中包含连续两个或多个均为 0 的组，则可以用双冒号 “::” 来代替，即上述地址可写为 2001:0:130F::9C0:876A:130B。



注意：

在一个 IPv6 地址中只能使用一次双冒号 “::”，否则当设备将 “::” 转变为 0 以恢复 128 位地址时，将无法确定 “::” 所代表的 0 的个数。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号码字段部分，接口标识相当于 IPv4 地址中的主机号码部分。

地址前缀的表示方式为：IPv6 地址/前缀长度。其中，IPv6 地址是前面所列出的任一形式，而前缀长度是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。

2. IPv6 的地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。



说明：

IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如表 1 所示。

表1 地址类型与格式前缀的对应关系

地址类型		格式前缀（二进制）	IPv6 前缀标识
单播地址	未指定地址	00...0 (128 bits)	::/128
	环回地址	00...1 (128 bits)	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址	其他形式	-
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

3. 单播地址的类型

IPv6 单播地址的类型可有多种，包括全球单播地址、链路本地地址和站点本地地址等。

- 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量。
- 链路本地地址用于邻居发现协议和无状态自动配置中链路本地节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。
- 站点本地地址与 IPv4 中的私有地址类似。使用站点本地地址作为源或目的地址的数据报文不会被转发到本站点（相当于一个私有网络）外的其它站点。
- 环回地址：单播地址 0:0:0:0:0:0:0:1（简化表示为::1）称为环回地址，不能分配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自己发送 IPv6 报文。
- 未指定地址：地址“::”称为未指定地址，不能分配给任何节点。在节点获得有效的 IPv6 地址之前，可在发送的 IPv6 报文的源地址字段填入该地址，但不能作为 IPv6 报文中的目的地址。

4. 组播地址

表 2 所示的组播地址，是预留的特殊用途的组播地址。

表2 预留的 IPv6 组播地址列表

地址	应用
FF01::1	节点本地范围所有节点组播地址
FF02::1	链路本地范围所有节点组播地址

地址	应用
FF01::2	节点本地范围所有路由器组播地址
FF02::2	链路本地范围所有路由器组播地址
FF05::2	站点本地范围所有路由器组播地址

另外，还有一类组播地址：被请求节点（**Solicited-Node**）地址。该地址主要用于获取同一链路上邻居节点的链路层地址及实现重复地址检测。每一个单播或任播 IPv6 地址都有一个对应的被请求节点地址。其格式为：

FF02:0:0:0:1:FFXX:XXXX

其中，**FF02:0:0:0:1:FF** 为 104 位固定格式；**XX:XXXX** 为单播或任播 IPv6 地址的后 24 位。

5. IEEE EUI-64 格式的接口标识符

IPv6 单播地址中的接口标识符用来标识链路上的一个唯一的接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。IEEE EUI-64 格式的接口标识符是从接口的链路层地址（MAC 地址）变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 **FFFE**（1111111111111110）。为了确保这个从 MAC 地址得到的接口标识符是唯一的，还要将 **Universal/Local (U/L)** 位（从高位开始的第 7 位）设置为“1”。最后得到的这组数就作为 **EUI-64** 格式的接口标识符。

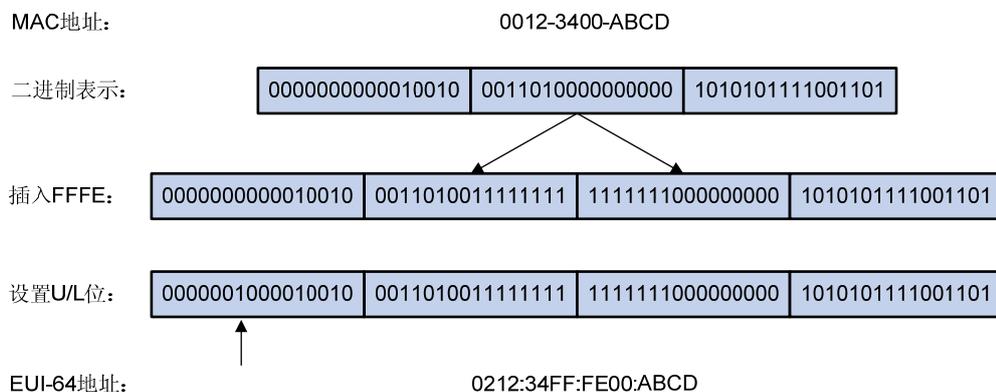


图2 MAC 地址到 EUI-64 格式接口标识符的转换过程

IPv6 邻居发现协议介绍

IPv6 邻居发现协议使用五种类型的 **ICMPv6** 消息，实现下面一些功能：地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向等功能。

