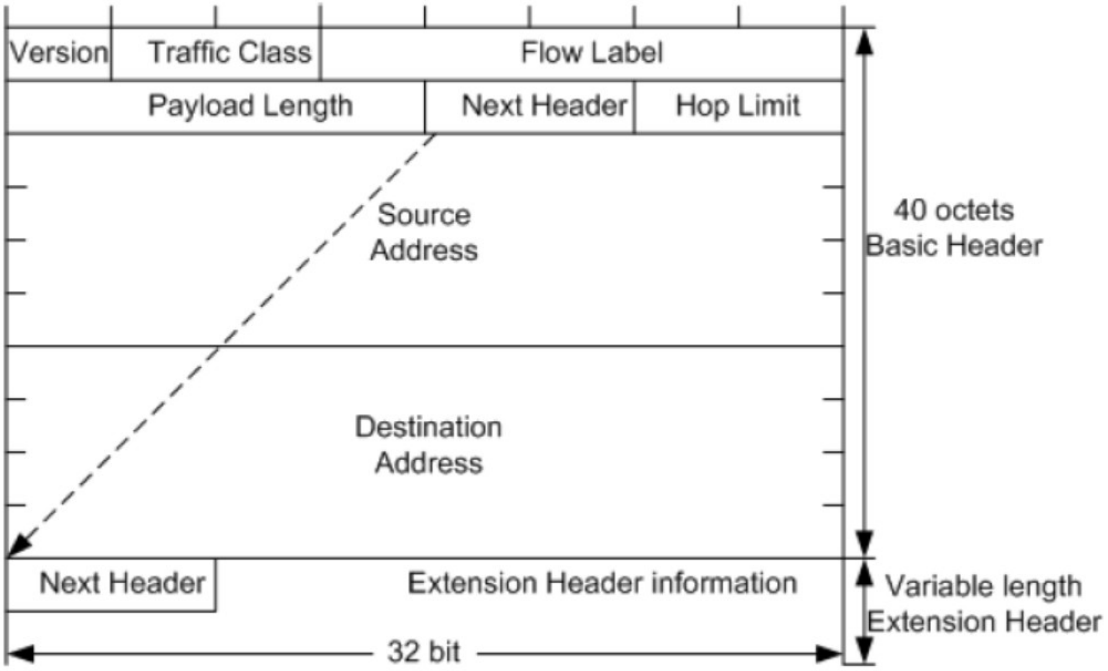
IPv6 报头

IPv6 报头有哪些字段？哪个是表示优先级的？
IPv6 基本报头有 8 个字段，固定大小为 40 字节，每一个 IPv6 数据报都必须报含报头。

```
Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff2a:15f7
   0110 .... = Version: 6
>  .... 1100 0000 .... .... .... .... .... = Traffic Class: 0xc0 (DSCP: CS6, ECN: Not-ECT)
   .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
   Payload Length: 24
   Next Header: ICMPv6 (58)
   Hop Limit: 255
   Source: ::
   Destination: ff02::1:ff2a:15f7
Internet Control Message Protocol v6
```



1 Version：版本号，长度为 4bit。对于 IPv6，该值为 6。
2 Traffic Class：流类别，长度为 8bit。等同于 IPv4 中的 TOS 字段，表示 IPv6 数据报的类或优先级，主要　应用于 QoS。

3 Flow Label：流标签，长度为 20bit。IPv6 中的新增字段，用于区分实时流量，不同的流标签+源地址　可以唯一确定一条数据流，中间网络设备可以根据这些信息更加高效率的区分数据流。
4 Payload Length：有效载荷长度，长度为 16bit。有效载荷是指紧跟 IPv6 报头的数据报的其它部分
（即扩展报头和上层协议数据单元）。
5 Next Header：下一个报头，长度为 8bit。该字段定义紧跟在 IPv6 报头后面的第一个扩展报头（如果存在）的类型，或者上层协议数据单元中的协议类型。
6 Hop Limit：跳数限制，长度为 8bit。该字段类似于 IPv4 中的 Time to Live 字段，它定义了 IP 数据报所能经过的最大跳数。
7 Source Address：源地址，长度为 128bit。表示发送方的地址。
8 Destination Address：目的地址，长度为 128bit。表示接收方的地址。
IPv6 和 IPv4 相比，去除了 IHL、identifiers、Flags、Fragment Offset、Header Checksum、 Options、Paddiing 域，只增了流标签域，因此 IPv6 报文头的处理较 IPv4 大大简化，提高了处理效率。另外，IPv6 为了更好支持各种选项处理，提出了扩展头的概念，新增选项时不必修改现有结构就能做到，理论上可以无限扩展，体现了优异的灵活性。

