实验二十二 OSPF 邻居交换报文结构分析

【实验目的】

1、掌握 OSPF 的报文格式；
2、掌握 OSPF 的工作过程。

【实验学时】

2 学时

【实验环境】

在本实验中需要 4 台路由、1 台交换机、1 台 RG-PATS 网络协议分析仪。四台路由器运行 RIP 路由协议，使用协议分析仪采集数据包，对采集到的数据进行分析。

将所有的路由器都接入到交换机上，并在交换机上配置端口映像功能，具体 IP 分配如下表：

表 6-4 设备 IP 地址分配表

设备	接口	IP 地址	连接到交换机
RSR-A	FA0/0	192.168.1.1/24	FA0/8
RSR-A	LO0	192.168.10.1/24	--
RSR-A	FA0/1	192.168.3.1/24	FA0/6
RSR-B	FA0/0	192.168.1.2/24	FA0/9
RSR-B	FA0/1	192.168.2.1/24	FA0/10
RSR-B	LO0	192.168.20.1/24	--
RSR-C	FA0/0	192.168.2.2/24	FA0/7
RSR-C	LO0	192.168.30.1/24	--
RSR-D	FA0/0	192.168.3.2/24	FA0/6
RSR-D	LO0	192.168.400.1/24	--
RG-PATS 网络协议分析仪	Eth 0	172.16.1.4	FA0/24

设备连接如下图所示：

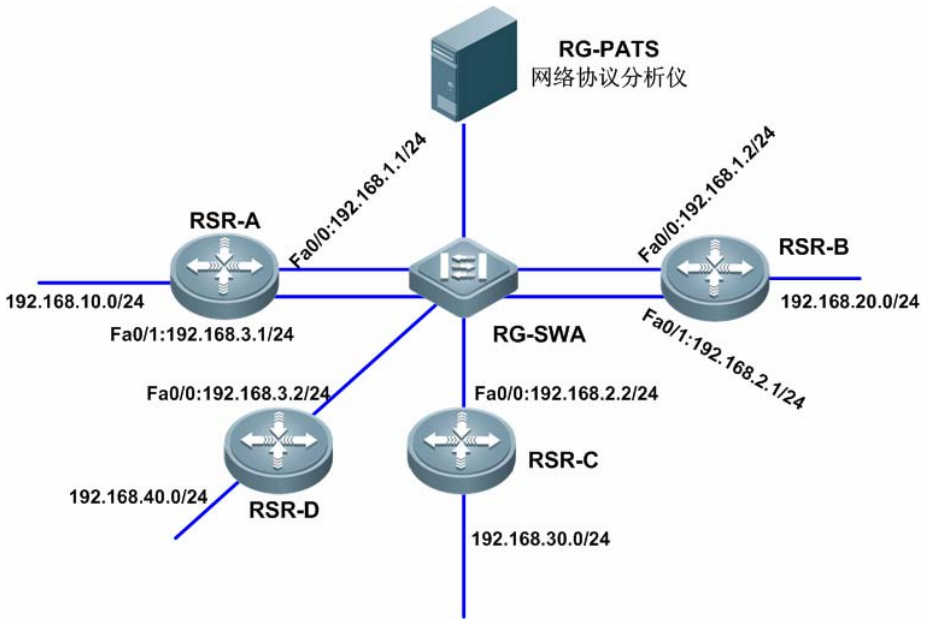

图 6-74 实验拓扑图

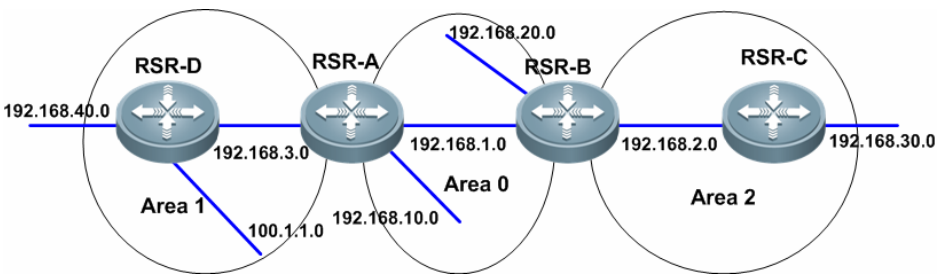

图 6-75 区域划分图

【实验内容】

1、掌握 OSPF 的工作原理；
2、学习 OSPF 的五种报文类型；
3、了解 OSPF 的特点；
4、了解 SPF 算法。

【实验流程】

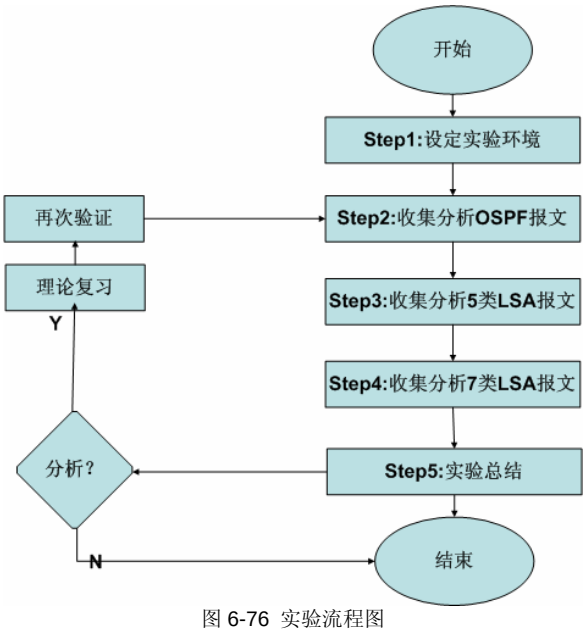

图 6-76 实验流程图

【实验原理】

OSPF 报文格式

OSPF 报文是由多重封装构成的，封装在 IP 头部内的是 5 种 OSPF 报文类型中的一种，每一种报文类型都是由一个 OSPF 报文头部开始，这个 OSPF 报文头部对于所有的报文类型都是相同的。

OSPF 所有报文类型都共享一个相似的报文结构，从一个通用的 24 字节首部开始，这种通用的首部使某些标准信息能够按照一致的方式进行传递，它还使收到 OSPF 报文的设备能够快速确定自己收到的是哪种类型的报文，以便了解是否还需要检查报文的剩余部分。如下图所示。

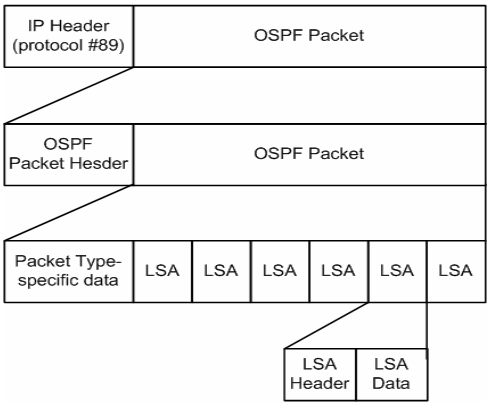

图 6-77 OSPF 报文由一系列封装组成

OSPF 有 5 种分组类型，这 5 种分组类型直接封装到 IP 分组的有效负载中，如图，OSFP 分组不使用传输控制协议（TCP）和用户数据报协议（UDP）。OSPF 要求使用可靠的分组传输机制，但由于没有使用 TCP，OSPF 将使用确认分组来实现自己的确认机制。

下表描述了 5 种 OSPF 分组类型。

表 6-5 OSPF 分组

类型	名称	描述
1	Hello	发现邻居并在它们之间建立邻接关系
2	数据库描述（DBD）	检查路由器的数据库之间是否同步
3	链路状态请求（LSR）	向另一台路由器请求特定的链路状态记录
4	LSU	发送请求的链路状态记录
5	LSAck	对其他类型的分组进行确认

在 OSPF 路由协议的数据包中，其数据包头长为 24 个字节，包含如下 8 个字段。在 IP 报头中，协议标识符 89 表示 OSPF 分组，所有 OSPF 分组开头的报文格式都相同，该报头中包含以下字段：如下图示。

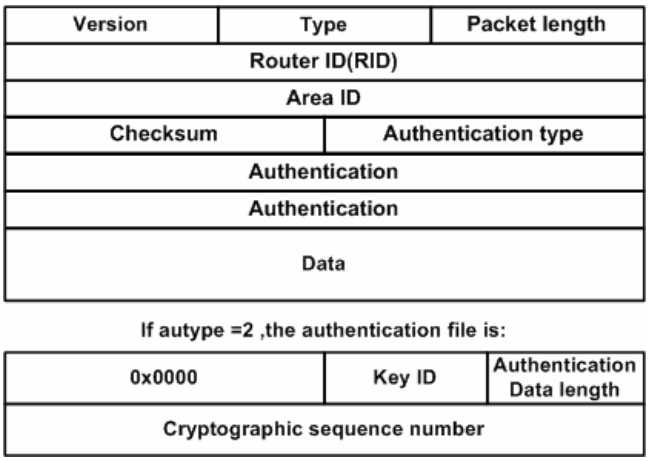

图 6-78 OSPF 分组报头的格式

- Version number：版本号，定义所采用的 OSPF 路由协议的版本，用于 OSPF 第 2 版。OSPF 版本 3 适用于 IPv6。
- Type：定义 OSPF 数据包类型。OSPF 数据包共有五种。1、Hello；2、Database Description；3、LinkState Request；4、LinkState Update；5、LinkState Acknowledgment。
- Packet length：定义整个数据包的长度，单位为字节。
- Router ID：用于描述数据包的源地址，以 IP 地址来表示路由器 ID，OSPF 路由器具有唯一的标识符，称为路由器 ID。路由器的 32 位长的一个唯一标识符，选举规则是，如果 loopback 接口不存在的话，就选物理接口中 IP 地址等级最高的那个；否则就选取 loopback 接口。这个路由器标识对于建立邻居关系和协调 LSU 交换非

常重要。在选举 DR/BDR 的过程中，如果 OSPF 优先级相同，则 RID 将用于决定谁赢得选举。如果该接口故障，则路由器就不可达。为了避免发生这种情况，最好定义一个回环接口作为强制的 OSPF 路由器 ID

- Area ID：用于区分 OSPF 数据包属于的区域号，所有的 OSPF 数据包都属于一个特定的 OSPF 区域。
- Checksum：校验位，用于标记数据包在传递时有无误码。
- Authentication type：指正在使用的认证模式，0 为没有认证、1 为简单口令认证、2 为加密检验和（MD5）。
- Authentication ：是指报文认证的必要信息，认证可以是 autype 字段中指定的任何一种认证模式，如是 autype＝0，将不检查这个认证字段，因此可以包含任何内容；如果 autype＝1，这个字段包含一个最长为 64 位的口令；如果 autype＝2，这个字段将包含一个 key ID、认证数据长度和一个不减小的加密序列号。
- Data：包含的信息随 OSPF 分组类型而异：

对于 Hello 分组，包含一个由已知邻居组成的列表。

对于 DBD 分组，包含 LSDB 摘要，其中包括所有已知路由器的 ID、最后使用用序列号和一些其他字段。

对于 LSR 分组，包含需要的 LSU 类型和能够提供所需 LSU 的路由器 ID。

对于 LSU 分组，包含完整的 LSA 条目，一个 OSPF 更新分组中可以包含多个 LSA 条目。

对 LSAck 分组，该字段为空。

Hello 报文

Hello 协议用来建立和保持 OSPF 邻居关系，采用多播地址 224.0.0.5。网络中的 OSPF 路由器必须彼此获知对方后才能共享信息，因为 OSPF 根据路由器之间的链路的状态来进行路由选择，这一过程是使用 Hello 协议来完成，Hello 协议通过确保邻居之间的双向通信来建立和维护邻接关系。路由器在从邻居那里收到的 Hello 分组中看到自己后，便进入了双向通信状态。

如下图所示，Hello 报文格式为：

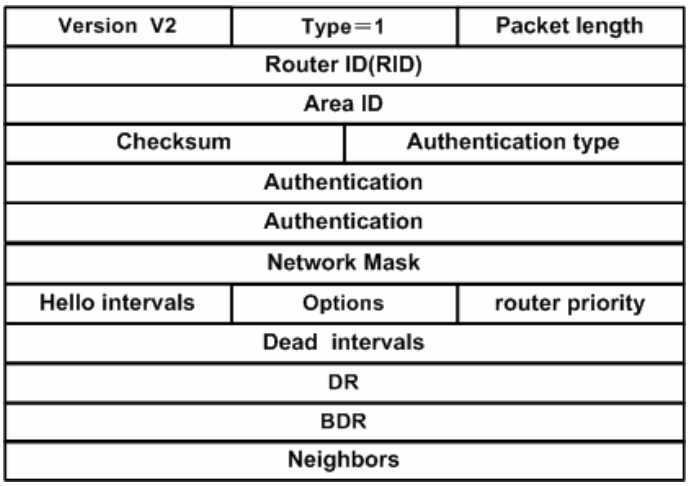

图 6-79　Hello 报文格式

- Network Mask：是指发送报文的接口的网络掩码。如果这个掩码和接收该报文的接口的网络掩码不匹配，那么该报文将被丢弃。这个技术性的措施可以确保路由器之间只有在它们共享网络的址精确匹配时才能互相成为邻居。
- Hello/Dead intervals：Hello 间隔和失效间隔，定义了发送 hello 包频率（默认在一个多路访问网络中间隔为 10 秒）；dead 间隔是 4 倍于 hello 包间隔。Hello 间隔是指接口上 Hello 报文传送之间的时间间隔，也是一个周期性的时间段，并以秒来计。Hello 失效间隔是指始发路由器在宣告邻居路由器无效之前，将要等待的从邻居路由器发出的 Hello 报文的时长，以秒数计，邻居路由器之间的这些计时器必须设置成一样，否则将不会建立邻接关系。如下图所示。

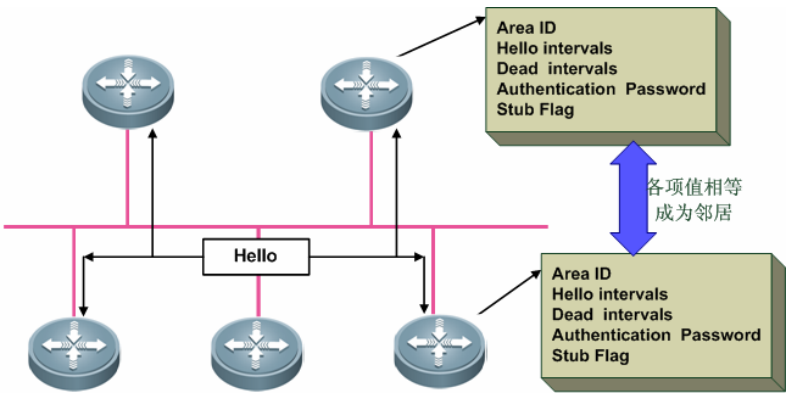

图 6-80 成为邻居时，hello 报文参数

- Option：这个字段允许路由器和其他路由器进行一些可选性能的通信。
- Router priority：路由器优先级，选举 DR 和 BDR 的时候使用，8 位长的一串数字。优先级值缺省为 1。 如果该字段设置为 0，那么始发路由器将没有资格选取成为 DR 和 BDR 路由器。
- DR：指定路由器，是指网络上指定路由器的接口的 IP 地址，注意，这里指的不是指定路由器的路由器 ID，在选取 DR 的过程中，这可能只是始发路由器所认为的 DR，而不是最终选举出来的 DR。如果没有 DR，那么这个字段将会设置为 0.0.0.0
- BDR：备份指定路由器，是指网络上备份指定路由器的接口的 IP 地址，同样，在选举 BDR 的过程中，这可能只是始发路由器的认为的 BDR，而不是最终选举出来的 BDR。如果没有 BDR，那么这个字段就会被设置为 0.0.0.0
- Neighbors：邻居列表，是一个循环重复的字段，它列出了始发路由器在过去的一个 Router Dead Interval 时间内收到有效 Hello 报文的网络上的所有邻居。邻居字段中包含已建立双向通信关系的邻接路由器。路由器在邻居发送的 hello 分组的邻居字段中看到自己后，便表明双向通信关系已建立。

