第7章 IPv6扩展头

本章讨论IPv6扩展头的含义、工作方式及与IPv4扩展头的区别，着重解释扩展头的顺序、使用方法，并讨论巨型报文、逐跳选项、目的地址选项、选路和分段头的使用。在第 9章将对安全性头(身份验证头和封装安全性净荷头)进一步讨论。

7.1 扩展头

第5章介绍了一种新的IPv6扩展头，它作为简化的IPv6头，由工作在无选项方式的大多数网络业务流所采用，同时它提高了网络对确实需要选项的包的处理能力。以下扼要重述第 5章的内容，这种新的IPv6扩展头包括：

- 逐跳选项头：此扩展头必须紧随在IPv6头之后，它包含包所经路径上的每个节点都必须检查的可选数据。到目前为止，只定义了一个选项：巨型净荷选项。该选项指明，此包的净荷长度超出了IPv6的16位净荷长度字段。只要包的净荷(包括逐跳选项头)超出65 535字节，就必须包含该选项。如果节点不能转发此包，则必须返回一个ICMPv6出错报文。
- 选路头：此扩展头指明包在到达目的地途中将经过的特殊的节点。它包含包沿途经过的各节点的地址列表。IPv6头的最初目的地址不是包的最终目的地址，而是选路头中所列的第一个地址。此地址对应的节点接收到该包后，对 IPv6头和选路头进行处理，然后将包发送到选路头列表中的第二个地址。如此继续，直至该包到达最终目的地。
- 分段头：此扩展头包含一个分段偏移值、一个“更多段”标志和一个标识字段，用于源节点对长度超出源端和目的端间路径MTU的包进行分段。
- 目的地选项头：此扩展头包含只能由最终目的地节点所处理的选项。目前，只定义了填充选项，将该头填充为64位边界，以备将来所用。
- 身份验证头(AH)：此扩展头提供了一种机制，对IPv6头、扩展头和净荷的某些部分进行加密的较验和计算。
- 封装安全性净荷(ESP)头：这是最后一个扩展头，不进行加密，它指明剩余的净荷已经加密，并为已获得授权的目的节点提供足够的解密信息。

除了理解上述扩展头的功能之外，还有必要了解这些扩展头的使用方法、工作情况以及将来如何用于扩展IPv6。下面一节将描述这些扩展头的正确用法，后续小节将详细解释每个扩展头的工作过程，与安全性相关的扩展头的内容参见第 9章。

7.2 扩展头的用法

将IPv4选项合并到标准IPv4头比较复杂。IPv4头最短为20字节，最长为60字节，附加数据包含IPv4选项，必须由路由器翻译以对 IP包进行处理。这种方法有两个影响：其一，路由器实现时往往对附加选项的包进行分流处理，因此导致处理效率降低；其二，由于选项导致性能下降，应用开发者倾向于不使用选项。

使用IPv6扩展头，可以在不影响性能的前提下实现选项。开发者可以在必要时使用选项，

而无须担心路由器会对带扩展选项的包区别对待，除非是设置了选路扩展头或逐跳选项。即使设置了这两个选项，路由器仍可以进行必要的处理，比使用 IPv4选项容易。

7.2.1 扩展头的标识

所有的IPv6头长度都一样，并且看起来几乎相同，唯一的区别在于下一个头字段。在没有扩展头的IPv6包中，此字段的值表示上一层协议。即，若 IP包中含有TCP段，则下一个头字段的8位二进制值是6(源自RFC 1700(已指派号码))；若IP包中含有UDP数据报，这个值就是17。表7-1中列举了下一个头字段的某些值。

下一个头字段值指明是否有下一个扩展头及下一个扩展头是什么，因此， IPv6头可以链接起来，从基本的IPv6头开始，逐个链接各扩展头。这种头连接链的构成见图 7-1。图中第一个IPv6包没有扩展头；第二个包有选路扩展头，其后为 TCP头和包的其余部分；最后一个包有更复杂的头链，IPv6头后面有分段扩展头，然后是身份验证扩展头，后接 ESP扩展头，最后是TCP头和包的其余部分。

