

# IPv6

## 为什么要有IPv6?

**IPv4地址空间有限：**IPv4使用32位地址，最多可提供约43亿个地址。随着互联网设备数量的爆炸式增长，这些地址已经几乎耗尽。

**IPv6地址空间庞大：**IPv6使用128位地址，可以提供大约 $3.4 \times 10^{38}$ 个地址，理论上可以为地球上的每一粒沙子分配一个地址。

## IPv6 特点

### 1. 地址空间扩展

IPv4使用32位地址，最多能提供约43亿个唯一的IP地址。随着互联网设备的爆炸性增长（如智能手机、物联网设备等），IPv4地址已经耗尽。而IPv6使用128位地址，能够提供约340万亿亿亿亿（ $3.4 \times 10^{38}$ ）个唯一地址，足以满足未来的需求。

### 2. 简化的网络配置

IPv6支持无状态地址自动配置（Stateless Address Autoconfiguration, SLAAC），允许设备在没有DHCP服务器的情况下自动获得IP地址。这样，网络配置和管理变得更加简单和自动化。

### 3. 增强的安全性

IPv6在设计时就考虑了安全性，IPsec（用于加密和验证IP包的协议）在IPv6中是强制的，而在IPv4中是可选的。这为IPv6网络提供了更强的安全保证。

### 4. 更高效的路由

IPv6的地址分配是基于分层结构的，使得路由表的大小大大减少，提高了路由效率。此外，IPv6还支持更高效的多播路由。

### 5. 改进的移动性支持

IPv6改进了对移动设备的支持，例如移动IPv6（MIPv6），使得设备在不同网络之间移动时能够保持其连接不变。

### 6. 消除网络地址转换（NAT）

由于IPv4地址短缺，NAT被广泛用于共享一个公共IPv4地址。然而，NAT增加了网络复杂性和管理开销，并且破坏了端到端连接的互联网模型。IPv6提供了足够的地址空间，使得每个设备都可以拥有一个唯一的全球可路由地址，消除了对NAT的需求。

### 7. 简化的报头结构

IPv6的报头结构被简化，某些字段被删除或变为可选，提高了路由器处理包的效率。尽管IPv6地址比IPv4长，但简化的报头结构在某些情况下可以提高网络性能。

## 8. 更好的扩展性

IPv6为未来的协议扩展提供了更好的支持。通过扩展头的使用，IPv6能够更灵活地添加新功能和服务，而不影响现有的协议结构。

## IPv6地址

IPv6 地址是一种用于标识网络设备的 128 位地址，设计用于替代现有的 IPv4 地址系统。IPv6 地址由 8 组 4 个十六进制数字组成，每组之间用冒号 (:) 分隔。以下是一些关于 IPv6 地址的重要信息：

### IPv6 地址格式

典型的 IPv6 地址示例：

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

每个 IPv6 地址由 8 组 16 位组成，总共 128 位。

### 缩写规则

#### 1. 前导零压缩：

- 在每组中的前导零可以省略。例如，`0db8` 可以写成 `db8`。

原始地址：

```
2001:0db8:0000:0000:0000:ff00:0042:8329
```

可以缩写为：

```
2001:db8:0:0:0:ff00:42:8329
```

#### 2. 连续零压缩：

- 一段连续的零可以用双冒号 (::) 代替。这种压缩在一个地址中只能出现一次。

原始地址：

```
2001:0db8:0000:0000:0000:ff00:0042:8329
```

可以进一步缩写为：

```
2001:db8::ff00:42:8329
```

### IPv6 地址类型

## 一、单播地址 (Unicast Address)

用于标识单个网络接口。

### 1. 全局单播地址 (Global Unicast Address)

- 可在整个互联网范围内使用的唯一地址。
- 以 `2000::/3` 开头。
- 例如: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`

### 2. 链路本地地址 (Link-Local Address)

- 用于单个链路上的通信, 不会路由到互联网。
- 以 `fe80::/10` 开头。
- 自动配置, 用于邻居发现和路由器发现。
- 例如: `fe80::1a2b:3c4d:5e6f:7g8h`

### 3. 站点本地地址 (Site-Local Address)

- 类似于 IPv4 的私有地址, 范围为 `fec0::/10`。
- 这种地址类型在最新的规范中已被弃用, 推荐使用唯一本地地址 (ULA)。

### 4. 唯一本地地址 (Unique Local Address, ULA)

- 用于本地通信, 不会在全局互联网路由。
- 以 `fc00::/7` 开头 (通常是 `fd00::/8`)。
- 例如: `fd12:3456:789a:1::1`

## 二、多播地址 (Multicast Address)

- IPv6多播地址用于将数据包发送到一个特定的组, 而不是单个设备或所有设备。多播地址的范围可以是链路本地、站点本地、组织本地或全球。IPv6多播地址的前缀是 `ff00::/8`, 其中的每一位和字段都有特定的意义。

### IPv6多播地址格式

IPv6多播地址的格式如下:

```
| 11111111 | flgs | scop | group ID |  
+-----+-----+-----+  
| 8      | 4      | 4      | 112     |
```