如下图是使用 RG-PATS 网络协议分析仪采集到的 Hello 报文：

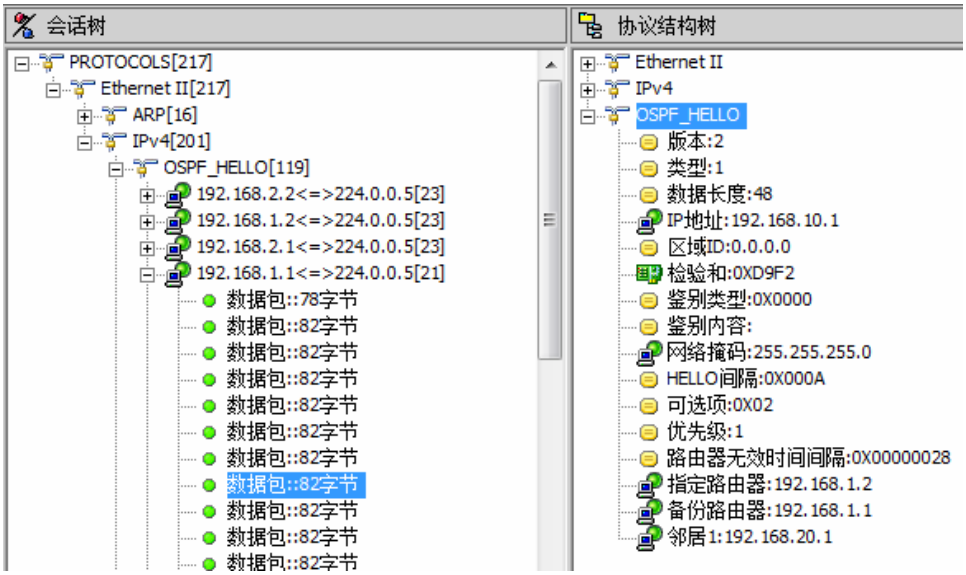

图 6-81 采集 Hello 报文

数据库描述报文

当 OSPF 中的两个路由器初始化连接时要交换数据库描述（DBD）报文。这个报文类型用于描述，而非实际地传送 OSPF 路由器的链路状态数据库内容。由于数据库的内容可能相当长，所以可能需要多个数据库描述报文来描述整个数据库。实际上，保留了一个域用于标识数据库描述报文序列。接收方对报文的重新排序使其能够真实地复制数据库描述报文。在 OSPF ExStart 状态下才开始交换 DBD 包，下图显示了数据库描述报文的格式：

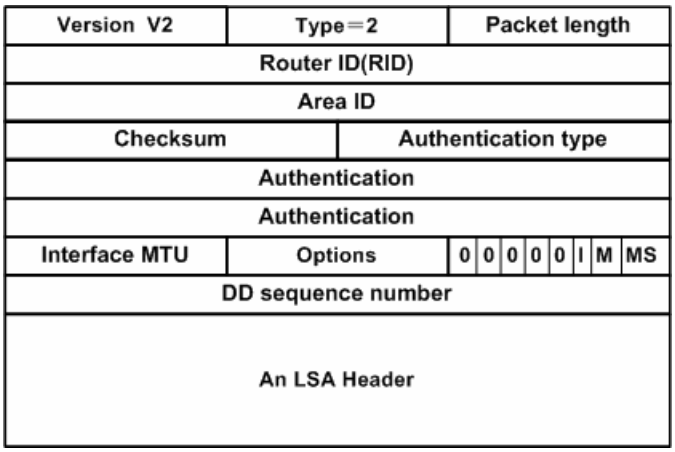

图 6-82 数据库描述数据包格式

DBD 交换过程按询问/应答方式进行，在这个过程中，一个路由器作为主路由器。另一个路由器作为从路由器，主路由器向从路由器发送它的路由表内容。显然，主从之间的关系会因每个 DD 交换的不同而不同。网络中的所有路由器会在不同时刻作用，在这个过程中既

可能是主又可能是从。

- Interface MTU：是指在报文不分段的情况下，始发路由器接口可以发送的最大 IP 报文大小，以 8bit 字节计。该字段用来检查两端 OSPF 路由器接口的 MTU 是否匹配。注意在 Virtual-link 中的 interface MTU 字段为 0，能匹配 MTU 可以在不进行 IP 分片时，最大可传输的 OSPF 数据库描述包。
- 选项字段：这个字段允许路由器和其他路由器进行一些可选性能的通信
- 报文下一个 8bit 字节的前 5 位没有被使用，而总是设置为 00000b。
- I 位，或称为初始位：当发送的是一系列数据库描述报文中是最初一个报文时，该位设置为 1。
- M 位，或称后继位：当发送报文还不是一系列数据库描述报文中的最后一个报文时，将该位置设置为 1。
- MS 位，或称为主/从位：在数据同步的过程中，该位置设置为 1，用来指明始发数据库描述报文的路由器是一个主路由器。从路由器将该位置设置为 0
- 在交换 DBD 包时，需要协商主从，比较 ROUTER-ID，最低的为 Master。MS 位是用来描述谁是主谁是从的角色。其中 M/S 为被置为 1，那该路由器为 Master。反之为 Slave。I/M 是二个位是用于传输 DBD 包时所使用的，I 位初始位，当每一个 DBD 包发送时它为被置为 1。M 位为 More DBD Packet，在同个 DD sequence number 中最后一个 DBD 包 M 位为 0，指示传输完毕。
- DD sequence number 为来标识一组 DBD 包。当第一个发送 DBD 包（也就是说该 DBD 包中的 I 位被置为 1，我们可以认为往往第一个 DBD 包一定是由 Master 发的）时，该 DD sequence number 字段开始被使用，在往后的 DBD 包中的 DD sequence number 都会递增 1。

对于 DBD 主要的作用在于，对于每台 OSPF 路由器都拥有他们各自的 LSA，但是双方并不知道对方有那些链路信息（或许有些信息是重复的），因此需要了解对方究竟有那些链路信息（LSA），所在 DBD 的作用在于收集对方有那些 LSA，但这 LSA 并不是明细的，只有一些简单的标识（An LSA Header）。通过比较自身拥有的 LSA，来检查自己有那些链路信息我没有的，这样可以减少 LSA 请求数量。

对于 LSA Header，一般可以简单标识一个 LSA。其中最主要的有 LS type/Link State ID/Advertising Router。

如下图是使用 RG-PATS 网络协议分析仪采集到的 DBD 报文：

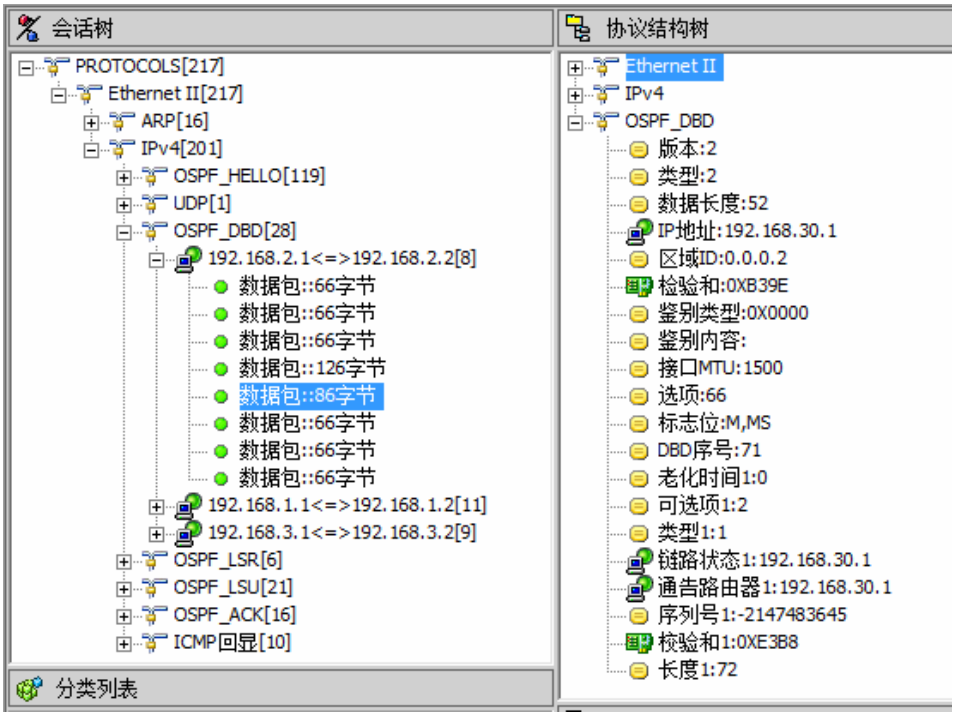

图 6-83 采集 DBD 报文

链路状态请求报文

OSPF 报文的第三种类型为链路状态请求报文。这个报文用于请求相邻路由器链路状态数据库中的一部分数据。表面上讲，在收到一个 DBD 更新报文之后，OSPF 路由器可以发现相邻信息不是比自己的更新就是比自己的更完全。如果是这样，路由器会发送一个或几个链路状态请求报文给它的邻居（具有更新信息的路由器）以得到更多的链路状态信息。

请求的信息必须是非常具体的。它必须使用下面的标准规范指明所要求的数据：

- 链路状态（LS）类型号。
- LS 标识。
- 通告路由器。

这些规范一起指明了一个具体的 OSPF 数据库子集，而不是它的一个事例。一个事例是与信息相同的子集，这个子集带有暂时边界（也就是时间戳）。记住，OSPF 是一个动态路由协议，它能对网络中链路状态的变化自动作出反应。因此，LS 请求的接收者把对这些特定路由信息解释为最新数据。如下图所示链路状态请求报文的数据格式：

Version V2	Type＝3	Packet length
Router ID(RID)		
Area ID		
Checksum	Authentication type	
Authentication		
Authentication		
LS type		
Link State ID		
Advertising Router		

图 6-84 链路状态请求报文数据包格式

- LSA Type：是一个链路状态类型号，长度为 4 个字节，表示正在请求的 LSA 的类型，用来指明 LSA 标识是一个路由器 LSA、一个网络 LSA 还是其他类型的 LSA 等。
- Link State ID：是 LSA 头部中和类型无关的字段。长度为 4 个字节，LSA 标识，通常是链接的路由器或网络的 IP 地址。
- Advertising Router，长度为 4 个字节，路由器的 ID，该路由器产生了这个正在请求更新的 LSA。

之前我们讲到 DBD 包，DBD 的作用在于是了解对方所拥有那些 LSA，那 LSR 就是用来请求，本地上没有的 LSA 而对方却有的 LSA。同样可以看到 LS type/Link State ID/Advertising Router 字段，这些字段可以用来唯一的标识 LSA。

LSA 实例，可认为是源 OSPF 路由器生成该 LSA，在往后的传输中，是以该 LSA 实例（对源 LSA 克隆）来继续传输给后面的 OSPF 路由器。或许一台路由器会收到不同的 LSA 实例，那他们如何确认是同个源 LSA 并且如何优选呢？答案是通在 LSA 包中的 LS sequence number、LS checksum，and LS age 这三个字段来描述。

如下图是使用 RG-PATS 网络协议分析仪采集到的 LSR 报文：

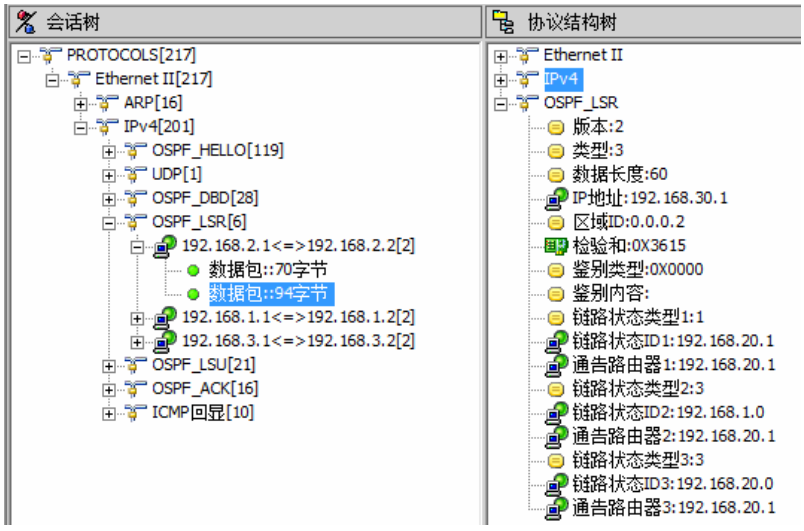

图 6-85 采集 LSR 报文

链路状态更新报文

链路状态更新报文用于把 LSA 发送给它的相邻节点。这些更新报文是用于对 LSA 请求的应答。有 5 种不同的 LSA 报文类型。这些报文类型用从 1 到 5 的类型号标识。

注意，由于 OSPF 通常把链路状态广播看作 LSA，因此会存在潜在的混淆。然而，实际上用于更新路由表的机制为链路状态更新报文—简称为 LSU。还有另一个报文结构，链路状态应答报文，简写为 LSAck；由于一些不可知的原因，这种报文称为链路状态应答，而 LSA 通常是指更新报文。下图显示 LSU 报文格式：

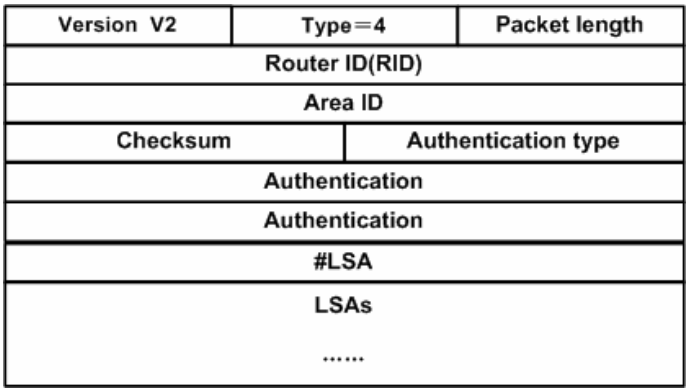

图 6-86 LSU 数据包格式

- #LSA 是 LSA 数量，长度为 4 个字节，表示该报文中所含的 LSA 数量
- LSAs 是可变长度的，一个或多个 LSA。每个更新报文都可以携带多个 LSA，它的大小可以达到传送这个报文的链路所允许的最大报文尺寸。

链路状态确认报文

第 5 种 OSPF 报文是链路状态应答报文。OSPF 的特点是可靠地传播 LSA 报文（L S A 表示链路状态通告（advertisement），不是链路状态应答），可靠性意味着通告的接收方必须应答。否则，源节点将没有办法知道 LSA 是否已到达目的地。因此，需要一些应答 LSA 接收的机制。这个机制是链路状态应答报文。如下图显示了确认报文的格式：

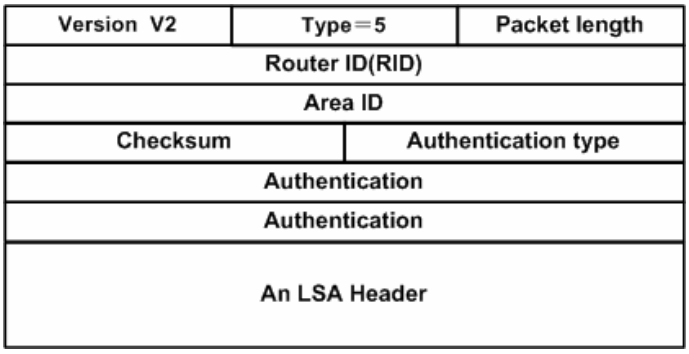

图 6-87 链路状态确认报文格式

链路状态应答报文惟一地标识其要应答的 LSA 报文。标识以包含在 LSA 头中的信息为基础，包括 LS 顺序号和通告路由器。LSA 与应答报文之间无需 1 对 1 的对应关系。多个 LSA 可以用一个报文来应答。一个链路状态确认报文的组成除了 OSPF 报文头部和一个 LSA 头部的列表之外，就没有其它多余的内容。