邻居发现协议使用的 **ICMPv6** 消息的类型及作用如表 3 所示。

表3 邻居发现协议使用的 ICMPv6 消息类型及作用

ICMPv6 消息	类型号	作用
邻居请求消息 NS (Neighbor Solicitation)	135	获取邻居的链路层地址
		验证邻居是否可达
		进行重复地址检测
邻居通告消息 NA (Neighbor Advertisement)	136	对 NS 消息进行响应
		节点在链路层变化时主动发送 NA 消息，向邻居节点通告本节点的变化信息
路由器请求消息 RS (Router Solicitation)	133	节点启动后，通过 RS 消息向路由器发出请求，请求前缀和其他配置信息，用于节点的自动配置
路由器通告消息 RA (Router Advertisement)	134	对 RS 消息进行响应
		在没有抑制 RA 消息发布的条件下，路由器会周期性地发布 RA 消息，其中包括前缀信息选项和一些标志位的信息
重定向消息 (Redirect)	137	当满足一定的条件时，缺省网关通过向源主机发送重定向消息，使主机重新选择正确的下一跳地址进行后续报文的发送

邻居发现协议提供的主要功能如下：

1. 地址解析

获取同一链路上邻居节点的链路层地址（与IPv4的ARP功能相同），通过邻居请求消息NS和邻居通告消息NA实现。如图3所示，节点A要获取节点B的链路层地址。

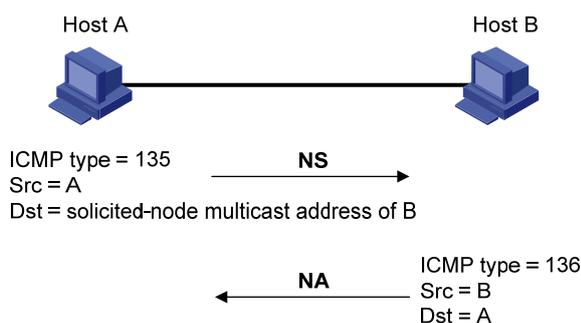


图3 地址解析示意图

- (1) 节点 A 以组播方式发送 NS 消息。NS 消息的源地址是节点 A 的接口 IPv6 地址，目的地址是节点 B 的被请求节点组播地址，消息内容中包含了节点 A 的链路层地址。

- (2) 节点 B 收到 NS 消息后，判断报文的地址是否为自己的 IPv6 地址对应的被请求节点组播地址。如果是，则节点 B 可以学习到节点 A 的链路层地址，并以单播方式返回 NA 消息，其中包含了自己的链路层地址。
- (3) 节点 A 从收到的 NA 消息中就可获取到节点 B 的链路层地址。

2. 验证邻居是否可达

在获取到邻居节点的链路层地址后，通过邻居请求消息 NS 和邻居通告消息 NA 可以验证邻居节点是否可达。

- (1) 节点发送 NS 消息，其中目的地址是邻居节点的 IPv6 地址。
- (2) 如果收到邻居节点的确认报文，则认为邻居可达；否则，认为邻居不可达。

3. 重复地址检测

当节点获取到一个 IPv6 地址后，需要使用重复地址检测功能确定该地址是否已被其他节点使用（与 IPv4 的免费 ARP 功能相似）。通过 NS 和 NA 可以实现重复地址检测，如图 4 所示。

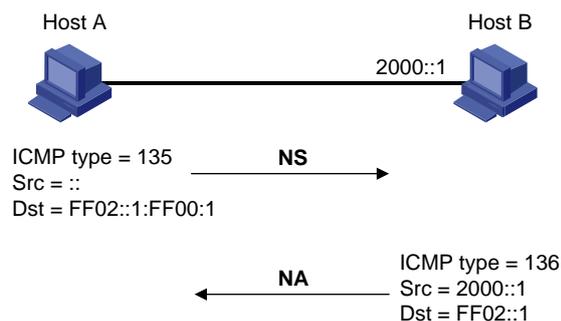


图4 重复地址检测示意图

- (1) 节点 A 发送 NS 消息，NS 消息的源地址是未指定地址::，目的地址是待检测的 IPv6 地址对应的被请求节点组播地址，消息内容中包含了待检测的 IPv6 地址。
- (2) 如果节点 B 已经使用这个 IPv6 地址，则会返回 NA 消息。其中包含了自己的 IPv6 地址。
- (3) 节点 A 收到节点 B 发来的 NA 消息，就知道该 IPv6 地址已被使用。反之，则说明该地址未被使用，节点 A 就可使用此 IPv6 地址。