### 字段详细说明

#### 1. 11111111 (8 bits)

- 固定前缀, 表示这是一个多播地址。

#### 2. flgs (4 bits)

- 标志位, 用于定义多播地址的属性。常见的值包括:
  - 0: 常规多播地址。
  - 1: 永久多播地址。
  - 其他值根据特定用途定义。

#### 3. scop (4 bits)

- 作用范围 (scope), 定义了多播地址的有效范围。常见的值包括:
  - 1: 接口本地 (Interface-local)
  - 2: 链路本地 (Link-local)
  - 5: 站点本地 (Site-local)
  - 8: 组织本地 (Organization-local)
  - E: 全球 (Global)

4. group ID (112 bits)

- 标识多播组的具体标识符。

常见的IPv6多播地址

- **ff02::1**
  - 所有节点的链路本地多播地址。发送到该地址的数据包将被链路本地范围内的所有设备接收。
- **ff02::2**
  - 所有路由器的链路本地多播地址。发送到该地址的数据包将被链路本地范围内的所有路由器接收。（RS 中的目的地址）
- **ff05::2**
  - 所有路由器的站点本地多播地址。发送到该地址的数据包将被站点本地范围内的所有路由器接收。
- **ff02::1:ffXX**
  - Solicited-node多播地址。用于邻居发现协议（NDP）中的地址解析过程。（NS 中的目的地址）

三、任播地址（Anycast Address）

用于标识一组接口，但数据包只传送到距离最近的一个接口。

- 没有特定的前缀，可以从单播地址中分配。
- 常用于负载均衡和服务冗余。

四、特殊的 IPv6 地址

1. 未指定地址（Unspecified Address）

- 表示没有指定的地址。
- 用 :: 表示，相当于所有 128 位都是零。

2. 环回地址（Loopback Address）

- 用于设备自身通信。
- 用 ::1 表示。

五、IPv6 地址范围和前缀总结

地址类型	前缀	示例
全局单播	2000::/3	2001:0db8:85a3::8a2e:0370:7334
链路本地	fe80::/10	fe80::1a2b:3c4d:5e6f:7g8h
唯一本地	fc00::/7	fd12:3456:789a:1::1
多播地址	ff00::/8	ff02::1
未指定地址	::/128	::
环回地址	::1/128	::1

这种分层和详细的分类方式可以帮助更好地理解记忆IPv6地址类型及其用途。

# IPv6 地址分配

IPv6 地址的分配由 IANA (Internet Assigned Numbers Authority) 和各个区域性互联网注册机构 (RIRs) 负责。IANA 分配给 RIRs 大块的地址空间，然后由 RIRs 进一步分配给 ISP 和最终用户。

## IPv6 实现

---

### ICMPv6

**互联网控制消息协议第六版，Internet Control Message Protocol Version 6；**

在 [RFC 4443](#) 中被定义；

用于报告IPv6节点数据包处理过程中的错误消息和完成一些网络诊断功能（如[ping](#)和[traceroute](#)等）

除了ICMPv4原有的功能，ICMPv6还承担了IPv4其他协议所实现的功能或IPv6所需的新功能，例如[邻居发现协议](#)（同时取代了[ARP/RARP](#)，[SEND](#)作为其安全扩展）、**多播管理（取代了IGMP）**。

### ICMPv6的功能

ICMPv6提供以下主要功能：

1. **错误报告**：当路由器或主机在处理IPv6数据包时遇到问题时，ICMPv6会发送错误消息。
2. **信息查询**：用于主机和路由器之间的信息交换，如邻居发现（Neighbor Discovery）和路由器通告（Router Advertisement）。
3. **组播监听**：管理组播组成员资格。