如下图是使用 RG-PATS 网络协议分析仪采集到的 LSAck 报文：

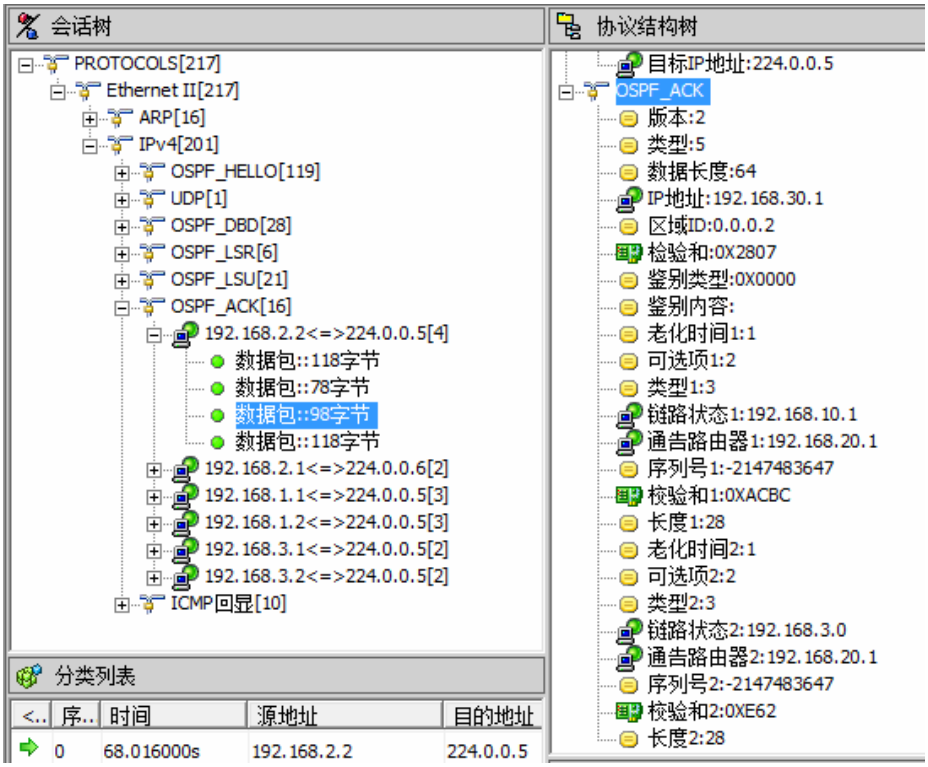

图 6-88 采集 LSAck 报文

OSPF 的 LSA 格式：

LAS 是 OSPF LSDB 的基本元素，下表总结了 LSA 类型：

表 6-6 OSPF LSA 类型

LSA 类型	描述
1 类	路由器 LSA
2 类	网络 LSA
3 类和 4 类	汇总 LSA
5 类	AS 外部 LSA
6 类	组播 OSPF LSA
7 类	为次末节区域定义的
8 类	BGP 的外部属性 LSA
9、10 或 11 类	不透明 LSA

常见的 LSA 类型为：

- Rauter LSA （路由器 LSA ，类型 1 ）：路由器 LSA 描述了路由器链路到区域的状态和耗费。所有这样的链路必须在一个 LSA 报文中进行描述。同时，路由器必须为它属于的每个区域产生一个路由器 LSA。所以，区域边界路由器将产生多个路由器 LSA，而区域内的路由器只需产生一个这样的更新。
- Network LSA （网络 LSA，类型 2 ）：网络 LSA 与路由器 LSA 相似，它描述的是连接进网络的所有路由器的链路状态和开销信息。二者的区别是网络 LSA 是网络中所有链路状态和开消信息的总和。只有网络的指定路由器记录这个信息，并由它来产生网络 LSA。
- Summary LSA-IP Network （网络汇总 LSA，类型 3）：只有 OSPF 网络中的区域边界路由器能产生这种 LSA 类型。使用这种 LSA 类型把一个区域的汇总路由信息和 OSPF 网络中相邻区域路由器信息进行交换。它经常汇总缺省的路由而不是传播汇总的 OSPF 信息至其他网络。
- Summary LSA-Autonomous System Boundary Router（自治系统边界路由器汇总 LSA ，类型 4）：类型 4 与类型 3 LSA 的关系密切。二者的区别是类型 3 描述区内路由，而类型 4 描述的是 OSPF 网络之外的路由。
- 自治系统外部 LSA（类型 5）：第 5 个 LSA 是自治系统外部 LSA。正如其名，这种 LSA 用于描述 OSPF 网络之外的目的地。这些目的地可以是特定主机或是外部网络地址。作为和外部自治系统相联系的 ASBR OSPF 节点负责把外部路由信息在它属于的整个区中传播。

这些 LSA 类型用于描述 OSPF 路由域的不同方面，它们直接寻址到 OSPF 区域中的每一个路由器并同时传输。这样的洪泛确保 OSPF 区域中的所有路由器关于网络的 5 个不同方面（LSA 类型）有一样的信息。路由器完整的 LSA 数据存储在链路状态数据库中。当 Dijkstra 算法应用于这些数据库的内容时会得到 OSPF 路由表。表和数据库的区别是数据库含有原始数据的完整集合，而路由表包含通过特定路由器接口到已知目的地的最短路径列表。

如下图显示了 LSA 头格式：

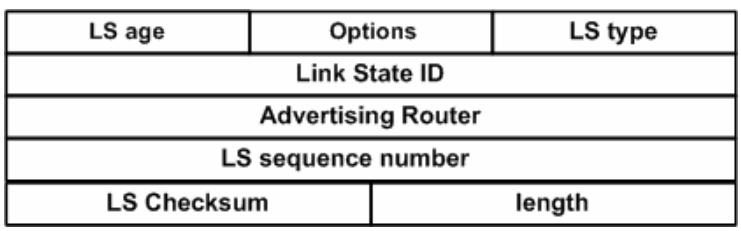

图 6-89 LSA 头格式

所有的 LSA 使用一个通用的头格式。这个头 20 字节长并附加于标准的 24 字节 OSPF 头后面。LSA 头惟一地标识了每种 LSA。所以，它包括关于 LSA 类型、链路状态 ID 及通告路由器 ID 的信息。下面是 LSA 头域：

- LS age：长度为 2 字节，是指自从发出 LSA 后所经历的时间，以秒计数。当泛洪

LSA 时，在从每一个路由器接口转发出来时，LSA 的老化时间都会增加一个 InfTransDelay 秒数。当然，当 LSA 驻留在链路状态数据库内时，这个老化时间也会增大。LSA 头中的前两个字节包含 LSA 的年龄。这个年龄是自从 LSA 产生时已消逝的时间秒数。

- Option：该字段指出在部分 OSPF 域中 LSA 能够支持的可选性能。
- LS Type：1 字节 LS 类型指出 5 种 LSA 类型中的一种。每种 LSA 类型的格式是不同的。因此，指出何种类型的数据附加在头后面必不可少。
- Link state ID：链路状态 ID 域 4 字节长，用于指明 LSA 描述的特定网络环境区域。这个域与前面提及的 LS 类型域关系紧密。实际上，这个域的内容直接依赖于 LS 类型。比如，在路由器 LSA 中，链路状态 ID 包含产生了这个报文的 OSPF 路由器 ID——通告路由器 ID。
- Advertising Router：产生该 LSA 的路由器的 ID 。
- LS 顺序号：OSPF 路由器会递增每个 LSA 报文的序列号。所以，接收到两个相同 LSA 事例的路由器有两种选择来决定哪一个是最新的报文， LS 顺序号域 4 字节长。检查这个域可以确定 LSA 在网络中已传输了多久。从理论上讲，一个新的 LSA 年龄比一个老的 LSA 年龄大是有可能的，特别是在大型复杂的 OSPF 网络中。所以，接收路由器比较 LS 顺序号。大号的 LSA 是最新生成的，这种机制不会因动态路由的变迁而受到损坏，而应认为其是一种更可靠的确定 LSA 时间的方法。
- LS 校验和：3 字节的 LS 校验和用于检查 LSA 在传输到目的地的过程中是否受到破坏。校验和采用简单的数学算法。它的输出结果依赖于其输入，并且有高度的一致性。给定相同的输入，校验和算法总是给出相同的输出。LS 校验和域使用部分 LSA 报文内容（包括头，不包括 LS 年龄和校验和域）来生成校验和值。源节点运行 Fletcher 算法并把结果存于 LS 校验和域中。目的节点执行相同的算法并把结果与存储在校验和域中的结果比较，如果两个值不相同，就可以认为报文在传输过程中被破坏。之后，产生一个传输请求。
- LS 长度：LS 长度域用于通知接收方 LSA 的长度（以字节为单位），这个域 1 个字节长。

LSA 报文体的剩余部分包含一个 LSA 的列表。每个 LSA 描述 OSPF 网络 5 个不同方面中的一个。所以，路由器 LS A 报文会广播区内已知存在的路由器信息。

如下图是使用 RG-PATS 网络协议分析仪采集到的 LSU 报文：

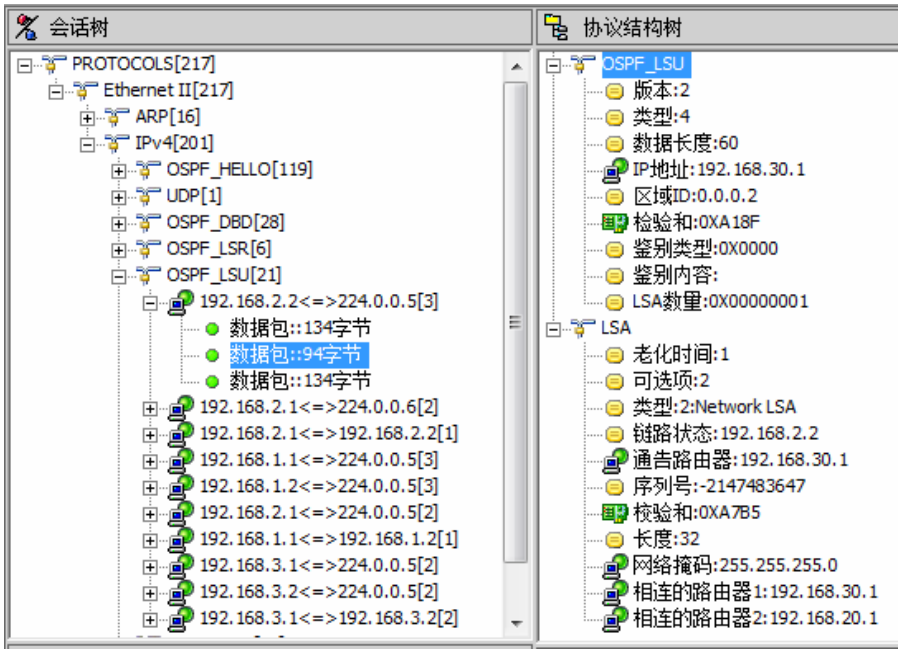

图 6-90 采集 LSU 报文

1 类 LSA

1 类 LSA：Router LSA，每台路由器都生成针对其所属区域的路由器的链路通告，路由器链路通告描述了路由器连接到区域的链路状态，只在区域内扩散，每种 LSA 的报头都是 20 字节，其中一个字段是链路状态 ID。如下图所示。

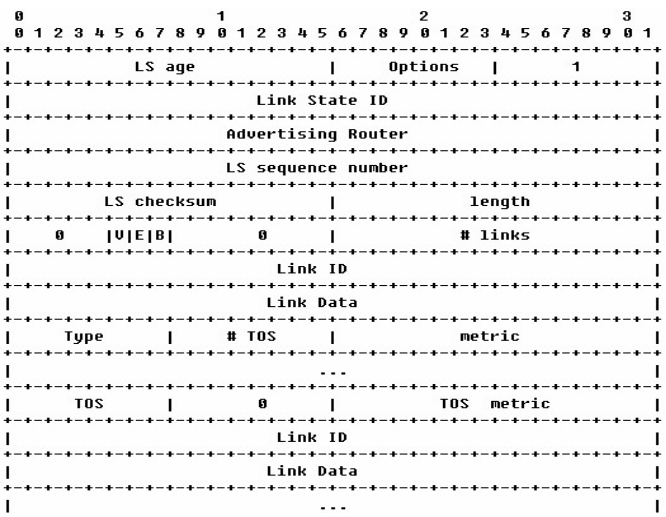

图 6-91 Router LSA 报文格式

- V，或虚链路端点位：设置 1 时，说明始发路由器是一条或多条具有完全邻接关系的虚链路的一个端点，则该区域是传送区域。
- E，或外部位：当始发路由器是一个 ASBR 路由器时，设置该位为 1。

- B，或边界位：当始发路由器是一个 ABR 路由器时，设置该位为 1。
- 链路数量：标明一个 LSA 所描述的路由器链路数量。对于 LSA 进行泛洪的区域，路由器 LSA 必须描述始发路由器的所有链路或接口。
- Type：字段中是对该链路信息的类型描述
  - 链路类型 1：点到点连接到另一台路器（Point-to-point connection to another router）：对于该类型一般出现在 OSPF P-T-P，其中 Link ID 为对端的 ROUTER-ID；Link Data 为本端的出接口地址。它描述要到达对方（ROUTER-ID），从我本端的那个出接口出去。
  - 链路类型 2：连接到一个传送网络（Connection to a transit network）：对于该类型一般出现在 OSPF NBMA BROADCAST，其中 Link ID 为 DR 的接口地址；Link Data 为本端到达 DR 的出接口地址。它描述的是如何到达我本链路上的 DR。
  - 链路类型 3：连接到一个末稍网络（Connection to a stub network）：对于该类型一般出现在 OSPF P-T-P LOOPBACK P-T-M，其中 Link ID 为该接口 IP 地址的网络前缀；Link Data 为接口 IP 地址的掩码。它描述一个末梢网络。
  - 链路类型 4：虚链路（Virtual link）：对于该类型出现在配置虚链路时出现的，其中 Link ID 为虚链路对方路由器的 router-id；Link Data
- Link ID：用来标识链路连接的对象，当连接的对象是一台路由器时，链路 ID 和在邻居路由器的 LSA 头部的链路状态 ID 是相同的。在计算路由选择表的期间，这个值可以用来发现链路状态数据库中邻居的 LSA。
- 链路数据：也是依赖于链路类型字段的值的字段。
  - 链路类型 1：链路数据字段的值为和网络相连的始发路由器接口的 IP 地址
  - 链路类型 2：链路数据字段的值为和网络相连的始发路由器接口的 IP 地址
  - 链路类型 3：链路数据字段的值为网络的 IP 地址或子网掩码
  - 链路类型 4：链路数据字段的值为始发路由器的接口的 MIB-II ifindex 值
- TOS：为列出这条链路指定服务类型度量的编号。虽然 RFC2328 已经不再支持 TOS，但为了同前兼容早期部署的 OSPF，仍旧保留这个字段。
- 度量：指一条链路（接口）的代价。

类型 1 的 LSA 只在一个 area 里传播，不会穿越 ABR。描述了和路由器直接相连的链路集体状态信息。RID 鉴别类型 1 的 LSA，LSA 描述了链路的网络号和掩码（即 link ID）。另外类型 1 的 LSA 还描述了路由器是否是 ABR 或 ASBR 。如下图所示