表7-1 IPv6下一个头字段的一些可能值，用以指明扩展头

下一个头字段值	描 述
0	逐跳头
43	选路头(RH)
44	分段头(FH)
51	身份验证头(AH)
52	封装安全性净荷(ESP)
59	没有下一个头
60	目的地选项头

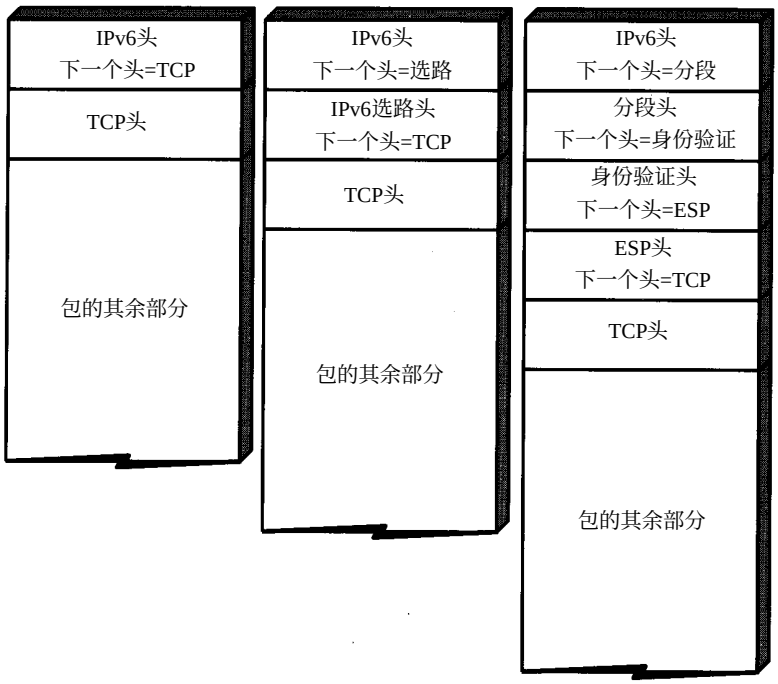

图7-1 三个不同的IPv6包：第一个包没有扩展头，第二个包有一个选路扩展头，第三个包有三个扩展头

7.2.2 扩展头的顺序

一个IPv6包可以有多个扩展头，但是，只有一种情况允许同一类型的扩展头在一个包中多次出现，而且各扩展头在链接时有一个首选顺序。 RFC 1883规定，扩展头应该依照如下顺序：

(1) IPv6头。
(2) 逐跳选项头。
(3) 目的地选项头(应用于IPv6目的地址字段的第一个目的地和选路头中所列的附加目的地中)。
(4) 选路头。
(5) 分段头。
(6) 身份验证头。
(7) ESP头。
(8) 目的地选项头(当使用选路头时，仅应用于包的最终目的地)。
(9) 上层头。

从以上顺序可知，在同一个 IP包中只有目的地选项扩展头可以多次出现，并且仅限于包中包含选路扩展头的情况。

上述顺序并不是绝对的。例如，前面已提及，在包的其余部分要加密时， ESP头必须是最后一个扩展头。同样，逐跳选项优先于所有其他扩展头，因为每个接收 IPv6包的节点都必须对该选项进行处理。

7.2.3 建立新的选项

扩展头必须通过IPv6头的下一个头字段来确认。这意味着由于这个字段为 8位，最多只能有256个不同值。即使将来该字段的可能取值的个数有所减少，也必须支持上一层头的所有可能值。即，该值不仅对扩展头进行标识，还标识着封装在 IP包内的所有其他协议。因此，目前已经指派了很多值，未指派的值相当有限。

IPv6用于扩展头的某些协议标识符沿自 IPv4，例如身份验证头和 ESP头。到目前为止，已指派了很多扩展头，但也允许通过逐跳选项扩展头和目的地选项扩展头来建立新的选项。