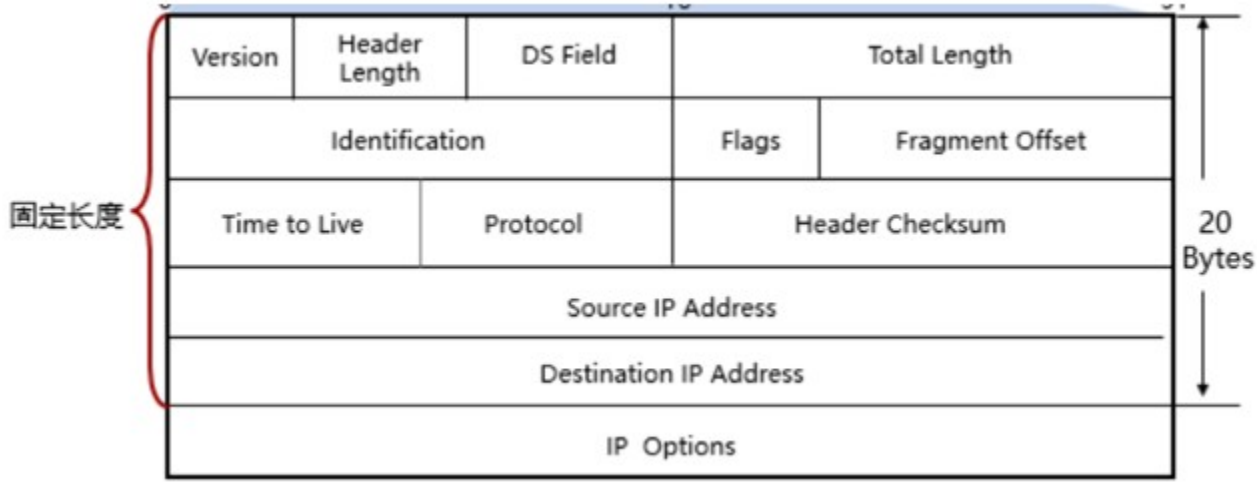
扩展问题 1：ipv6 的扩展报头？
答：当超过一种扩展报头被用在同一个分组里时，报头必须按照下列顺序出现：
IPv6 基本报头
1.逐跳选项扩展报头
2.目的选项扩展报头

3.路由扩展报头
4.分段扩展报头
5.认证扩展报头
6.封装安全有效载荷扩展报头
7.目的选项扩展报头
8.上层协议数据报文

扩展问题 2：ipv6 的扩展报头可以无序出现吗？
答：不能，必须有序出现。

扩展问题 3：扩展报头可以重复出现吗？
答：只有目的选项扩展头部可以；

扩展问题 4：ipv6 和 ipv4 报头到的区别？
1、ipv6 中没有了 ip 报头长度字段，因为 ipv6 的基本报头是固定长度为 40 字节；
2、ipv6 将 ipv4 中的分片字段放在了 ipv6 扩展报头中；
3、ipv6 将 ipv4 中的校验和字段（checksum）去除；
4、ipv6 中增加了 flow label 来支持 Qos；



IPv6 过渡技术

扩展问题 1：手动隧道和自动隧道的区别？
1、手动隧道需要指定目的 IPV4 地址，而自动隧道不需要指定目的 IPV4 地址；
2、手工隧道支持路由协议，自动隧道不支持路由协议；
3、手工隧道多个站点互联的时候，需要配置多个 tunnel 接口，而自动隧道多个站点互联不需要配置多个隧道接口；

扩展问题 2：为什么手动隧道需要指定目的地址，而自动隧道不需要指定？
因为在使用自动隧道时，设备可以根据目的 ipv6 地址生成目的 ipv4 地址，而手动隧道不行；
举例：6to4 自动隧道中，从特定的 ipv6 地址（2002:0202:0202::1）中将第 2 和第 3 段取出来，成为目的 ipv4 地址（2.2.2.2）；

扩展问题 3：为什么手工隧道可以支持路由协议，而自动隧道不支持？
因为配置了静态隧道之后，隧道的源地址和目的地址都是确定的，相当于两个 site 之间点到点的连接，所以可以将隧道也宣告进路由协议中；

扩展问题 4：6to4 中配置静态路由的作用？
答：静态路由是配置在边界路由器上的，然后我们在边界路由器上将该静态路由（2002:: 16 tunnel0/0/0），引入到 site 的 IGP 中，让 site 内的设备能通过该路由访问到其他 site。