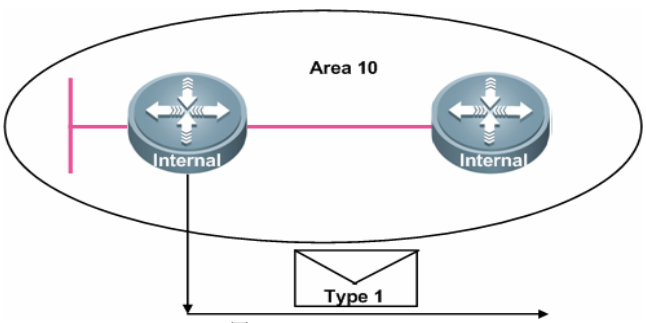

图 6-92 Router LSA

类型 1 的 LSA 不同的链路类型的 link ID 如下：

- point-to-point 的 link ID 是邻居的 RID
- transit network 的 link ID 是 DR 的接口地址
- stub network 的 link ID 是 IP 网络号
- virtual link 的 link ID 是邻居的 RID

每个路由器都产生 Router LSA，这种 LSA 描述了路由器所有的链路和接口、状态和开销。如下图所示。使用 RG-PATS 协议分析仪采集到类型 1 的 LSA：

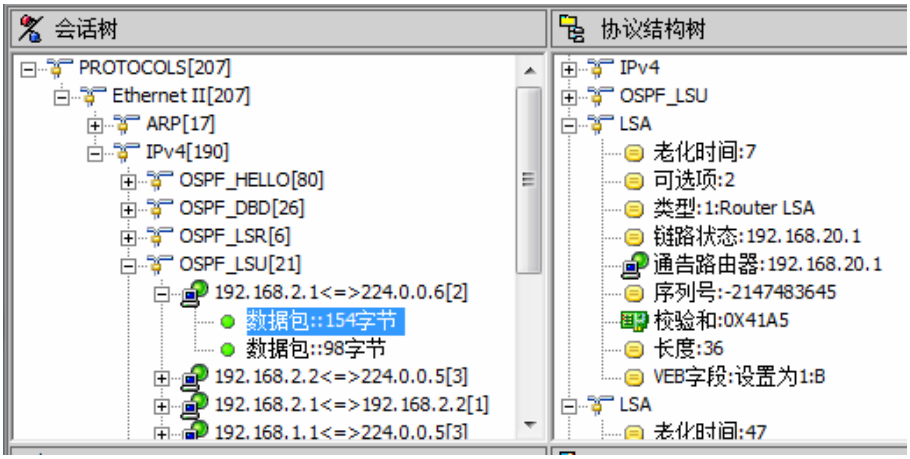

图 6-93 采集类型 1LSA 报文

2 类 LSA

2 类 LSA：Network LSA 为多路访问网络生成的网络链路通告，描述了特定多路访问网络上的一组路由器，网络链路通告在网络所在的区域内扩散。如下图所示 2 类 LSA 报文格式：

Network-LSAs 只有 OSPF Brocast and NBMA 网络类型才有。它与 OSPF Brocast and NBMA LSA 相结合，它描述一个 Transit Network 中有多少个网络节点 Attached to the network，包括 DR 自身。Network-LSAs 是由 DR 所产生的。

- Link state ID：网络 LSA 的链路状态 ID 是指网络中 DR 路由器接口上的 IP 地址。
- Network Mask：指定这个网络上使用的地址或子网的掩码。
- Attached Router：列出了网络上所有与 DR 形成完全邻接关系的路由器的路由器 ID，以及 DR 路由器本身的路由器 ID，表示 Transit Network 的节点，Router-id 标识。

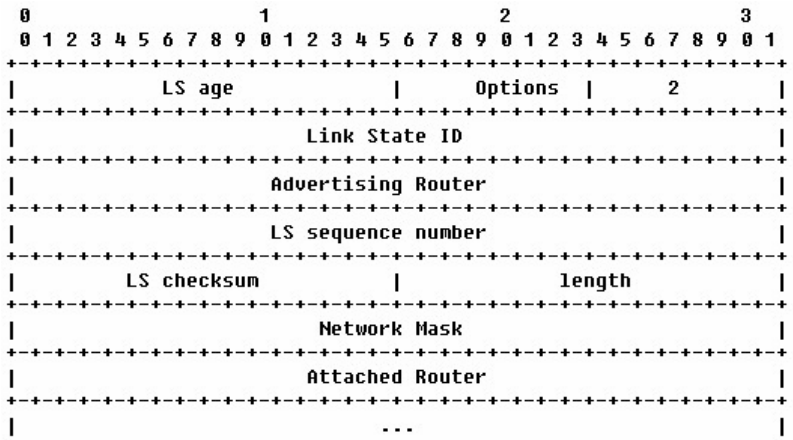

图 6-94 Network-LSAs 报文格式

2 类 LSA 的链路 ID 为 DR 的 IP 接口地址。类型 2 的 LSA 只在一个区域里传播，不会穿越 ABR。描述了组成 Transit Network 的直连的路由器，Transit Network 直连至少 2 台 OSPF 路由器。DR 负责宣告类型 2 的 LSA，然后在 transit network 的一个 area 里进行洪泛。如下图所示。

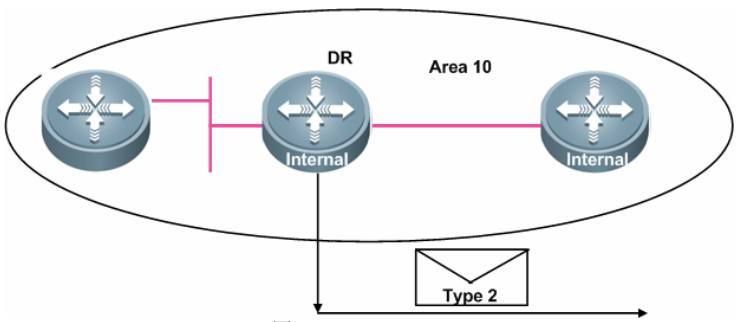

图 6-95 Network LSA

使用 RG-PATS 协议分析仪采集到类型 2 的 LSA：

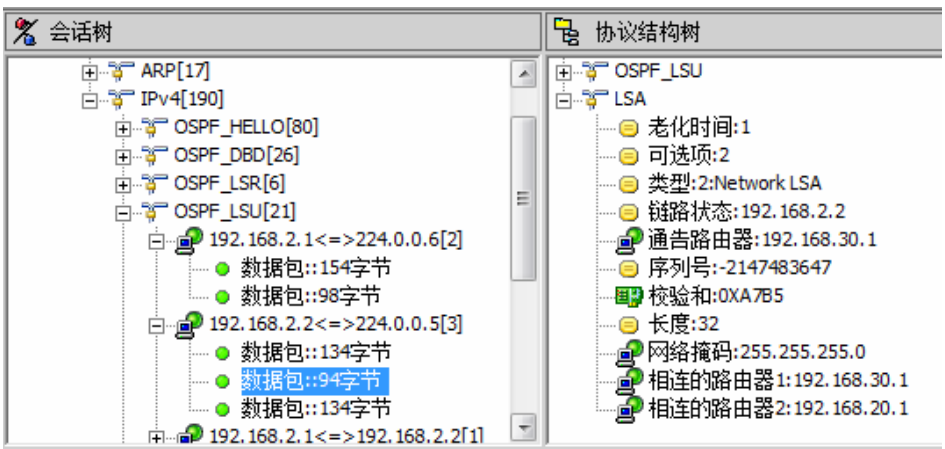

图 6-96 采集到的 network LSA

3 类 LSA

3 类的 LSA：Network Summary LSA 是由 ABR 生成的，报文格式如下图所示：

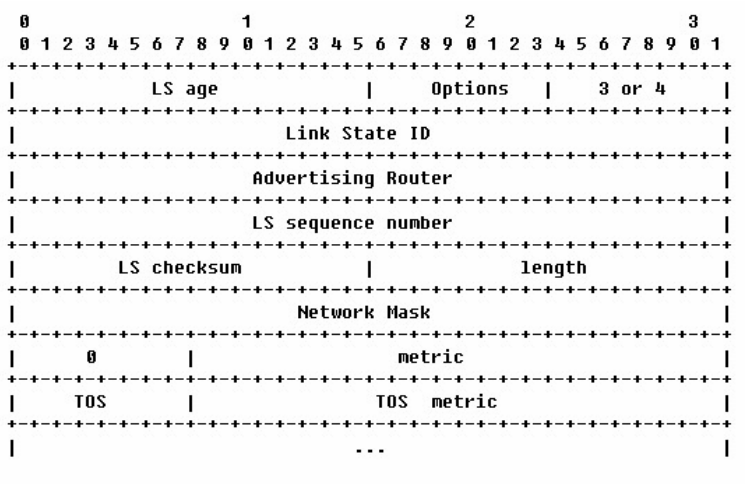

图 6-97 Network Summary-LSAs

- Link state ID：对于类型 3 的 LSA 来说，它是所通告的网络或子网的 IP 地址。
- Network Mask：在类型 3 的 LSA 中，是指所通告的网络的子网掩码或地址。如是一条类型 3 的 LSA 通告是一条缺省路由，那链路状态 ID 和网络掩码字段都将是 0.0.0.0。
- Metric：是指到达目的地的路由代价。

3 类 LSA 是由 ABR 所产生，它描述如果到达该区域的目的网段，将区域内的 1 类 LSA 和 2 类 LSA 结合起来算出路由，再将其转成 3 类 LSA。如果一个区域有两个 ABR，他们都会执行转换，如果到这两个 ABR 的 COST 都相同的话，都负载均衡的状态。

注意无论是 3 类 LSA 还是 4 类 LSA 的，如果是穿越某个区域的 ABR 到达该域内，LSA3/LSA4 的 Advertising Router 都会被改写成该区域的 ABR。也就是说某一域内收到 LSA3/LSA4 的 LSA 都是由该区域的 ABR 所产生的。

它将一个区域内的网络通告（路由信息）给 OSPF AS 中的其他区域。如下图所示：

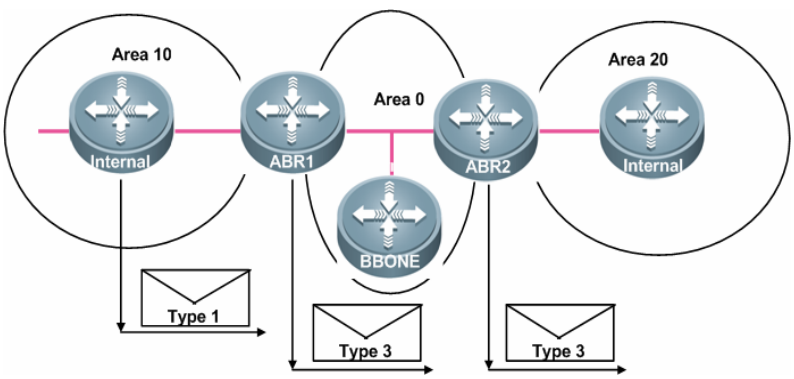

图 6-98 Network Summary LSA

LSA 都将扩散汇总到整个 AS。LINK ID 为目标网络网络地址。.默认 OSPF 不会对连续子网进行汇总。可在 ABR 上进行人工设定启用汇总。

如果 ABR 知道有多条路径可以到达目标地址，但是它仍然只发送单个的 Network Summary LSA，并且是开销最低的那条，同样，如果 ABR 从其他的 ABR 那里收到多条 Network Summary LSA 的话，它会只选择开销最低的，并把这条 Network Summary LSA 宣告给其他区域。如下图所示。

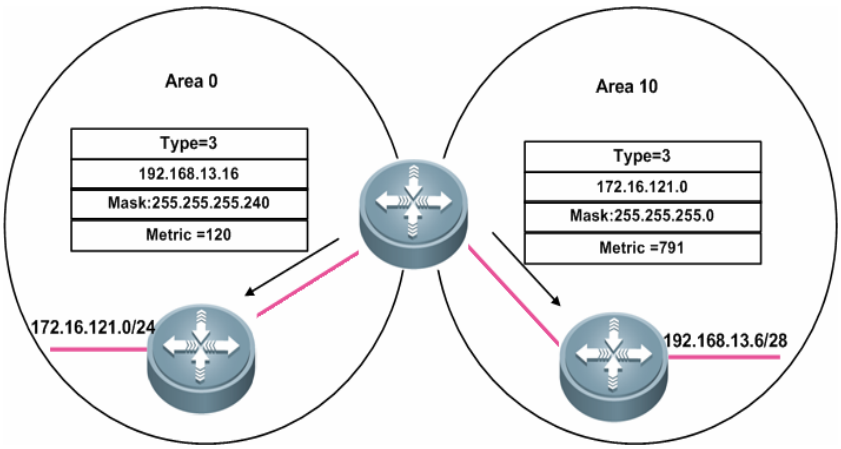

图 6-99 Network Summary LSA 传播

当其它的路由器收到来自 ABR 的 Network Summary LSA 以后，它不会运行 SPF 算法，它只简单的加上到达那个 ABR 的开销和 Network Summary LSA 中包含的开销，通过 ABR 到达目标地址的路由和开销一起被加进路由表里，这种依赖中间路由器来确定到达目标地址的完全路由实际上是距离矢量路由协议的行为。

使用 RG-PATS 协议分析仪采集到类型 3 的 LSA：

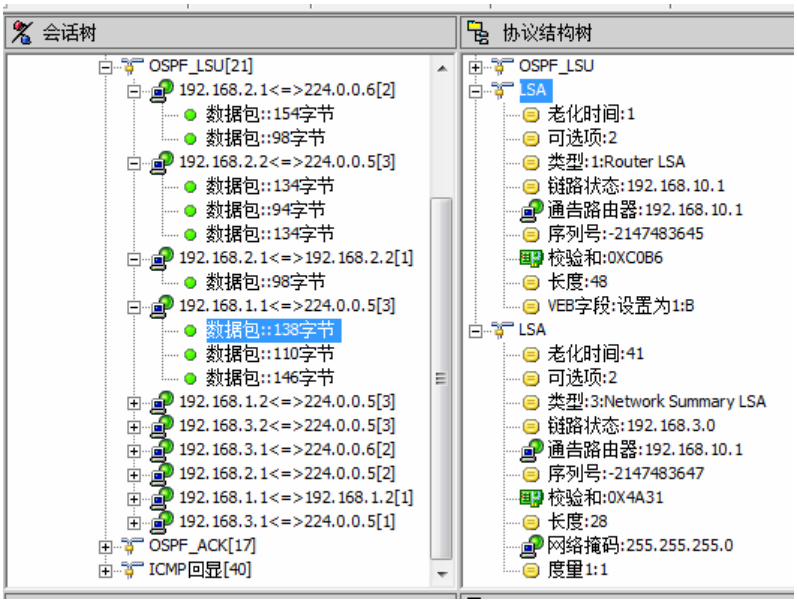

图 6-100 采集类型 3LSA 报文

4 类 LSA

4 类 LSA：ASBR summary LSA，仅当区域中存在 ASBR 时，才会使用 4 类 LSA，类型 4 的 LSA 由 ABR 生成，并在整个 AS 里进行洪泛。报文格式如下图所示。