### ICMPv6消息类型

ICMPv6消息分为两类：错误消息和信息消息。

#### 错误消息

##### 1. 目的不可达 (Destination Unreachable)

- 类型：1
- 用于通知发送方目标地址不可达。
- 子类型包括：没有路由到目标地址、通信管理被禁止、地址不可达、端口不可达等。

##### 2. 分片超出 (Packet Too Big)

- 类型：2
- 当数据包大小超过路径MTU（最大传输单元）时，通知发送方分片超出。

##### 3. 超时 (Time Exceeded)

- 类型：3
- 用于通知发送方数据包在传输过程中因跳数限制或传输时间过长而被丢弃。

##### 4. 参数问题 (Parameter Problem)

- 类型：4
- 用于通知发送方数据包中的某些参数有问题，如报头字段无效。

## 信息消息

### 1. 回显请求 (Echo Request) 和回显应答 (Echo Reply)

- 类型：128 (回显请求)，129 (回显应答)
- 用于诊断网络连接情况，类似于IPv4中的Ping。

### 2. 邻居发现协议 (Neighbor Discovery Protocol, NDP)

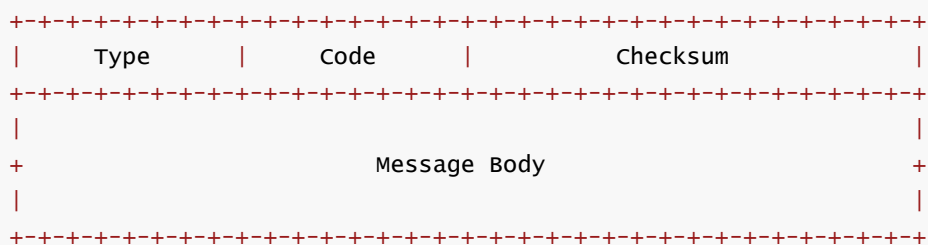
- 邻居请求 (Neighbor Solicitation)
  - 类型：135
  - 用于查询邻居节点的链路层地址。
- 邻居通告 (Neighbor Advertisement)
  - 类型：136
  - 用于响应邻居请求或通告地址变化。
- 路由器请求 (Router Solicitation)
  - 类型：133
  - 主机请求路由器发送路由器通告消息。
- 路由器通告 (Router Advertisement)
  - 类型：134
  - 路由器向本地链路上的所有节点通告其存在及配置信息。
- 重定向消息 (Redirect Message)
  - 类型：137
  - 路由器通知主机有更好的下一跳地址。

### 3. 组播监听 (Multicast Listener Discovery, MLD)

- 组播监听器查询 (Multicast Listener Query)
  - 类型：130
- 组播监听器报告 (Multicast Listener Report)
  - 类型：131
- 组播监听器终止 (Multicast Listener Done)
  - 类型：132

## ICMPv6消息格式

ICMPv6消息的基本格式如下：



**Type**：消息类型，指示消息的用途。

**Code**：消息子类型，进一步指示消息的具体含义。

**Checksum**：校验和，用于检测消息在传输过程中是否被损坏。

**Message Body**：消息的具体内容，根据消息类型和子类型不同而变化。

- **Type (类型)** : 133
  - 表示这是一个Router Solicitation消息。
- **Code (代码)** : 0
  - 必须设置为0。
- **Checksum (校验和)** : 16位
  - 用于检测报文在传输过程中是否被损坏。
- **Reserved (保留位)** : 32位
  - 保留用于将来使用, 应设置为0。
- **Options (选项)** : 可变长度
  - 包含源链路层地址等选项。每个选项有一个通用格式:

- **Type:** 选项类型。
- **Length:** 选项长度（以8字节为单位）。
- **Option Data:** 选项的具体数据。

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|           1           |           1           | 00:11:22:33:44:55           |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```



## RS 报文的工作流程

### 1. 主机发送RS报文

- 当主机启动或网络接口启用时，主机会发送RS报文到本地链路上的所有路由器。

### 2. 路由器接收RS报文

- 本地链路上的路由器接收到RS报文后，会发送RA报文，提供网络配置和路由信息。

### 3. 主机接收RA报文

- 主机接收RA报文后，根据RA报文中的信息进行网络配置，包括IPv6地址配置、默认路由器、MTU等。

## RA (Router Advertisement, 路由器通告)

### 报文格式

```
+++++Type+++++Code+++++Checksum+++++
|   Type   |   Code   |   Checksum   |
+++++Type+++++Code+++++Checksum+++++
| Cur Hop Limit | M|O|H|Prf|Resvd|   Router Lifetime   |
+++++Type+++++Code+++++Checksum+++++
|                                     Reachable Time                                     |
+++++Type+++++Code+++++Checksum+++++
|                                     Retrans Timer                                     |
+++++Type+++++Code+++++Checksum+++++
|   Options ...   |
+++++Type+++++Code+++++Checksum+++++
```