扩展问题 5：手动隧道和自动隧道的优缺点？
1、如果是两个固定的 site，手工隧道只需要在两个 site 的边界路由器上配置即可，而配置自动隧道的话，比如 6to4，需要将 site 内的设备的 ipv6 地址配置成特定的 ipv6 地址；

2、如果是多个运行 ipv6 网络的 site，需要通过 ipv4 网络互联互通，此时使用自动隧道配置会更加简单，因为自动隧道会自动发现目的 ipv4 地址。

扩展问题 6：ipv6 over ipv4 和 ipv6 over ipv4 gre 的区别？
1、报文封装不同，GRE 多了一个 4 字节的 GRE 头部；
2、GRE 可以承载更多种类的上层数据；
3、GRE 可以提供一定的安全性（gre key 123）；
4、GRE 可以检测隧道是否可用；

扩展问题 7：IPv4 协议号里标识下一个头是 GRE 头的数值是哪个？
protocol 为 47 时，标识下一个头是 GRE；

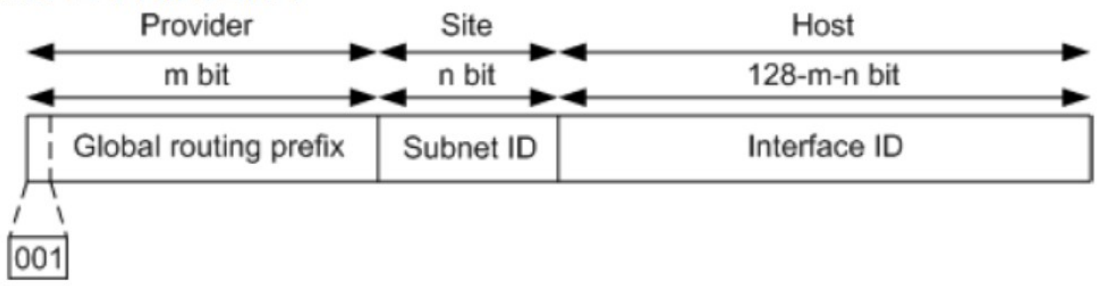
扩展问题 8：GRE 头里哪个字段标识接下来是 IPV6 头部？
用 Protocol Type 字段，protocol type：0X86DD，标识下一个头部为 ipv6 头部；

=========
IPv6 地址分类
IPv6 地址分为单播地址、任播地址（Anycast Address）、组播地址三种类型。

单播地址
IPv6 定义了多种单播地址，目前常用的单播地址有：未指定地址、环回地址、全球单播地址、链路本地地址、唯一本地地址 ULA（Unique Local Address）。
未指定地址:　即 0:0:0:0:0:0:0:0/128 或者::/128。
环回地址：即 0:0:0:0:0:0:0:1/128 或者::1/128。环回与 IPv4 中的 127.0.0.1 作用相同，主要用于设备给自己发送报文。

全球单播地址：是带有全球单播前缀的 IPv6 地址，其作用类似于 IPv4 中的公网地址。
全球路由前缀（Global routing prefix）、子网 ID（subnet ID）和接口标识（Interface ID）组成，

图 2 全球单播地址格式



目前已经分配的全球路由前缀的前 3bit 均为 001。因此前缀为 2000::/3。

链路本地地址 ： link-local 前缀 FE80::/10
是 IPv6 中的应用范围受限制的地址类型，只能在连接到同一本地链路的节点之间使用。它使用了特定的本地链路前缀 FE80::/10（最高 10 位值为 1111111010），同时将接口标识添加在后面作为地址的低 64 比特。

当一个节点启动 IPv6 协议栈时，启动时节点的每个接口会自动配置一个链路本地地址（其固定的前缀+EUI-64 规则形成的接口标识）。这种机制使得两个连接到同一链路的 IPv6 节点不需要做任何配置就可以通信。所以链路本地地址广泛应用于邻居发现，无状态地址配置等应用。

类似于 IPv4 的 169.254.0.0/16 是一个本地链接地址段

唯一本地地址 ： site-local FC00::/7
是另一种应用范围受限的地址，它仅能在一个站点内使用。它的作用类似于 IPv4 中的私网地址，任何没有申请到提供商分

配的全球单播地址的组织机构都可以使用唯一本地地址。唯一本地地址只能在本地网络内部被路由转发而不会在全球网络中被路由转发。

类似于 IPv4 的私有地址
A 类 10.0.0.0 - 10.255.255.255
B 类 172.16.0.0 - 172.31.255.255
C 类 192.168.0.0 - 192.168.255.255