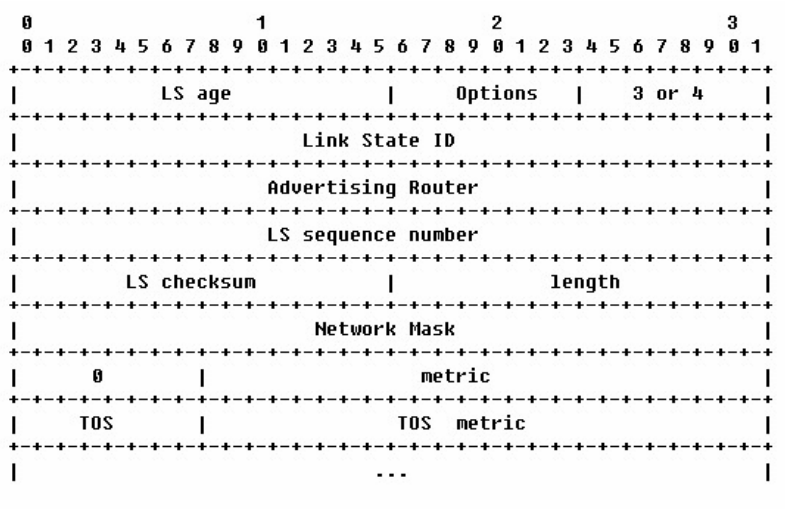

图 6-101 ASBR Summary-LSAs

- Link state ID：对于类型 4 的 LSA 来说，链路状态 ID 是所通告的 ASBR 路由器的路由器 ID。
- Network Mask：在类型 4 的 LSA 中，这个字段没有什么意义，并被设置为 0.0.0.0。如是一条类型 3 的 LSA 通告是一条缺省路由，那链路状态 ID 和网络掩码字段都将是 0.0.0.0。
- Metric：是指到达目的地的路由代价。

4 类 LSA 标识 ASBR，并提供一条前往 ASBR 的路由，链路状态 ID 被设置为 ASBR 的路由器 ID。前往外部 AS 的数据流要求路由选择表中包含有关通告外部路由的 ASBR 的信息。如下图所示：

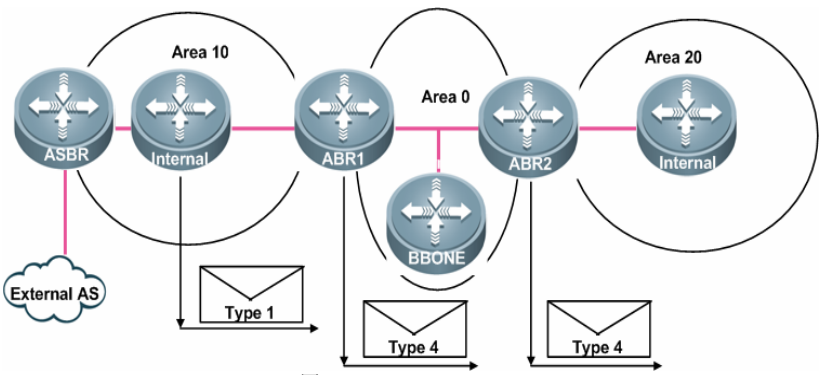

图 6-102 Summary LSA

使用 RG-PATS 协议分析仪采集到类型 4 的 LSA：

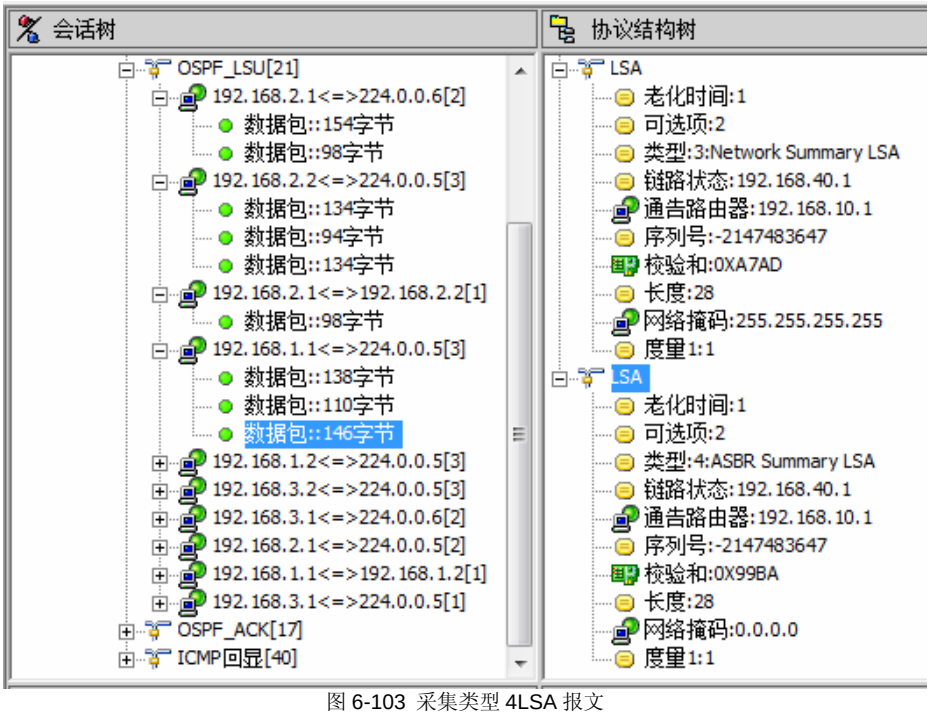

图 6-103 采集类型 4LSA 报文

5 类 LSA

5 类 LSA：Autonmous system external LSA，描述了前往 OSPF AS 外部的网络路由。下图所示 5 类 LSA 报文格式：

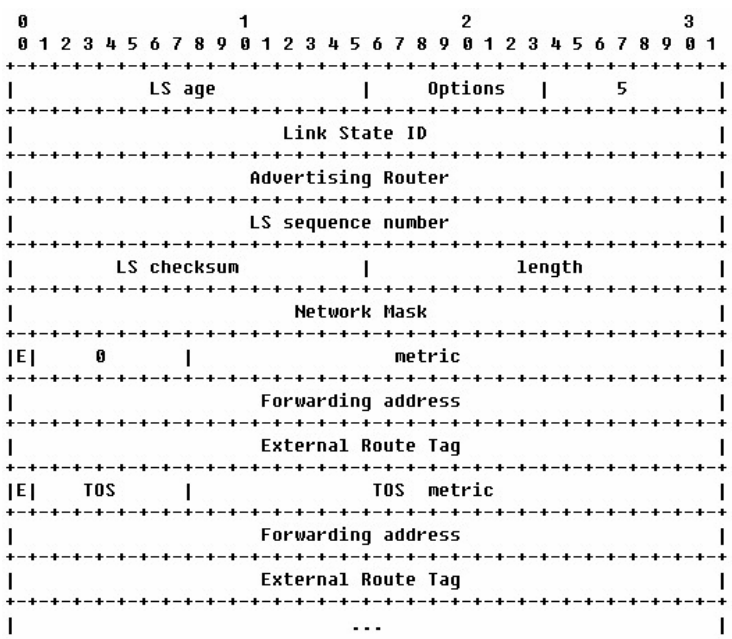

图 6-104 AS-external-LSAs 报文格式

- Link state ID：自治系统外部 LSA 的链路状态 ID 是指目的地的 IP 地址。
- Network Mask：是指所通告的目的地的子网掩码，如果类型 5 的 LSA 正在通告一条缺省路由，那么链路状态 ID 和网络掩码字段都将被设置为 0.0.0.0
- E，或外部度量位：用来指定这条路由使用的外部度量的类型。如果该 E 位设置为 1，那么度量类型是 E2，如果 E 位设置为 0，那么度量类型就是 E1。
- Metric：是指路由的代价，由 ASBR 路由器设定。
- Forwarding Address：转发地址，是指到达所通告的目的地的数据包应该被转发到的地址。如果转发地址是 0.0.0.0，那么数据包将被转发到始发 ASBR 上。
- External route tag：外部路由标志，是一个应用于外部路由的任意标志，OSPF 协议本身并不使用这个字段，而是由外部路由管理和控制。

5 类 LSA 由 ASBR 生成，并在整个 AS 内洪泛。鉴于其扩散，应该进行路由汇总。以缓解扩散问题。如下图所示。

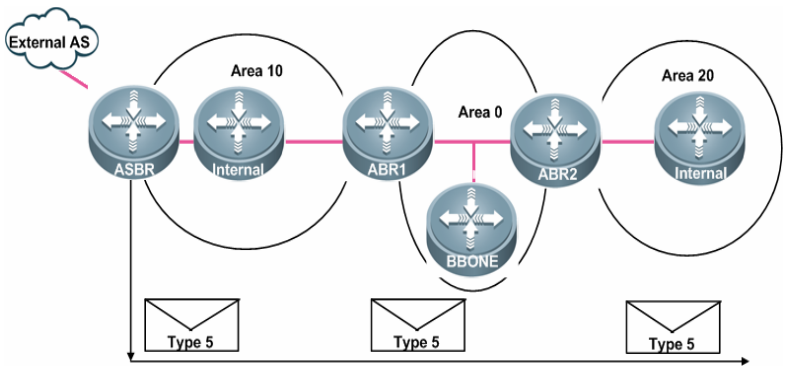

图 6-105 Autonmous system external LSA

使用 RG-PATS 协议分析仪采集到类型 5 的 LSA：

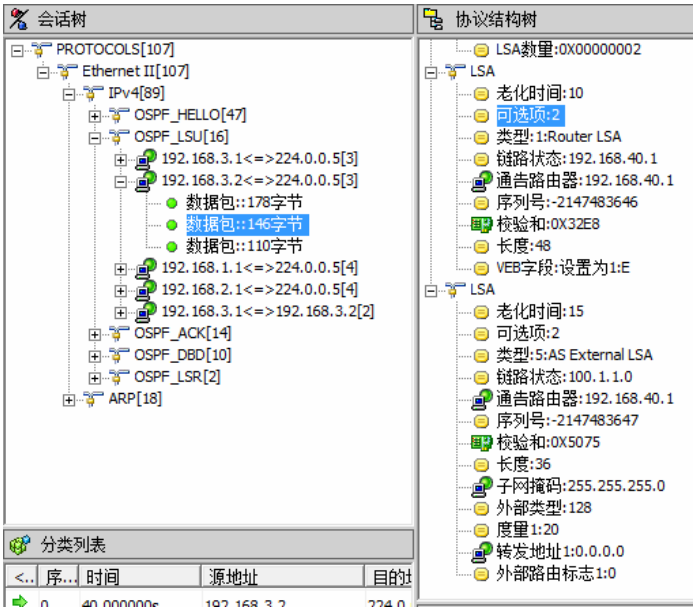

图 6-106 采集类型 5LSA 报文

7 类 LSA

7 类 LSA：NSSA 外部 LSA 是由一个 NSSA 区域内的 ASBR 路由器始发的，如下图所示，除了转发地址段外，NSSA 外部 LSA 的所有字段都是和一个 AS 外部 LSA 的字段相同的，不像 AS 外部 LSA 那样是在整个 OSPF 自治系统中进行泛洪的，NSSA 外部 LSA 仅仅在始发它们的一个非纯末稍区域中进行泛洪。

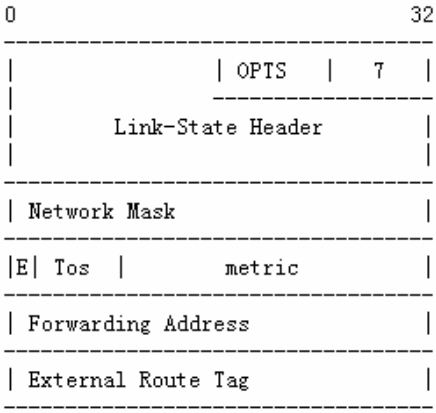

图 6-107 7 类 LSA 报文格式

转发地址：如果网络是在一个 NSSA ASBR 路由器和邻接的自治系统之间是作为一条内部路由通告的，那么这个转发地址就是指这个网络的下一跳地址。如果网络不是作为一条内部路由通告的，那么这个转发地址将是 NSSA ASBR 路由器的路由器 ID。

使用 RG-PATS 协议分析仪采集到类型 7 的 LSA：

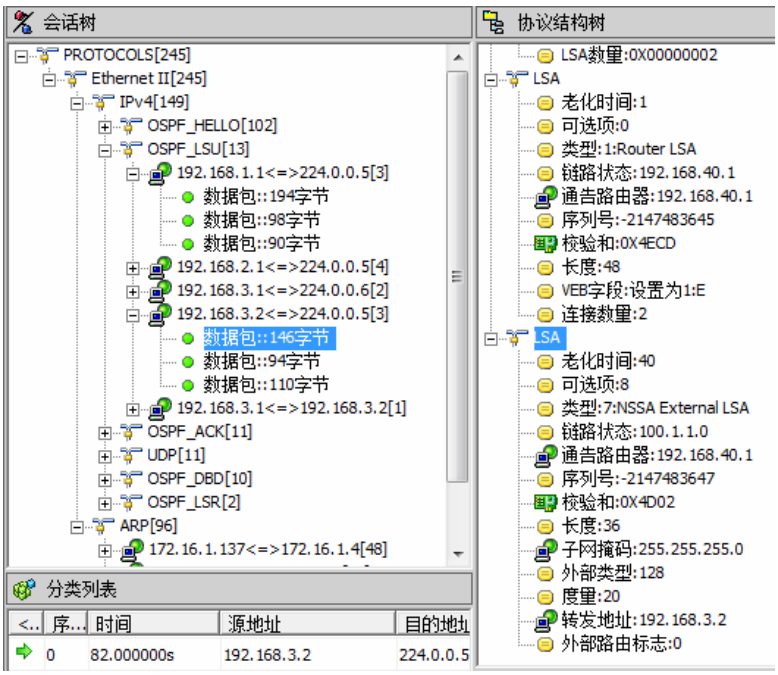

图 6-108 采集类型 7LSA 报文

选项字段：

在各类的 LSA 报文中都关于选项的字段，下面是关于选项字段的介绍：

*	O	DC	EA	N/P	MC	E	T

图 6-109 选项字段格式

- * ：表示这一位是不使用的，通常设置为 0。

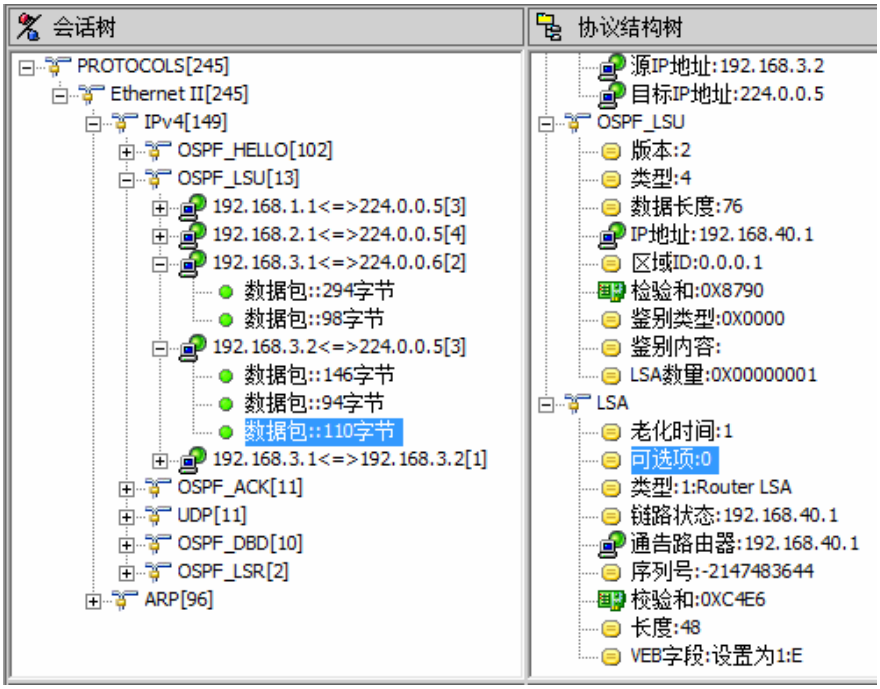

图 6-110 LSA 报头可选项

- O：比特用于不透明的 LSA（Opaque LSA）在 RFC2370 中提及。
- DC：用于请求线路（Demand circuit）的性能，也就是说具有按需电路上的 OSPF 能力时，在 RFC1793 中提及。
- EA：是外部特征。
- N/P： N 位只用在 Hello 报文中，一台路由器设置 N＝1 表明它支持 NSSA 外部 LSA。如果设置 N＝0，那路由器将不接受和发送 NSSA 外部 LSA。邻居如果错误配置了 N 位将不会形成邻居关系，这个限制可以确保一个区域内的所有路由器都同样具有支持 NSSA 的能力，如果 N＝1，那么 E 位必须设置为 0。P 位只用在 NSSA 外部 LSA 的头部（由于这种情况，N 和 P 可以使用在同一位置）。将告诉一个非完全末稍区域中的 ABR 路由器将类型 7 的 LSA 转换成类型 5 的 LSA。在 RFC1587 中提及。