**Type (类型) :** 134

- 表示这是一个Router Advertisement消息。

**Code (代码) :** 0

- 必须设置为0。

**Checksum (校验和) :**

- 用于检测报文在传输过程中是否被损坏。值会根据报文内容计算。

**Cur Hop Limit (当前跳数限制) :** 64

- 建议主机在发送数据包时使用的默认跳数限制。默认值为64。

**M (管理地址配置标志) :** 0

- 如果设置为1，表示主机应使用DHCPv6获取地址。默认值为0（未使用DHCPv6获取地址）。

**O (其他配置标志) :** 0

- 如果设置为1，表示主机应使用DHCPv6获取其他配置信息。默认值为0（未使用DHCPv6获取其他信息）。

**H (家庭代理标志) :** 0

- 用于家庭代理配置（RFC 6275）。默认值为0（未使用）。

**Prf (路由器优先级) :** 00

- 路由器优先级。默认值为00（Medium）。

**Resvd（保留位）：**000000

- 保留用于将来使用，应设置为0。

**Router Lifetime（路由器寿命）：**1800

- 表示该路由器作为默认路由器的有效时间（以秒为单位）。默认值为1800秒（30分钟）。

**Reachable Time（可达时间）：**0

- 表示邻居保持可达状态的时间（以毫秒为单位）。默认值为0（使用默认值）。

**Retrans Timer（重传计时器）：**0

- 邻居请求消息的重传时间（以毫秒为单位）。默认值为0（使用默认值）。

**RA 报文示例**

```
> Frame 11111: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{459749E1-E347-4805-AC73-C4CA381402BD}, id 0
  Ethernet II, Src: 26:14:4c:0d:60:b9 (26:14:4c:0d:60:b9), Dst: IPv6mcast_01 (33:33:00:00:00:01)
    > Destination: IPv6mcast_01 (33:33:00:00:00:01)
    > Source: 26:14:4c:0d:60:b9 (26:14:4c:0d:60:b9)
      Address: 26:14:4c:0d:60:b9 (26:14:4c:0d:60:b9)
      ....01. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....00. .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
  > Internet Protocol Version 6, Src: fe80::2414:4cff:fe0d:60b9, Dst: ff02::1
    0110 .... = Version: 6
    > ....0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    ....1111 1010 1000 0000 0111 = Flow Label: 0xfa807
    Payload Length: 88
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::2414:4cff:fe0d:60b9
    Destination Address: ff02::1
  > Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xd0b3 [correct]
    [Checksum Status: Good]
    Cur hop limit: 254
    > Flags: 0x08, Prf (Default Router Preference): High
      Router lifetime (s): 3600
      Reachable time (ms): 0
      Retrans timer (ms): 0
    > ICMPv6 Option (Source link-layer address : 26:14:4c:0d:60:b9)
    > ICMPv6 Option (MTU : 1500)
    > ICMPv6 Option (Prefix information : 240e:46c:8600:63d::/64)
    > ICMPv6 Option (Recursive DNS Server 240e:46c:8600:63d::21)
```

**flag 示例**

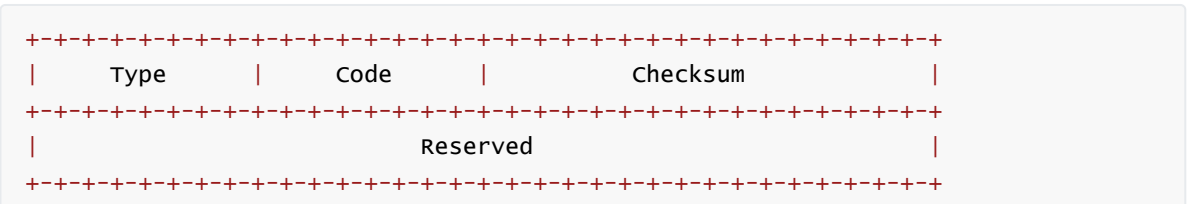
```
  > Flags: 0x08, Prf (Default Router Preference): High
    0... .... = Managed address configuration: Not set
    .0.. .... = Other configuration: Not set
    ..0. .... = Home Agent: Not set
    ...0 1... = Prf (Default Router Preference): High (1)
    .... .0.. = ND Proxy: Not set
    .... ..00 = Reserved: 0
    Router lifetime (s): 3600
```

**Neighbor Solicitation（NS，邻居请求）**

是IPv6中的一种ICMPv6消息，用于邻居发现协议（NDP）。NS报文用于解决IPv6地址到链路层地址的映射问题，类似于IPv4中的ARP请求。

**NS 报文格式**

NS报文的格式如下：





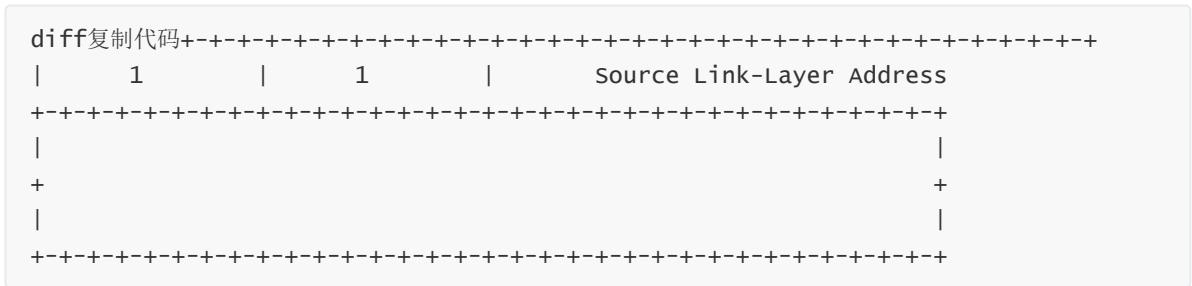
字段详细说明

- **Type (类型)** : 135
  - 表示这是一个Neighbor Solicitation消息。
- **Code (代码)** : 0
  - 必须设置为0。
- **Checksum (校验和)** : 16位
  - 用于检测报文在传输过程中是否被损坏。
- **Reserved (保留位)** : 32位
  - 保留用于将来使用，应设置为0。
- **Target Address (目标地址)** : 128位
  - 目标节点的IPv6地址。
- **Options (选项)** : 可变长度
  - 通常包含源链路层地址选项，用于提供发送NS报文的节点的链路层地址。