除了为下一个头字段保存协议值以外，通过使用这些选项头扩展，很容易健壮地实现新选项。如果使用一个全新的头类型来发送 IP包，若目的节点支持新的头类型，则一切顺利；反之，如果新的头类型对目的节点是未知的，则目的节点只能丢弃该包。另一方面，所有的IPv6节点都必须支持逐跳选项扩展头、目的地选项扩展头以及一些基本选项 (参见下节)。此时，如果目的节点收到带有目的地选项扩展头的包，即使不支持该扩展头中的选项，它也能够响应。即，这些选项可以向接收节点请求适当的响应，即使接收节点对选项并不理解。例如，选项可能是“ 做X，如果不理解X，就丢弃此包 ”这样的形式，或者可以是“ 做 X，如果不理解X，就跳过此选项，并完成对扩展头的处理 ”。选项也可以请求目的节点发回一个 ICMP出错报文，以指明目的节点不理解此选项。

7.2.4 选项扩展头

逐跳选项扩展头和目的地选项扩展头可以包含特定的选项。 RFC 1883中定义了两个填充

选项，用于确保扩展头字段符合边界要求。即，如果选项使用 3个8位字段后接一个32位字段，就必须插入(即填充)附加的8位，以确保在越过一个 32位字边界时，选项中的 32位字段不会被拆开。图7-2给出了该过程。如果无需填充，则只定义一个功能选项，即逐跳选项扩展头中使用的巨型净荷选项。

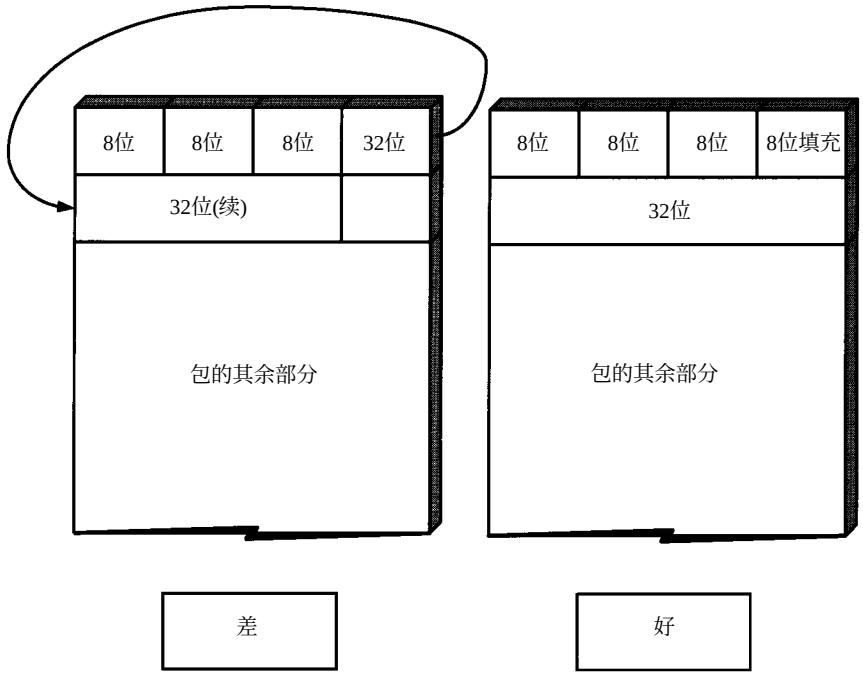

图7-2 选项头可能需要填充，以保证字段在越过32位字边界时不会被拆开

所有的选项扩展头 —— 逐跳选项扩展头和目的地选项扩展头都有类似的帧格式，见图 7-3。很简单，这些扩展头只有两个预定义的字段：下一个头字段和头扩展长度字段。所有 IPv6头都包含下一个头字段。头扩展长度字段占 8位，指明该选项头的长度。该长度以 8字节为单位，不包含扩展头的第一个8字节，即如果选项扩展头只有 8字节长，该字段值即为0。该字段限制了扩展头最多为2048字节。扩展头的其余部分为该扩展头所包含的选项。