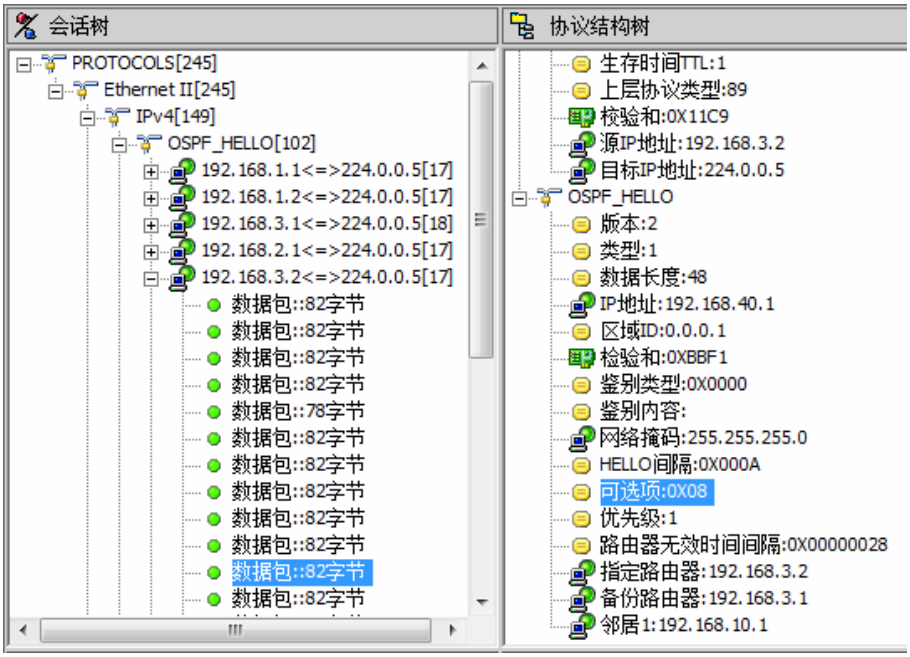

图 6-111 Hello 报文可选项

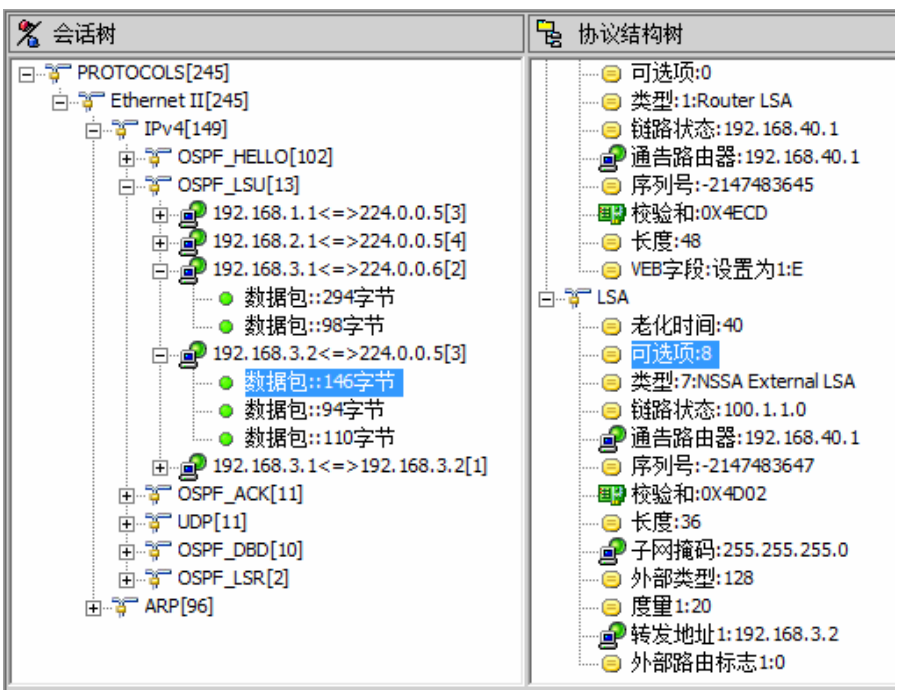

图 6-112 LSA 报文可选项

- MC：指多播 OSPF。
- E：当设置时，表示在这个区域中允许出现外部 LSA。当始发路由器具有接受 AS 外部 LSA 的能力时，该位将设置为 1。而在所有始发于末稍区域的 LSA 中，该位

设置为 0。另外，可以在 Hello 报文中使用该位来表明一个接口具有接收和发送类型 5 的 LSA 的能力。E 配置错误的邻居路由器将不能形成邻接关系，这个限制可以确保一个区域的所有路由器都同样具有支持末稍区域的能力。

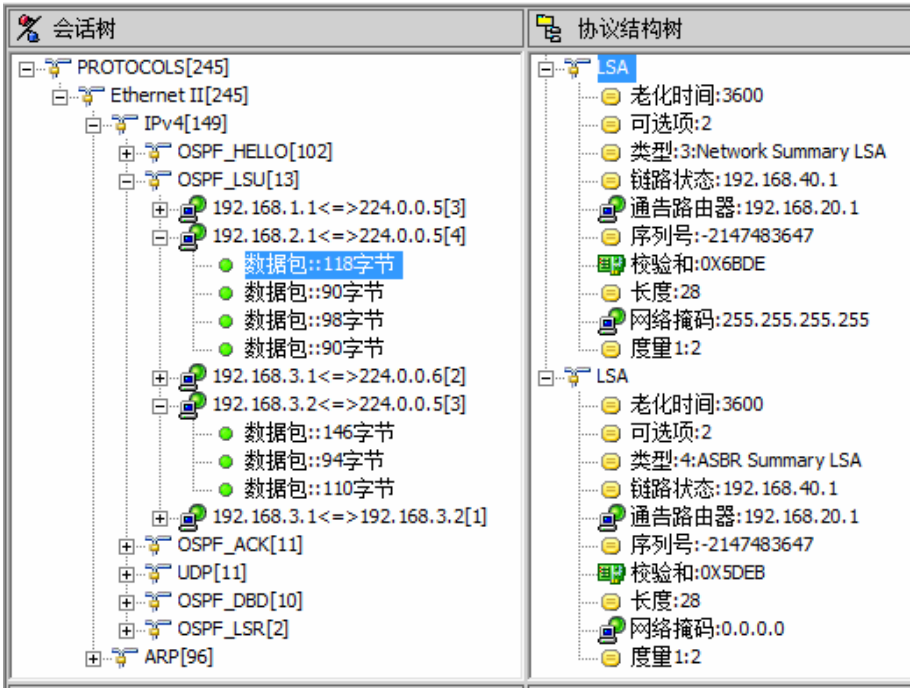

图 6-113 LSA 报文可选项

- T 比特用于 TOS 特性，（通常设置为 0）。

【实验步骤】

步骤一：设定实验环境

1、配置端口映射

S3750#
S3750#configure terminal
S3750(config)#monitor session 1 destination interface FastEthernet 0/24
S3750(config)#monitor session 1 source interface FastEthernet 0/1 – 10 both

2、在路由器上配置 OSPF 路由协议

RA(config)#interface FastEthernet 0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config)#interface FastEthernet 0/1

```
RA(config-if)#ip address 192.168.3.1 255.255.255.0
RA(config)#interface Loopback 0
RA(config-if)#ip address 192.168.10.1 255.255.255.0
RA(config)#router ospf 10
RA(config-route)#network 192.168.1.0 0.0.0.255 area 0
RA(config-route)#network 192.168.3.0 0.0.0.255 area 1
RA(config-route)#network 192.168.10.0 0.0.0.255 area 0

RB(config)#interface FastEthernet 0/0
RB(config-if)#ip address 192.168.1.2 255.255.255.0
RB(config)#interface FastEthernet 0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config)#interface Loopback 0
RB(config-if)#ip address 192.168.20.1 255.255.255.0
RB(config)#router ospf 10
RB(config-route)#network 192.168.1.0 0.0.0.255 area 0
RB(config-route)#network 192.168.2.0 0.0.0.255 area 2
RB(config-route)#network 192.168.20.0 0.0.0.255 area 0

RC(config)#interface FastEthernet 0/0
RC(config-if)#ip address 192.168.2.2 255.255.255.0
RC(config)#interface Loopback 0
RC(config-if)#ip address 192.168.30.1 255.255.255.0
RC(config)#interface Loopback 1
RC(config-if)#ip address 172.16.1.1 255.255.255.0
RC(config)#interface Loopback 2
RC(config-if)#ip address 172.16.2.1 255.255.255.0
RC(config)#router ospf 10
RC(config)#network 172.16.1.0 0.0.0.255 area 2
RC(config-route)#network 172.16.2.0 0.0.0.255 area 2
RC(config-route)#network 192.168.2.0 0.0.0.255 area 2
RC(config-route)#network 192.168.30.0 0.0.0.255 area 2

RD(config)#interface FastEthernet 0/0
RD(config-if)#ip address 192.168.3.2 255.255.255.0
RD(config)#interface Loopback 0
RD(config-if)#ip address 192.168.40.1 255.255.255.0
RD(config)#interface Loopback 1
RD(config-if)#ip address 100.1.1.1 255.255.255.0
RD(config)#router ospf 10
RD(config-route)#network 100.1.1.0 0.0.0.255 area 1
RD(config-route)#network 192.168.3.0 0.0.0.255 area 1
RD(config-route)#network 192.168.40.0 0.0.0.255 area 1
```

步骤二：使用 RG-PATS 网络协议分析仪采集 OSPF 报文

当前拓扑是一个多路访问的网络，当拓扑中的路由器启动后，所有路由器的 OSPF 路由协议进程开始启动，以路由器 RA 和路由器 RA 为例，路由器 RA 变为有效状态，并会在其接口上发送 hello 报文，其目标地址为 224.0.0.5，由于其还没有学习到任何邻居，因而这个 hello 报文的邻居字段为空，而 DR 和 BDR 字段设置为 0.0.0.0。其报文格式如下图所示：

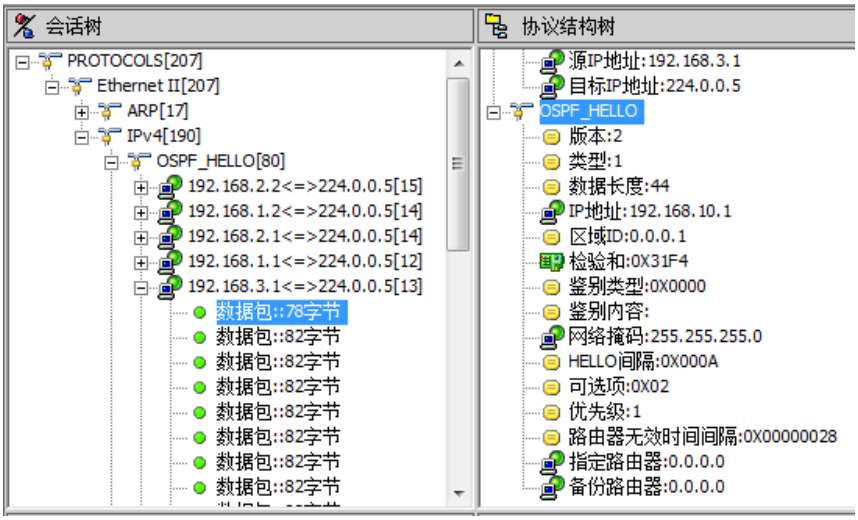

图 6-114 采集到的 Hello 报文

其 RID 为 192.168.10.1，因为这是其 loopback0 的接口地址。其鉴别类别为 0，表示没有认证；hello 间隔为 10 秒，失效时间间隔为 40 秒，优先级为 1。

当路由器 RD 收到路由器 RC 的 hello 报文时，路由器 RD 就会创建一个邻居数据结构，并将路由器 D 的状态设置为初始状态（Init）。路由器 RD 将发送一个 hello 报文给路由器 RA，并将这个 hello 报文的邻居字段里设置路由器 RA 的路由器 ID。其报文格式如下图所示：

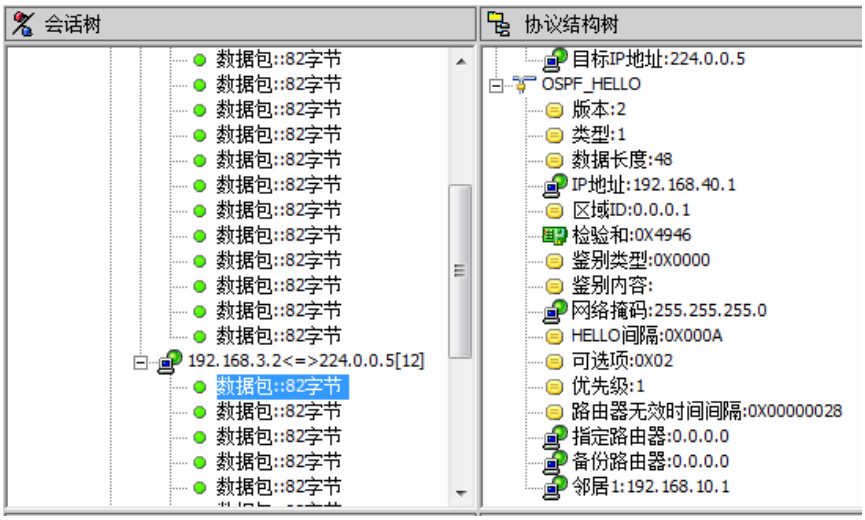

图 6-115 报文中的 RID

其 RID 为 192.168.40.1，其鉴别类别为 0，表示没有认证；hello 间隔为 10 秒，失效时间间隔为 40 秒，优先级为 1。

路由器 RD 和路由器 RA 通过检查区域 ID、hello 间隔、hello 失效时间间隔、认证、stub 标志位都相同，刚两台路由器形成了邻居，这时为双向通信的关系（2－way）。