4. 路由器发现/前缀发现及地址自动配置

路由器发现/前缀发现是指节点从收到的 RA 消息中获取邻居路由器及所在网络的前缀，以及其他配置参数。

地址无状态自动配置是指节点根据路由器发现/前缀发现所获取的信息，自动配置 IPv6 地址。

路由器发现/前缀发现通过路由器请求消息 **RS** 和路由器通告消息 **RA** 来实现，具体过程如下：

- (1) 节点启动时，通过 **RS** 消息向路由器发出请求，请求前缀和其他配置信息，以便用于节点的配置。
- (2) 路由器返回 **RA** 消息，其中包括前缀信息选项（路由器也会周期性地发布 **RA** 消息）。
- (3) 节点利用路由器返回的 **RA** 消息中的地址前缀及其他配置参数，自动配置接口的 **IPv6** 地址及其他信息。

 说明：

- 前缀信息选项中不仅包括地址前缀的信息，还包括该地址前缀的首选生命期（**preferred lifetime**）和有效生命期（**valid lifetime**）。节点收到周期性发送的 **RA** 消息后，会根据该消息更新前缀的首选生命期和有效生命期。
- 在有效生命期内，自动生成的地址可以正常使用；有效生命期过期后，自动生成的地址将被删除。

5. 重定向功能

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。当满足一定的条件时，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（与 **IPv4** 的 **ICMP** 重定向消息的功能相同）。

设备在满足下列条件时会发送对主机重定向的 **ICMPv6** 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 **ICMPv6** 重定向报文创建或修改过；
- 被选择的路由不是缺省路由；
- 被转发的 **IPv6** 数据报文中不包含路由扩展头。

IPv6 PMTU 发现

报文从源端到目的端的传输路径中所经过的链路可能具有不同的 **MTU**。在 **IPv6** 中，当报文的长度大于链路的 **MTU** 时，报文的分片将在源端进行，从而减轻中间转发设备的处理压力，合理利用网络资源。

PMTU（**Path MTU**，路径**MTU**）发现机制的目的就是要找到从源端到目的端的路径上最小的**MTU**。**PMTU**的工作过程如图 5所示。

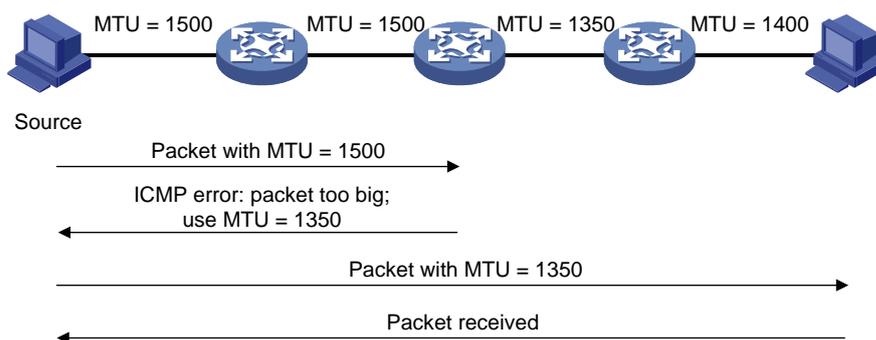


图5 PMTU 发现工作过程

- (1) 源端主机使用自己的 MTU 对报文进行分片，之后向目的主机发送报文。
- (2) 中间转发设备接收到该报文进行转发时，如果发现转发报文的接口支持的 MTU 值小于报文长度，则会丢弃报文，并给源端返回一个 ICMPv6 差错报文，其中包含了转发失败的接口的 MTU。
- (3) 源主机收到该差错报文后，将使用报文中所携带的 MTU 重新对报文进行分片并发送。
- (4) 如此反复，直到目的端主机收到这个报文，从而确定报文从源端到目的端路径中的最小 MTU。

IPv6 DNS 简介

在 IPv6 网络中，通过支持 IPv6 的 DNS（Domain Name System，域名系统）实现域名与 IPv6 地址的转换。IPv6 DNS 与 IPv4 DNS 的区别只是将域名转换为 IPv6 地址，而非 IPv4 地址。

IPv6 DNS 与 IPv4 DNS 相同，也分为静态域名解析和动态域名解析。两种域名解析的作用和实现方式也与 IPv4 DNS 一样。具体描述请参见“IP 业务分册”中的“域名解析配置”。

通常，连接 IPv4 和 IPv6 网络的 DNS 服务器中既包含 A 记录（IPv4 地址）也包含 AAAA 记录（IPv6 地址），可以进行域名与 IPv4 地址的转换，也可以进行域名与 IPv6 地址的转换。此时，DNS 服务器兼具 IPv6 DNS 和 IPv4 DNS 的功能。