常见的NS报文选项

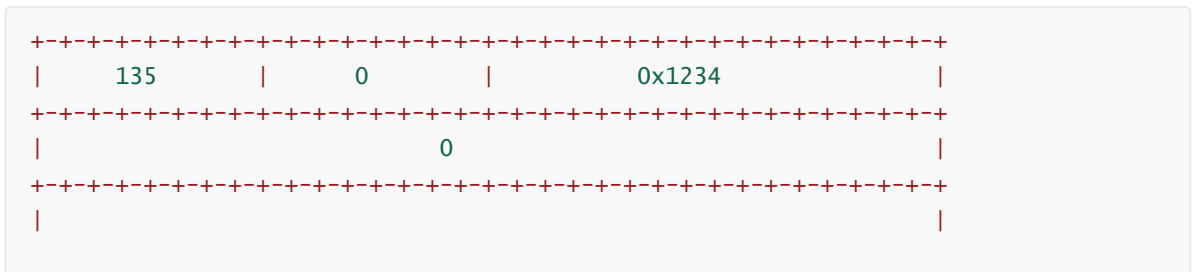
1. **源链路层地址 (Source Link-Layer Address)**
  - **Type**: 1
  - **Length**: 1 (8字节)
  - **Option Data**: 包含发送NS报文的节点的链路层地址 (MAC地址) 。

选项部分的示例



示例NS报文

假设有一个NS报文，其中包含了源链路层地址选项：





```

> Frame 5669: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{459749E1-E347-4805-AC73-C4CA381402B0}, id 0
< Ethernet II, Src: Intel_62:f9:30 (d4:e9:8a:62:f9:30), Dst: IPv6mcast_ff:0d:60:b9 (33:33:ff:0d:60:b9)
  > Destination: IPv6mcast_ff:0d:60:b9 (33:33:ff:0d:60:b9)
  > Source: Intel_62:f9:30 (d4:e9:8a:62:f9:30)
    Type: IPv6 (0x86dd)
< Internet Protocol Version 6, Src: fe80::d2f:345b:72ac:d847, Dst: ff02::1:ff0d:60b9
  0110 .... = Version: 6
  < .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 00.... = Differentiated Services Codepoint: Default (0)
  .... 0000 0000 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 32
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  Source Address: fe80::d2f:345b:72ac:d847
  Destination Address: ff02::1:ff0d:60b9
< Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x6700 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
  Target Address: fe80::2414:4cff:fe0d:60b9
< ICMPv6 Option (Source link-layer address : d4:e9:8a:62:f9:30)
  Type: Source link-layer address (1)
  Length: 1 (8 bytes)
  Link-layer address: Intel_62:f9:30 (d4:e9:8a:62:f9:30)

```

## NS 报文的工作流程

### 1. 发送NS报文

- 当一个节点需要解析另一个节点的链路层地址时，它会发送一个NS报文。NS报文的目标地址是要解析的IPv6地址，目的地址是目标地址的Solicited-Node多播地址。