因为网络类型为多路访问网络，这时两台路由器需要选择 DR 和 BDR，根据 DR 选举的规则先选出 DR，如下图所示：

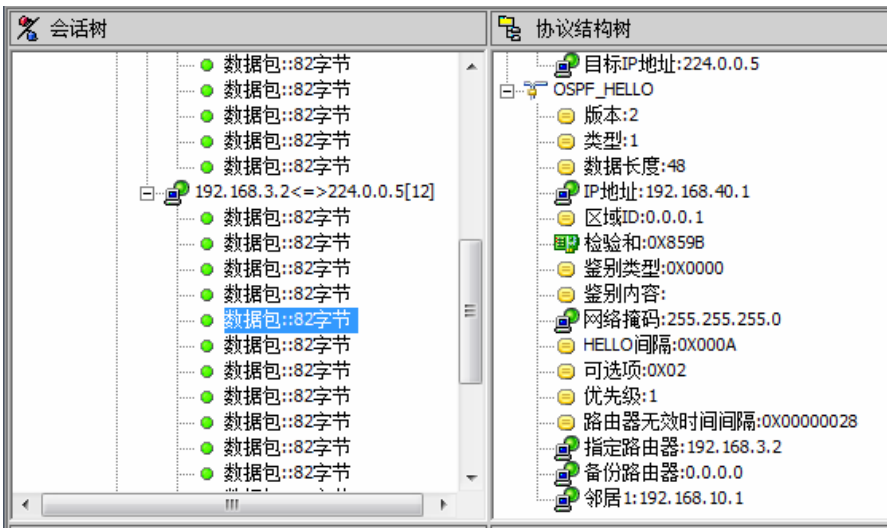

图 6-116 DR 选举

然后再选举出 BDR，如下图所示：

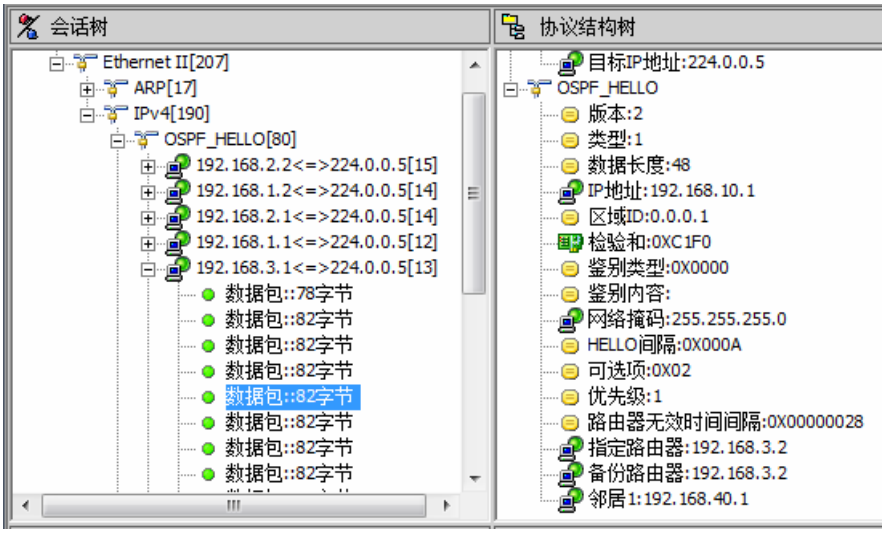

图 6-117 BDR 选举

当路由器 RA 接收到来自于路由器 RD 的 hello 报文，并看到自己的路由器 ID 时，路由器 RA 将为路由器 RD 创建一个邻接数据库结构，并把路由器 RD 的状态设置为 ExStsrt 状态，以便开始进行主/从关系的协商，接着路由器 RA 产生一个空的数据库描述报文，并把

数据库描述的序列号设置为 73，同时设置初始位（I 位）来说明这个报文是路由器 RA 用来进行本次信息交换的最初的数据库描述报文，并设置后继位（M 位）来说明这个报文不是最的数据库描述报文，最后还要设置主从位（MS 位）来说明路由器 RA 声称自己是“主”路由器。如下图所示：

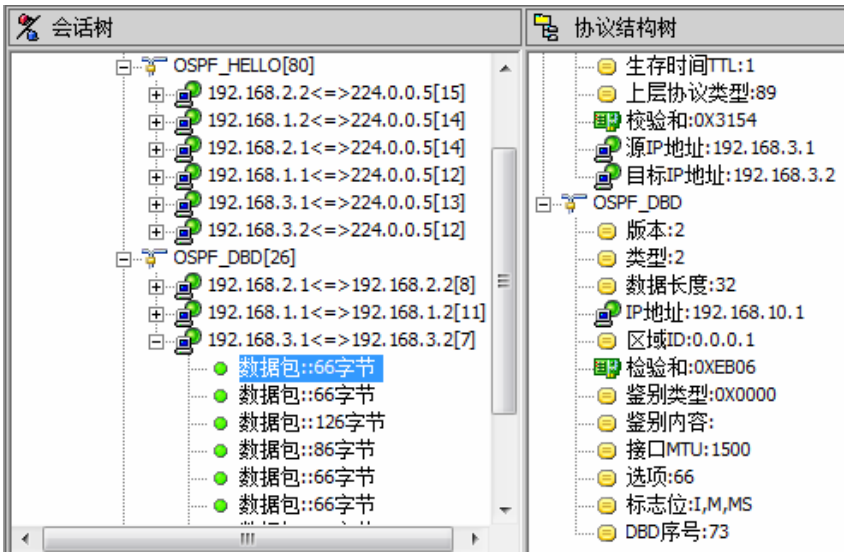

图 6-118 主路由器选举

路由器 RD 一旦收到来自路由器 RA 的数据库描述报文，就会把路由器 RA 的状态转换到 ExStsrt 状态，接着，它将发送一个响应的数据库描述报文，并把这个数据库描述报文的序列号设置为 74，由于路由器 RD 拥有比路由器 RA 更高的路由器 ID，因此它将把自己的 MS 位设置为 1。如下图所示：

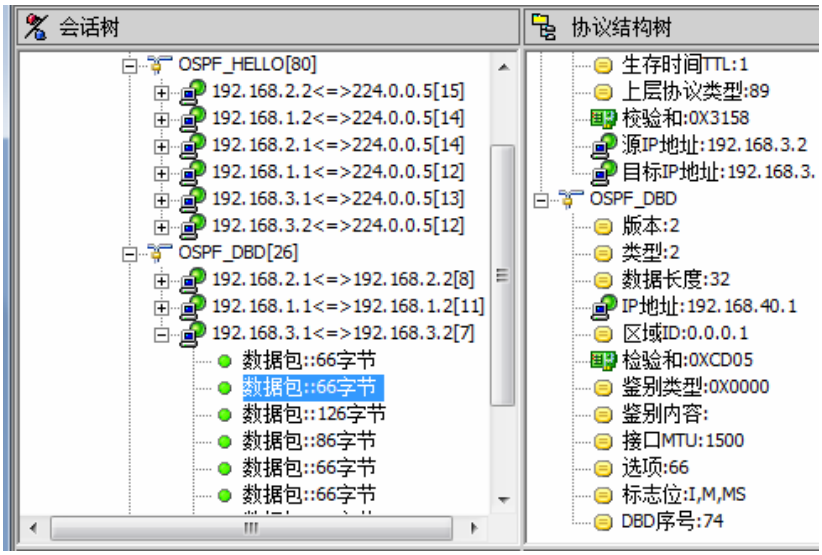

图 6-119 DBD 报文中的标志位

当这两台邻居路由器同意路由器 RD 是主路由器后，路由器 RA 就把路由器 RD 的状态

转换为 Exchange 状态。路由器 RA 将产生一个数据库描述报文，这个报文的序列号使用路由器 RD 的数据库描述报文的序列号 74，并设置 MS 位为 0 用来指明路由器 RA 是“从”路由器，同时，该报文会将会传送路由器 RA 的链路状态摘要列表中的 LSA 头部。如下图所示：

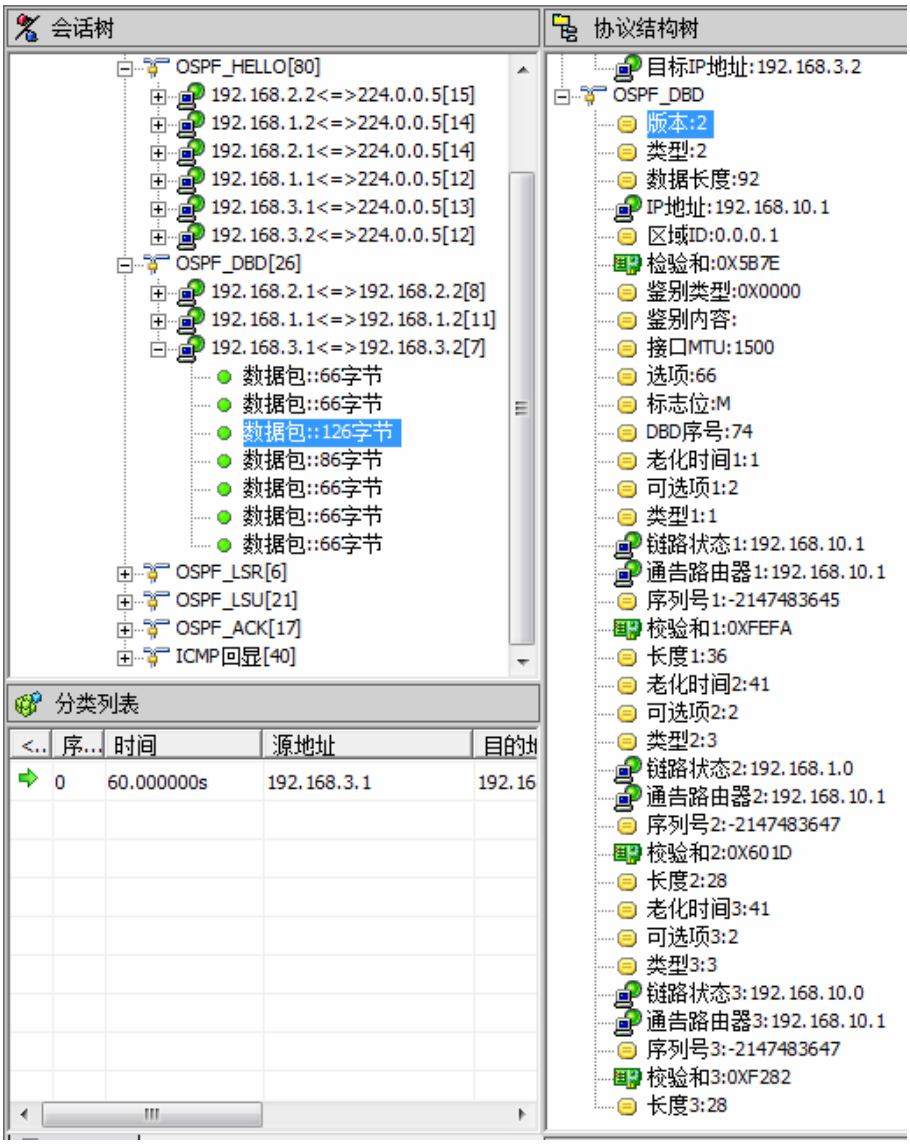

图 6-120 DBD 报文

路由器 RD 一旦收到来自于路由器 RA 的数据库描述报文，就会把它的邻居状态转换到 Exchange 状态。接着，它将发送一个数据库描述报文，这个报文包含路由器 RD 自己的链路状态摘要列表中的 LSA 头部，并使它的数据库描述序列号增加到 74＋1。如下图所示：

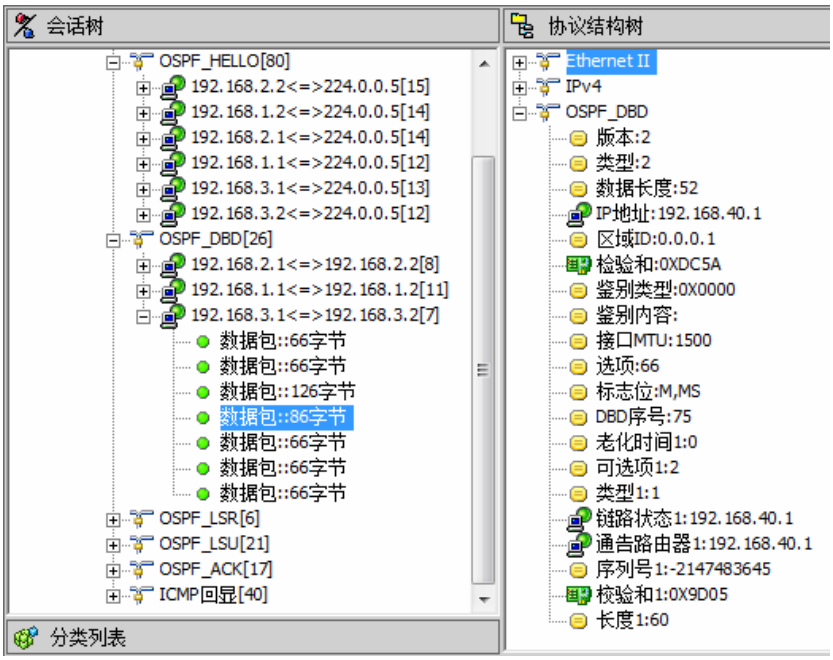

图 6-121 DBD 序列号

当路由器 RA 从路由器 RD 收到上述报文后，路由器 RA 就会发送一个包含相同序列号的确认报文，如下图所示：

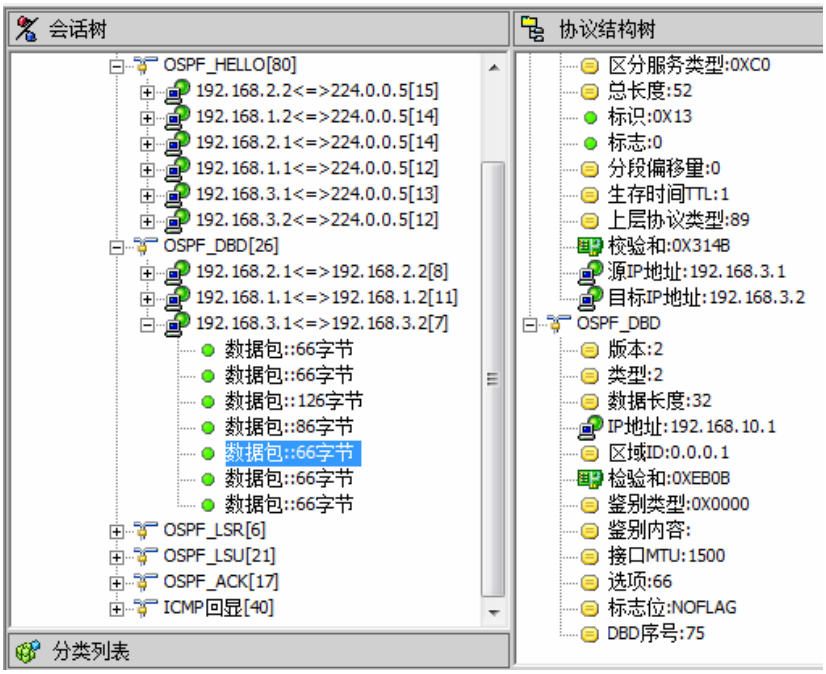

图 6-122 DBD 确认序列号

这个过程一直延续，路由器 RD 发送一个单一的数据库描述报文，接着等待从路由器 RA 发出的包含相同序列号的确认报文，然后路由器 RD 再发送一个数据库描述报文，直到

路由器 RD 发出包含最的一个 LSA 摘要的数据库描述报文，并把这个报文的 M 位设置为 0。如下图所示：

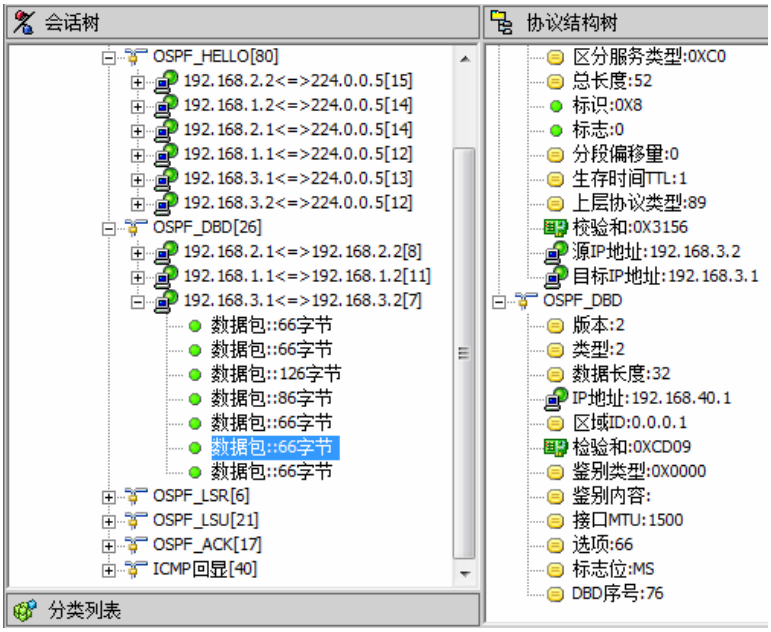

图 6-123 DBD 报文 M 位设置

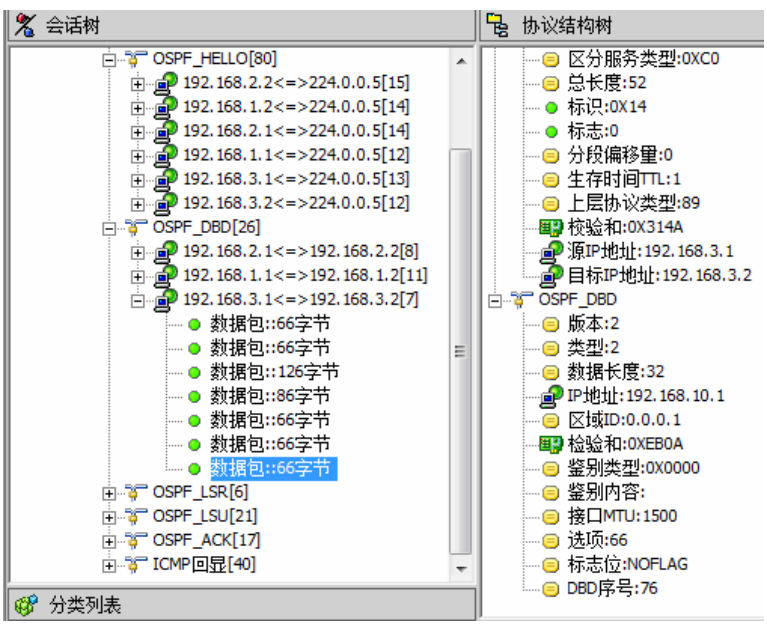

图 6-124 DBD 确认报文

收到上述这个报文，并且确认它所发出的确认报文中包含它自己的 LSA 摘要后，路由器 RA 就会认为 Exchange 状态已经完成，然而，路由器 RA 的链路状态请求列表中还存在 LSA 条目，因此，它将转换到信息加载状态（Loading）。