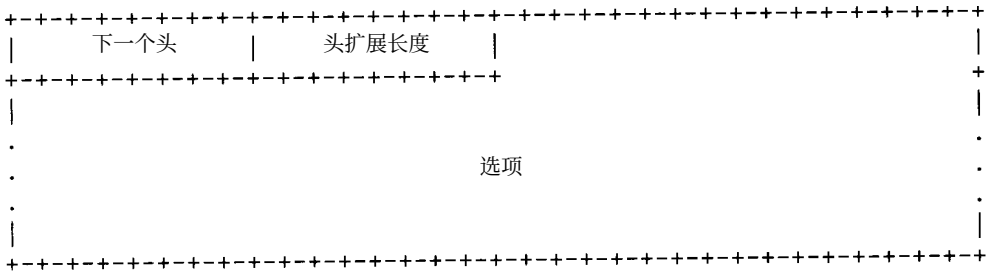

图7-3 RFC 1883中定义的标准选项头格式

7.2.5 选项

IPv6选项包含如下三个字段：

- 选项类型：该字段为8位标识符，指明选项的类型。即使目的节点不能够识别选项，也可以由该字段的前3位编码翻译出选项的类型。
- 选项数据长度：该字段为8位整数，表示选项数据字段的长度。该字段最大值为 255。
- 选项数据：该字段包含选项特定的数据，最大长度为 255字节。

选项类型字段的前2位表示目的节点在不能识别特定的选项时应该采取的动作，共有如下四种选项类型：

- 00：忽略此选项，完成对扩展头其余部分的处理。
- 01：丢弃整个包。
- 10：丢弃包，不论该包的目的地址是否是组播地址，都向该包的源地址发送一个 ICMP报文。
- 11：丢弃包，如果该包的目的地址是单播地址或任意点播地址 (即非组播地址)，则向该包的源地址发送一个ICMP报文。

选项类型的第3位指明在包从源地址到目的地址的传送过程中，选项数据的值是否可以改变。若为0，则不允许改变；若为1，则选项数据是可变的。

逐跳选项扩展头和目的地选项扩展头都包含的相同选项是两个填充选项：填充选项 1和填充选项N。填充选项1很特别，它只有8位，全部置为0，没有选项数据长度字段和其他选项数据。

而填充选项N是由前面的四种选项类型之一来标识的，它使用多个字节来填充扩展头。如果扩展头需要N字节填充，则选项数据长度字段值为 N-2，即选项数据字段占 N-2个字节，全部置为0。再加上1字节的选项类型字段、 1字节的选项数据长度字段，一共填充了 N字节。

7.3 逐跳选项

从源节点到目的节点的路由上的每个节点，即每个转发包的路由器都检查逐跳选项中的信息。到目前为止，只定义了一个逐跳选项：巨型净荷选项。图 7-4描述了RFC 1883所定义的使用巨型净荷选项的逐跳扩展头。

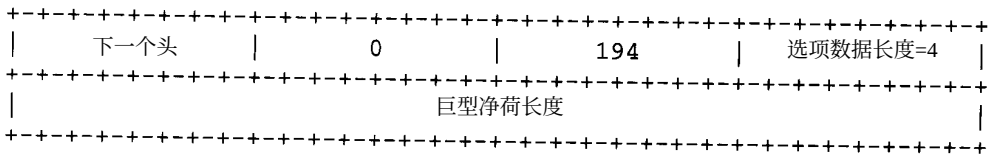

图7-4 RFC 1883中定义的包含巨型净荷选项的逐跳扩展头，允许IPv6包中的净荷超过65 535字节

与其他选项扩展头相同，前两个字段指明了下一个头协议和扩展头的长度 (此时，由于整个选项只有8位，扩展头长度的字段值为 0)。巨型净荷选项从扩展头的第三个字节开始。第三个字节为扩展头类型，其值为 194；第四个字节，即巨型净荷选项数据长度的值为 4。选项的最后一个字段为巨型净荷长度，指明包括逐跳选项扩展头在内， IP包中所包含的实际字节数，但不包括IPv6头。