### 2. 接收NS报文

- 目标节点接收到NS报文后，会检查报文中的目标地址是否匹配。如果匹配，目标节点会发送一个Neighbor Advertisement (NA) 报文作为响应。

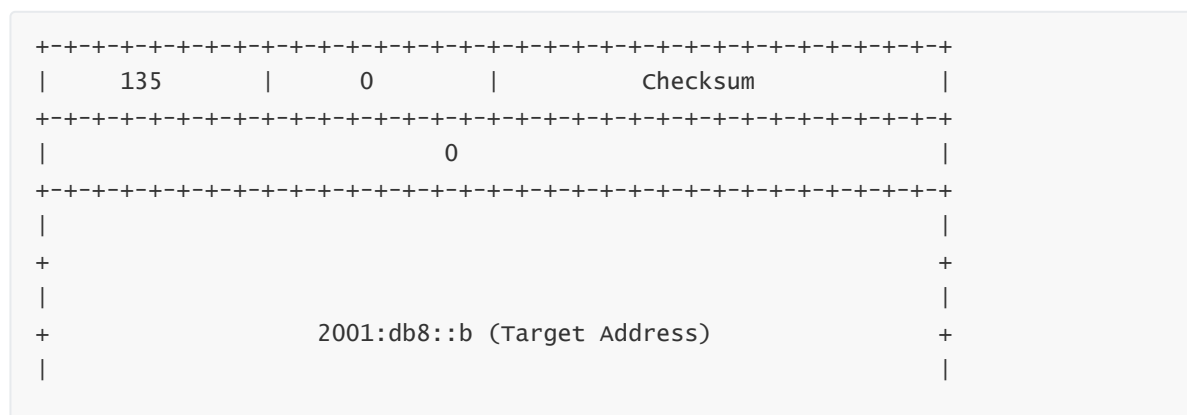
### 3. 发送NA报文

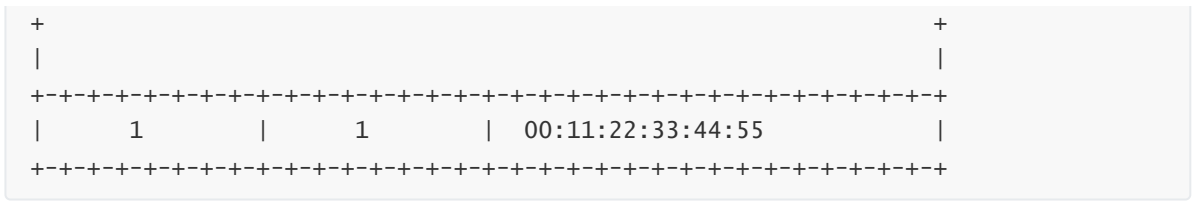
- 目标节点发送NA报文，其中包含目标节点的链路层地址信息。源节点接收到NA报文后，可以更新其邻居缓存表，将IPv6地址与链路层地址对应起来。

## NS 报文示例

假设有以下网络场景：节点A（IPv6地址为 2001:db8::a，链路层地址为 00:11:22:33:44:55）想要解析节点B（IPv6地址为 2001:db8::b）的链路层地址。

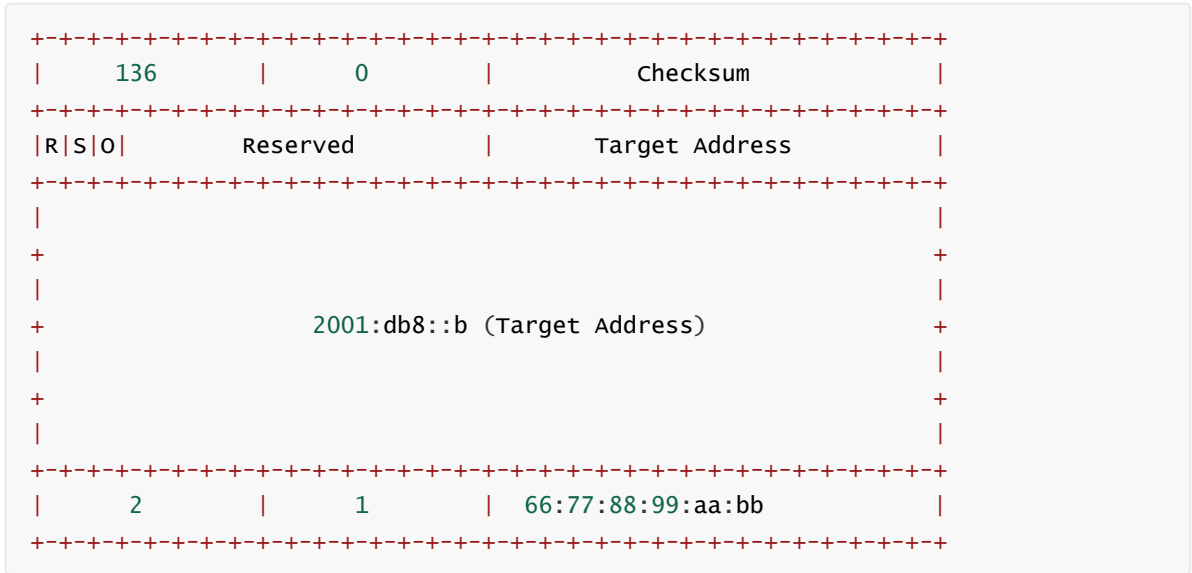
### 节点A发送NS报文





### 节点B接收并响应NA报文

假设节点B的链路层地址为 66:77:88:99:aa:bb，它会发送以下NA报文：



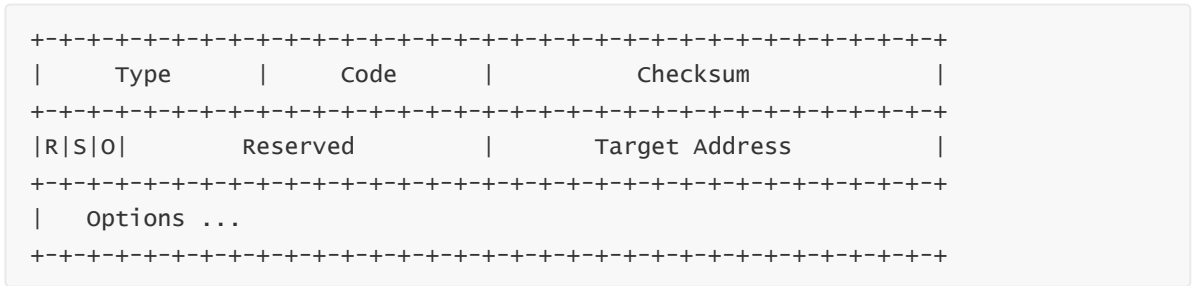
## Neighbor Advertisement (NA, 邻居通告)