唯一本地地址具有如下特点：
具有全球唯一的前缀（虽然随机方式产生，但是冲突概率很低）。
可以进行网络之间的私有连接，而不必担心地址冲突等问题。
具有知名前缀（FC00::/7），方便边缘路由器进行路由过滤。
如果出现路由泄漏，该地址不会和其他地址冲突，不会造成 Internet 路由冲突。
应用中，上层应用程序将这些地址看作全球单播地址对待。
独立于互联网服务提供商 ISP（Internet Service Provider）。

组播地址

IPv6 的组播与 IPv4 相同，用来标识一组接口，一般这些接口属于不同的节点。一个节点可能属于 0 到多个组播组。发往组播地址的报文被组播地址标识的所有接口接收。
一个 IPv6 组播地址由前缀，标志（Flag）字段、范围（Scope）字段以及组播组 ID（Global ID）4 个部分组成：
前缀：IPv6 组播地址的前缀是 FF00::/8（1111 1111）类似于 224.0.0.0
标志字段（Flag）：长度 4bit，只用最后一比特（前三位必须置 0），
当该位值为 0 时，表示当前的组播地址是由 IANA

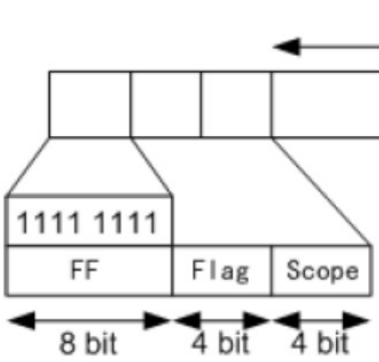
所分配的一个永久分配地址；

当该值为 1 时，表示当前的组播地址是一个临时组播地址（非永久分配地址）。

范围字段（Scop）：长度 4bit，用来限制组播数据流在网络中发送的范围

组播组 ID（Global ID）：长度 112bit，用以标识组播组。目前，并没有将所有的 112 位都定义成组标识，而是建议仅使用该 112 位的最低 32 位作为组播组 ID，将剩余的 80 位都置 0。这样每个组播组 ID 都映射到一个唯一的以太网组播 MAC 地址

0：预留
1：节点本地范围
2：链路本地范围，例如 FF02::1
5：站点本地范围
8：组织本地范围
E：全球范围
F：预留



field	value	description
Flag	1	temporary multicast address
	0	permanent multicast address
Scope	1	node
	2	link
	4	management
	5	site
	8	organization
	E	global
	the rest	unsigned or reserved

被请求节点组播地址

被请求节点组播地址（Solicited-Node Multicast Address）通过节点的单播或任播地址生成。当一个节点具有了单播或任播地址，就会对应生成一个被请求节点组播地址，并且加入这个组播组。一个单播地址或任播地址对应一个被请求节点组播地址。该地址主要用于邻居发现机制和地址重复检测功能。

IPv6 中没有广播地址，也不使用 ARP。但是仍然需要从 IP 地址解析到 MAC 地址的功能。在 IPv6 中，这个功能通过邻居请求 NS（Neighbor Solicitation）报文完成。当一个节点需要解析某个 IPv6 地址对应的 MAC 地址时，会发送 NS 报文，该报文的目的 IP 就是需要解析的 IPv6 地址对应的被请求节点组播地址；只有具有该组播地址的节点会检查处理。
被请求节点组播地址由前缀 FF02::1:FF00:0/104 和单播地址的最后 24 位组成。

任播地址

任播地址标识一组网络接口（通常属于不同的节点）。目标地址是任播地址的数据包将发送给其中路由意义上最近的一个网络接口。适合于“One-to-One-of-Many”（一对组中的一个）的通讯场合。

IPv6 任播地址仅可用被分配给路由设备，不能应用于主机。
任播地址不能作为 IPv6 报文的源地址。

任播地址设计用来在给多个主机或者节点提供相同服务时提供冗余功能和负载分担功能。目前，任播地址的使用通过共享单播地址方式来完成。将一个单播地址分配给多个节点或者主机，这样在网络中如果存在多条该地址路由，当发送者发送以任播地址为目的 IP 的数据报文时，发送者无法控制哪台设备能够

收到，这取决于整个网络中路由协议计算的结果。这种方式可以适用于一些无状态的应用，例如 DNS 等。
IPv6 中没有为任播规定单独的地址空间，任播地址和单播地址使用相同的地址空间。目前 IPv6 中任播主要应用于移动 IPv6。在 6to4 中继中也使用了任播前缀（2002:c058:6301::）。