只有沿途每个路由器都能够处理时，节点才能使用巨型净荷选项来发送大型 IP包。因此，该选项在逐跳扩展头中使用，要求沿途的每个路由器都必须检查此信息。

巨型净荷选项允许IPv6包净荷长度超过 65 535字节，最多可以为 $2^{32}-1$字节，超过了40亿

字节。如果使用该选项，要求IPv6头的16位净荷长度字段值必须为0，扩展头中的巨型净荷长度字段值不小于65 535。如果不满足这两个条件，接收包的节点应该向源节点发送 ICMP出错报文，通知有问题发生。此外还有一个限制：如果包中有分段扩展头，就不能同时使用巨型净荷选项，因为使用巨型净荷选项时不能对包进行分段。

7.4 选路头

选路头代替了IPv4中所实现的源选路。源选路允许用户指定包的路径，即到达目的地沿途必须经过的路由器。在IPv4源选路中，使用IPv4选项，对用户可以指定的中间路由器的个数有一定限制：带扩展的IPv4头有40个附加字节，最多只能填入10个32位地址。此外，由于路径上的每个路由器都必须处理整个地址列表，而不论该路由器是否在列表中，因而对源路由包的处理很慢。

IPv6定义了一个通用的选路扩展头，有两个字段，各占1字节：选路类型字段和剩余段数字段。其中选路类型字段表示所使用的选路头的类型；而剩余段数字段表示扩展头的其余部分所列出的附加路由器的个数，这些路由器是在到达最终目的地的途中包必须经过的。扩展头的其余部分为类型特定的数据，与选路头类型相关。RFC 1883中定义了一种类型，即类型0选路头。

类型0选路扩展头解决了IPv4源选路的主要问题。只有列表中的路由器才处理选路头，其他路由器则不必处理。而且列表中最多可以指定256个路由器。对选路头的操作过程如下：

- 由源节点构造包必须经过的路由器的列表，并构造类型 0选路头，头中包括路由器的列表、最终目的节点地址和剩余段数，剩余段数 (8位整数)指明在包向目的节点交付之前所必须经过的特定路由器的数目。
- 源节点发送包时，将IPv6头目的地址设置为选路头列表中的第一个路由器的地址。
- 该包一直转发，直到到达路径中的第一站，即 IPv6头的目的地址(选路头列表中的第一个路由器)，只有该路由器才检查选路头，沿途的中间路由器都忽略选路头。
- 在第一站和所有后续其他站，路由器检查选路头以确保剩余段数与地址列表一致。若剩余段数的值等于0，则表示此路由器节点实际上是该包的最终目的地，节点将继续对包的其他部分进行处理。
- 假定此节点不是该包的最终目的地，它将自己的地址从 IPv6头的目的地址字段取出，并以选路头列表中的下一个节点地址来替代。同时，节点将剩余段数字段的值减 1。然后将包发送往下一站。列表中的其他节点重复此过程，直到包到达最终目的地。

RFC 1883对类型0选路头的定义中，在剩余段数字段后保留了一个字节，并增加了24位严格/宽松位映射字段。该字段将24个标志映射到最多24个中间路由器，由此源节点可以指定使用严格选路还是宽松选路。严格选路不允许经过列表中不包含的中间路由器，而宽松选路则允许。目前没有采纳该方案，剩余段数字段之后的整个 32位都作为保留位。未使用严格/宽松位映射字段表示头中所列举的路由器个数只受限于 8位的剩余段数字段，当然也表示在类型 0选路头中不能使用严格选路。

7.5 分段头

IPv6只允许源节点对包进行分段，简化了中间节点对包的处理。而在 IPv4中，对于超出本地链路允许长度的包，中间节点可以进行分段。这种处理方式要求路由器必须完成额外的