报文是IPv6中的一种ICMPv6消息，用于邻居发现协议（NDP）。NA报文主要用于以下两种情况：

1. **响应Neighbor Solicitation (NS, 邻居请求) 报文**：当节点A发送NS报文请求节点B的链路层地址时，节点B通过NA报文回应。
2. **通告自身的链路层地址**：节点在网络上宣布自己的链路层地址（MAC地址），类似于**免费ARP**。

### NA 报文格式

NA报文的格式如下：



### 字段详细说明

- **Type (类型)** : 136
  - 表示这是一个Neighbor Advertisement消息。
- **Code (代码)** : 0
  - 必须设置为0。
- **Checksum (校验和)** : 16位
  - 用于检测报文在传输过程中是否被损坏。
- **R (Router)** : 1位

- 表示发送者是否是一个路由器。设置为1表示发送者是一个路由器。
- **S (Solicited) : 1位**
  - 表示这是对一个NS报文的回应。设置为1表示这是对NS报文的回应；设置为0表示这是一个主动通告消息。
- **O (Override) : 1位**
  - 表示是否覆盖邻居缓存中的现有条目。设置为1表示覆盖。
- **Reserved (保留位) : 29位**
  - 保留用于将来使用，应设置为0。
- **Target Address (目标地址) : 128位**
  - 目标节点的IPv6地址，这也是发送NA报文的节点的IPv6地址。
- **Options (选项) : 可变长度**
  - 通常包含源链路层地址等选项。每个选项有一个通用格式：

```
diff复制代码+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-++-+
|      Type      |      Length      |      Option Data ...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

- **Type:** 选项类型。
- **Length:** 选项长度（以8字节为单位）。
- **Option Data:** 选项的具体数据。

## 常见的NA报文选项

### 1. 源链路层地址 (Source Link-Layer Address)

- **Type: 1**
- **Length: 1** (8字节)
- **Option Data:** 包含发送NA报文的节点的链路层地址 (MAC地址)。

## 示例NA报文

假设节点A (IPv6地址为 2001:db8::a，链路层地址为 00:11:22:33:44:55) 要响应节点B (IPv6地址为 2001:db8::b) 的NS报文：

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      136      |      0      |      0x1234      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 1 | 0 |      0      |      2001:db8::a      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      1      |      1      |      00:11:22:33:44:55      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

```
> Frame 5691: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{459749E1-E347-4805-AC73-C4CA38140280}, id 0
▼ Ethernet II, Src: 26:14:4c:0d:60:b9 (26:14:4c:0d:60:b9), Dst: Intel_G2:f9:30 (d4:e9:8a:62:f9:30)
  > Destination: Intel_G2:f9:30 (d4:e9:8a:62:f9:30)
  > Source: 26:14:4c:0d:60:b9 (26:14:4c:0d:60:b9)
  Type: IPv6 (0x86dd)
▼ Internet Protocol Version 6, Src: fe80::2414:4c:ff:fe0d:60b9, Dst: fe80::d2f:345b:72ac:d847
  0110 .... = Version: 6
  ▼ .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
    .... ..00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 32
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  Source Address: fe80::2414:4c:ff:fe0d:60b9
  Destination Address: fe80::d2f:345b:72ac:d847
▼ Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0x9011 [correct]
  [Checksum Status: Good]
  ▼ Flags: 0x00000000, Router, Solicited, Override
    1... .... = Router: Set
    ..1. .... = Solicited: Set
    ...1. .... = Override: Set
    ...0 0000 0000 0000 0000 0000 0000 = Reserved: 0
  Target Address: fe80::2414:4c:ff:fe0d:60b9
  ▼ ICMPv6 Option (Target link-layer address : 26:14:4c:0d:60:b9)
    Type: Target link-layer address (2)
    Length: 1 (8 bytes)
    Link-layer address: 26:14:4c:0d:60:b9 (26:14:4c:0d:60:b9)