========
NDP 的作用
NDP（Neighbor Discovery Protocol，邻居发现协议）替代了 IPv4 的 ARP（Address Resolution Protocol）和 ICMP 路由器发现（Router Discovery），它定义了使用 ICMPv6 报文实现地址解析，跟踪邻居状态，重复地址检测，路由器发现以及重定向等功能。

NDP 的 7 个作用
1 路由器发现
2 无状态自动配置
3 重复地址检测
4 地址解析
5 邻居的状态跟踪
6 前缀重编址：
7 路由器重定向

========
IPv6 地址获取的方式：

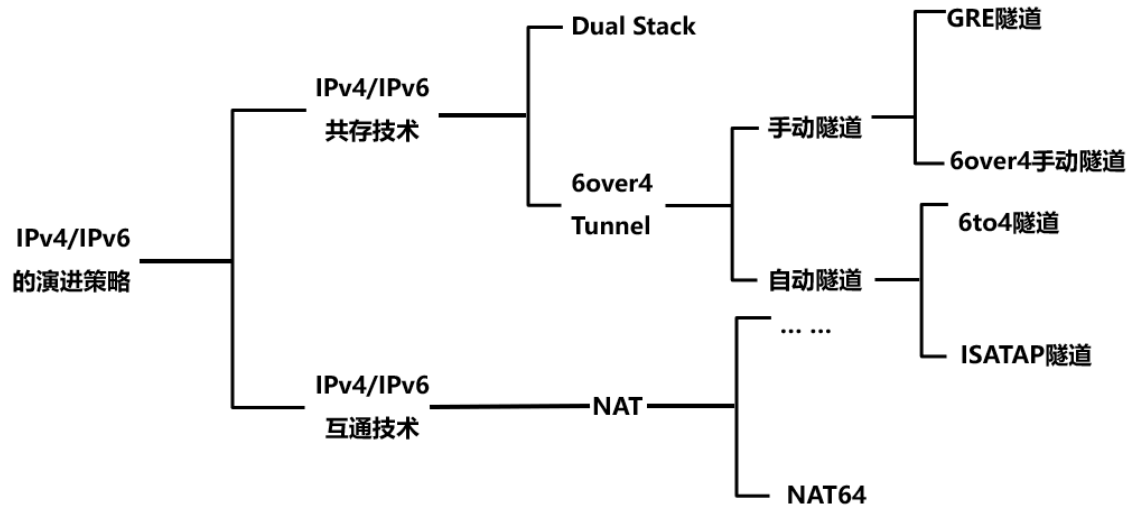
1.手工配置：此方法配置和 IPV4 的配置方法相同，在 IPV6 中主要是一些重要的服务器或路由器接口等需要用此方法来配置。

2.无状态自动获取：此方法要借助 ICMPv6 报文来实现，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。

3.通过 EUI-64 来自动生成 IPV6 地址：
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。

4.通过 DHCPV6 来获取地址：此方法由 DHCPV6 服务器实现

========
IPv6 IPv4 过渡技术



双栈技术 ：节点同时支持 IPv4 和 IPv6 协议栈。

IPv6 over IPv4 隧道：通过隧道技术，使 IPv6 报文在 IPv4 网络中传输。

手动隧道包括 IPv6 over IPv4 手动隧道和 IPv6 over IPv4 GRE 隧道。

自动隧道包括 IPv4 兼容 IPv6 自动隧道、6to4 隧道和 ISATAP 隧道

双栈技术

双栈技术是 IPv4 向 IPv6 过渡的一种有效的技术。网络中的节点同时支持 IPv4 和 IPv6 协议栈，源节点根据目的节点的不同选用不同的协议栈，而网络设备根据报文的协议类型选择不同的协议栈进行处理和转发。双栈可以在一个单一的设备上实现，也可以是一个双栈骨干网。对于双栈骨干网，其中的所有设备必须同时支持 IPv4/IPv6 协议栈，连接双栈网络的接口必须同时配置 IPv4 地址和 IPv6 地址。

隧道

隧道（Tunnel）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自身的报文中，然后在网络中传输。隧道是一个虚拟的点对点的连接。一个 Tunnel 提供了一条使封装的数据报文能够传输的通路，并且在一个 Tunnel 的两端可以分别对数据报文进行封装及解封装。**隧道技术就是指包括数据封装、传输和解封装在内的全过程。**隧道技术是 IPv6 向 IPv4 过渡的一个重要手段。