工作，并且在传输过程中包可能被多次分段。当一个节点要发送的包对于本地链路的单个数据传送单元来说太大时，就需要分段。例如，以太网允许传送的 MTU为1500字节，要发送一个4000字节的IP包，如果不分成三段，每段均小于 1500字节，就无法在以太网链路上传送。前方有些链路可能具有更小的 MTU，比如576字节，这种链路上的路由器就必须将已经分成1500字节的IP包分段，再次分成更小的段。

IPv4中的分段很令人烦恼，它使得中间节点和目的节点都必须增加处理分段的必要开销。通过使用路径MTU发现机制，源节点可以确定源节点到目的节点之间的整个链路中能够传送的最大包长度，从而可以避免中间路由器的分段处理。 RFC 1883规定最小的MTU为576字节，但在将用来代替RFC 1883的文档草案中，最小的MTU要求已增加到1280字节，并建议将链路配置为应该至少可以传送1500字节长的包。

上述规定表明，源节点可以发送长达 1280字节的包，而不必顾虑这些包会被分段。长达1500字节的包也很可能不被分段。但是， IPv6规范建议所有节点都执行路径 MTU发现机制，并只允许由源节点分段。换言之，在发送任意长度的包之前，必须检查由源节点到目的节点的路径，计算出可以无需分段而发送的最大长度的包。如果要发送超出此长度的包，就必须由源节点进行分段。

在IPv6中，分段只发生在源节点，并使用分段头来表示。 RFC 1883中规定的帧格式如图7-5所示。分段头字段包括：

- 下一个头字段：此8位字段对所有的IPv6头是共同的。
- 保留：此8位字段目前未用，设置为0。
- 分段偏移值字段：与 IPv4的分段偏移值字段很相似。此字段共 13位，以8字节为单位，表示此包(分段)中数据的第一个字节与原来整个包中可分段部分的数据的第一个字节之间的位置关系。换言之，若该值为 175，表示分段中的数据从原包的第 1400字节开始。
- 保留字段：此2位字段目前未用，设置为0。
- M标志：此位表示是否还有后续字段。若值为 1，表示后面还有后续字段；若值为 0则表示这是最后一个分段。
- 标识字段：该字段与 IPv4的标识字段类似，但是为 32位，而在IPv4中为16位。源节点为每个被分段的IPv6包都分配一个32位标识符，用来唯一标识最近 (在包的生存期内)从源地址发送到目的地址的包。

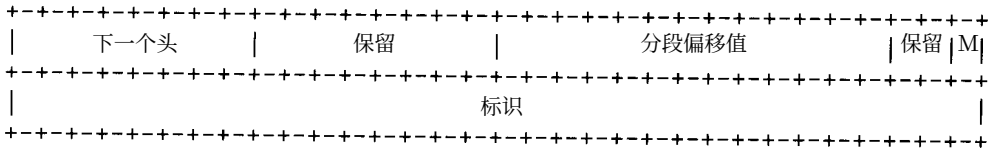

图7-5 RFC 1883中定义的IPv6分段扩展头字段

整个IPv6包中只有部分可以被分段，可分段的部分包括：净荷和只能在到达最终目的地时才处理的扩展头。对于 IPv6头和在发往目的节点的途中必须由路由器处理的扩展头，如选路头或逐跳选项头，则不允许进行分段。

7.6 目的地选项

类似逐跳选项头，目的地选项头提供了一种随着 IPv6包来交付可选信息的机制。其余的

扩展头选项，如分段头、身份验证头和ESP头，都是每次出于某一个特定的理由而定义的，而目的地选项扩展头则是允许为目的节点而定义的新选项。目的地选项将使用前面所描述的构造选项的格式。

到目前为止，除了前面提到的填充选项，在已发布的 RFC中尚未定义任何目的地选项，但是Internet草案中定义了一些和移动IP相关的选项，具体内容参见第11章。