0000  d4 e9 8a 62 f9 30 26 14  4c 0d 60 b9 86 dd 60 00  ...b 0& L'...'
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 24 14  ...:.....$.
0020  4c ff fe 0d 60 b9 fe 80  00 00 00 00 00 0d 2f  L'...../
0030  34 5b 72 ac d8 47 88 00  9b 11 e0 00 00 fe 80  4[...G.....
0040  00 00 00 00 00 24 14  4c ff fe 0d 60 b9 02 01  ....$. L'.....
0050  26 14 4c 0d 60 b9  &L'..
```

解释

- **Type:** 136（表示这是一个NA报文）。
- **Code:** 0（代码字段为0）。
- **Checksum:** 0x1234（校验和）。
- **R:** 1（节点A是路由器）。
- **S:** 1（这是对NS报文的回应）。
- **O:** 0（不覆盖现有条目）。
- **Target Address:** 2001:db8::a（发送NA报文的节点的地址）。
- **Options:** 包含源链路层地址 00:11:22:33:44:55。

NA 报文的工作流程

1. 响应NS报文
  - 当一个节点（如节点B）接收到NS报文时，如果NS报文的目标地址与其自身的地址匹配，节点B会发送一个NA报文来响应请求。NA报文中包含目标地址（节点B的地址）及其链路层地址。
2. 主动通告
  - 节点也可以主动发送NA报文，通告自己的链路层地址，这在网络拓扑变化时非常有用，确保其他节点了解其链路层地址。
3. 更新邻居缓存
  - 接收到NA报文的节点会更新其邻居缓存，将IPv6地址和链路层地址的映射关系保存起来，以便后续通信使用。

NA 报文的作用

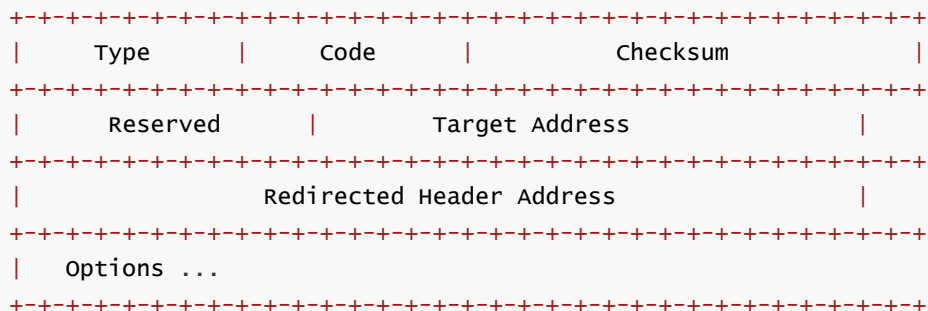
- **地址解析:** 通过NA报文，节点可以快速获取目标节点的链路层地址，实现IPv6地址到链路层地址的映射。
- **邻居可达性检测:** NA报文用于检测节点的可达性，确保网络通信的稳定性和可靠性。

重定向

**Redirect** 报文是IPv6中的一种ICMPv6消息，用于邻居发现协议（NDP）。它用于向源节点通知某个数据包的更优转发路径，通常是更接近目标的路由器。这在网络拓扑发生变化时非常有用，能够帮助主机更新其路由信息，从而优化数据包的传输路径。

## Redirect 报文格式

Redirect报文的格式如下：



### 字段详细说明

- **Type (类型)** : 137
  - 表示这是一个Redirect消息。
- **Code (代码)** : 0
  - 必须设置为0。
- **Checksum (校验和)** : 16位
  - 用于检测报文在传输过程中是否被损坏。
- **Reserved (保留位)** : 24位
  - 保留用于将来使用，应设置为0。
- **Target Address (目标地址)** : 128位
  - 数据包原本要发送到的目标IPv6地址。
- **Redirected Header Address (重定向报头地址)** : 128位
  - 指出重定向后的新路由器的IPv6地址，通常是当前路由器的地址，这个字段用于指出从源主机到目标地址的最佳路径。
- **Options (选项)** : 可变长度
  - 通常包含源链路层地址等选项，用于提供发送Redirect报文的路由器的链路层地址。

### 常见的Redirect报文选项

#### 1. 源链路层地址 (Source Link-Layer Address)

- **Type**: 1
- **Length**: 1 (8字节)
- **Option Data**: 包含发送Redirect报文的路由器的链路层地址 (MAC地址) 。

### 示例Redirect报文

假设节点A (IPv6地址为 2001:db8::a) 通过路由器R (IPv6地址为 2001:db8::r) 发送数据包到节点B (IPv6地址为 2001:db8::b)，但路由器R发现直接将数据包发送到节点B的路径更优，因此R发送了一个Redirect报文给节点A。假设R的链路层地址为 00:11:22:33:44:55，示例Redirect报文如下：



137	0	0x1234
0		
2001:db8::b (Target Address)		
2001:db8::r (Redirected Header Address)		
1	1	00:11:22:33:44:55

解释

- **Type:** 137（表示这是一个Redirect报文）。
- **Code:** 0（代码字段为0）。
- **Checksum:** 0x1234（校验和）。
- **Reserved:** 0（保留位）。
- **Target Address:** 2001:db8::b（原始目标地址）。
- **Redirected Header Address:** 2001:db8::r（重定向后的新路由器地址）。
- **Options:** 包含源链路层地址 00:11:22:33:44:55。

Redirect 报文的工作流程

1. 检测更优路径
  - 路由器在转发数据包时，如果发现有更直接的路径到达目标地址，它会生成Redirect报文。
2. 发送Redirect报文
  - 路由器将Redirect报文发送到原始数据包的源节点，告知源节点一个更优的路径。
3. 更新路由
  - 源节点接收到Redirect报文后，会更新其路由信息，直接将数据包发送到重定向的目标地址，而不是通过原始的路由器。
4. 优化数据传输
  - 更新后的路由信息有助于优化数据包的传输路径，提高网络性能和效率。

使用场景

- **网络拓扑变化:** 当网络拓扑发生变化时，路由器可以通过Redirect报文通知主机更新其路由信息。
- **路径优化:** 在某些情况下，数据包可以通过更短的路径到达目标地址，Redirect报文可以帮助源节点优化路径选择。