当路由器 RD 收到 RA 的最后一个数据库描述报文时，路由器 RD 将把路由器 RA 的状

态转换为完全邻接状态（Full），这是因为在它的链路状态请求列表中已经没有 LSA 条目了。

路由器 RA 根据数据描述报文得知，其没有关于链路状态类型为 1、链路状态 ID 为 192.168.40.1、通告路由器为 192.168.40.1 路由信息，则其发送链路请求报文 LSR，如下图所示：

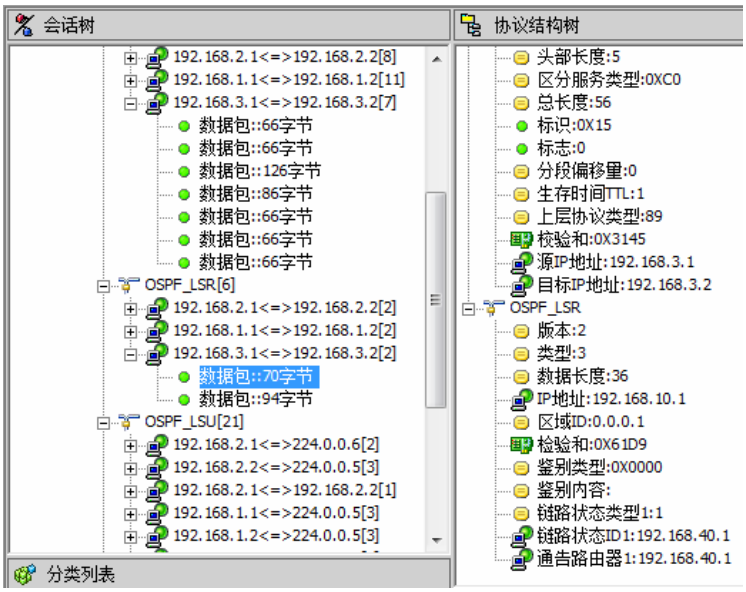

图 6-125 LSR 报文

同样路由器 RD 根据数据库描述报文得知，其没有多条关于链路状态类型为 1、3、链路状态 ID 为 192.168.10.1、通告路由器为 192.168.10.1 的路由信息，所以路由器 RD 也发送链路状态请求报文 LSR，如下图所示：

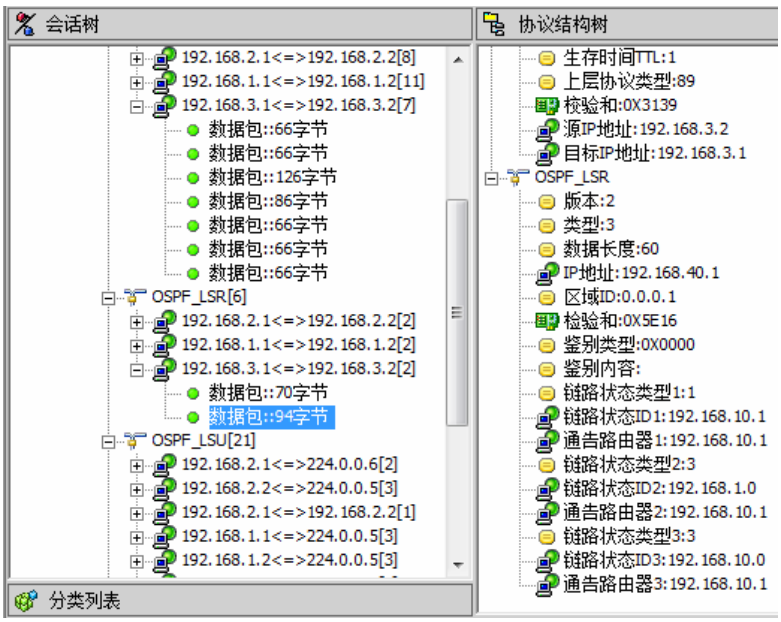

图 6-126 LSR 报文

路由器 RA 收到了路由器 RD 的链路请求报文，路由器 RD 用链路状态更新报文 LSU 发送关于请求路由更新详细信息，并创建序列号为 2147483645、2147483647 的 LSU 报文发送给路由器 RD，如下图所示：

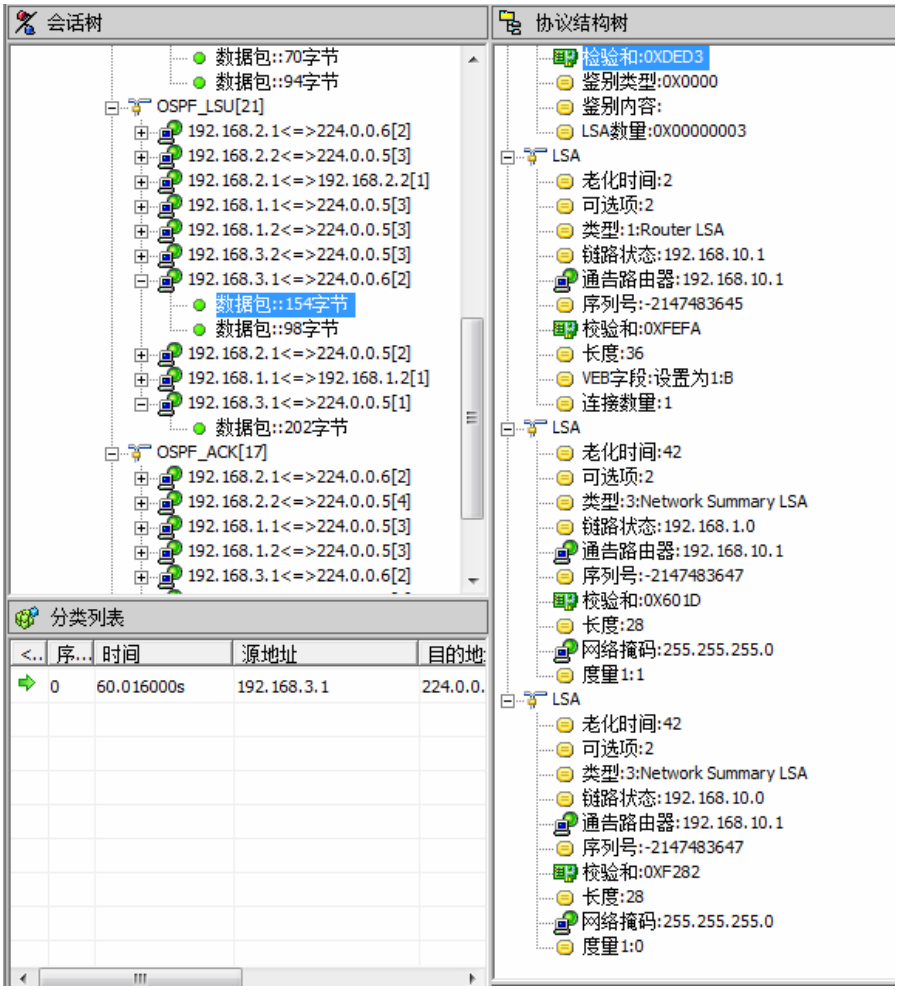

图 6-127 LSR 报文

当路由器 RD 收到了路由器 RA 的 LSU 报文后，并发送一个确认报文，序列号为请求报文中的序列号，如下图所示：

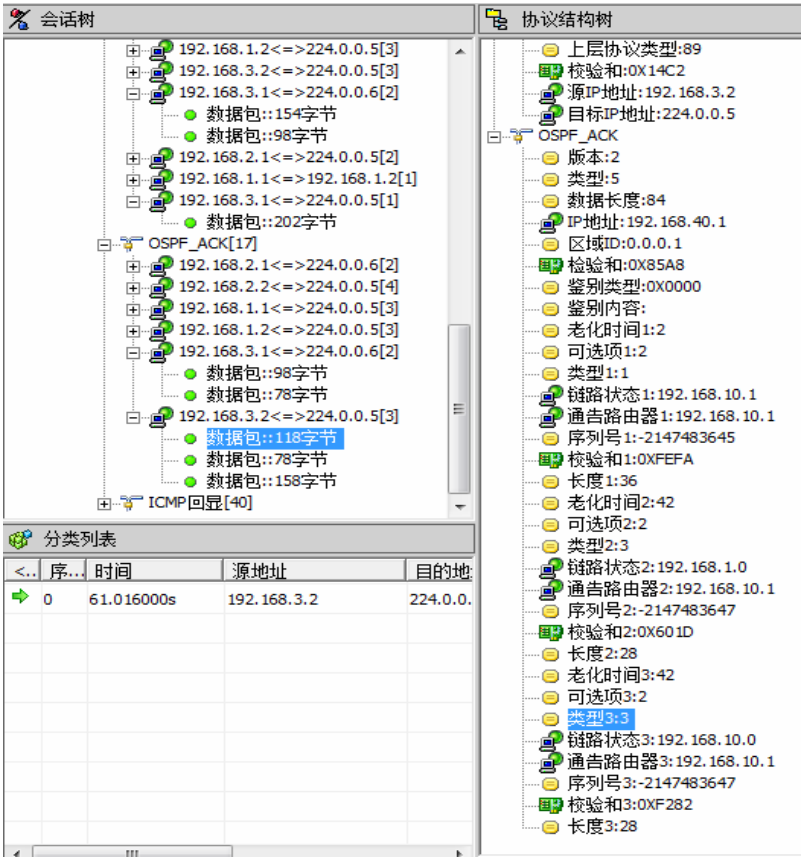

图 6-128 LSAck 报文

同样路由器RD收到了路由器RA的链路请求报文，路由器RA用链路状态更新报文LSU发送关于请求路由更新详细信息，并创建序列号为2147483644的LSU报文发送给路由器RA，如下图所示：

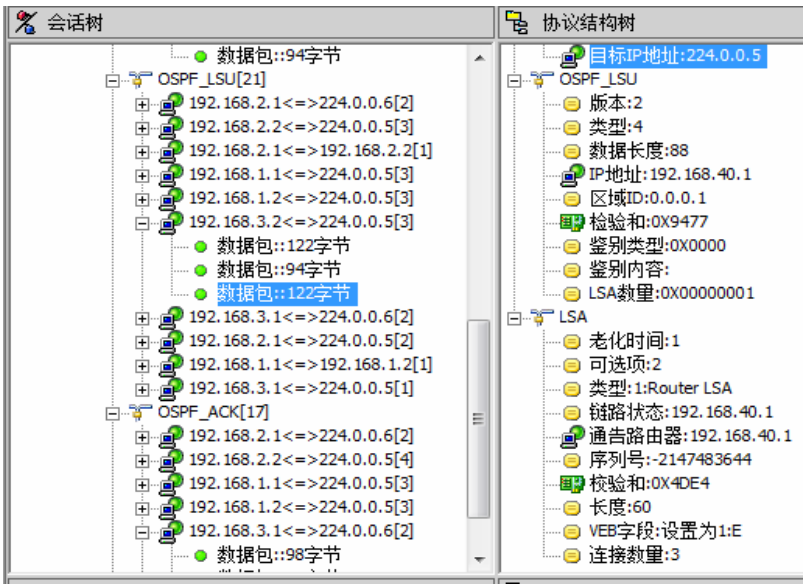

图 6-129 LSU 报文

当路由器 RA 收到了路由器 RD 的 LSU 报文后，并发送一个确认报文，序列号为请求报文中的序列号，如下图所示：

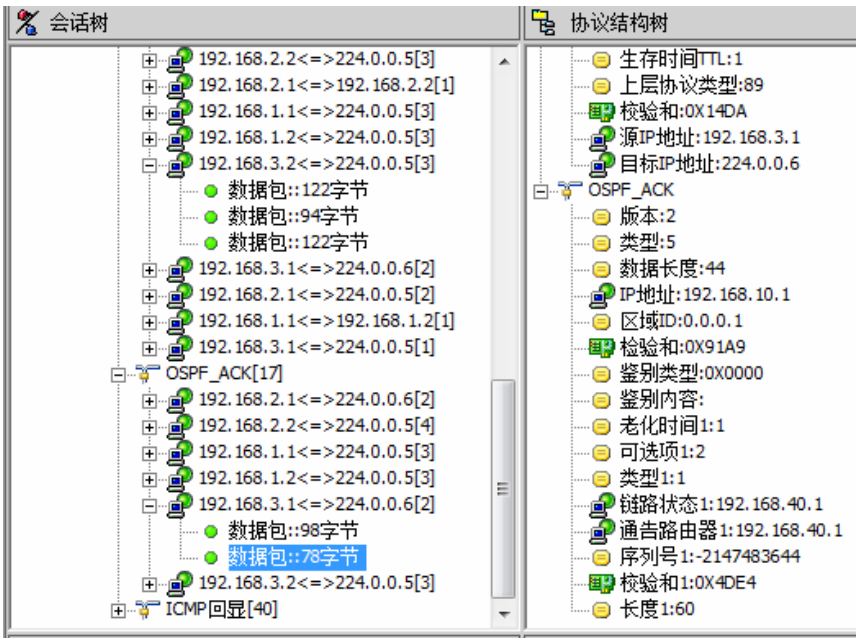

图 6-130 LSAck 报文

路由器 RA 发送链路状态请求报文，而且路由器 RD 通过链路状态更新报文发送被请求的 LSA 通告，这个过程一直持续到路由器 RA 的链路状态列表变成空表，然后，路由器 RA 也将把路由器 RD 的状态转换为完全邻接状态。

步骤三：使用 RG-PATS 网络协议分析仪采集 5 类 LSA 报文

1、在路由器上配置路由重分发

修改路由器 RD 的配置：

```
RD(config)#router ospf 10
RD(config-route)#redistribute connected subnets
RD(config-route)# redistribute rip metric 50 subnets
RD(config-route)#network 192.168.3.0 0.0.0.255 area 1
RD(config-route)# network 192.168.40.0 0.0.0.255 area 1
RD(config)router rip
RD(config-route)#version 2
RD(config-route)#network 100.0.0.0
RD(config-route)#no auto-summary
RD(config-route)#redistribute ospf metric 4
```

2、采集 5 类 LSA 报文

下图是使用 RG－PATS 采集到的 5 类 LSA 报文：

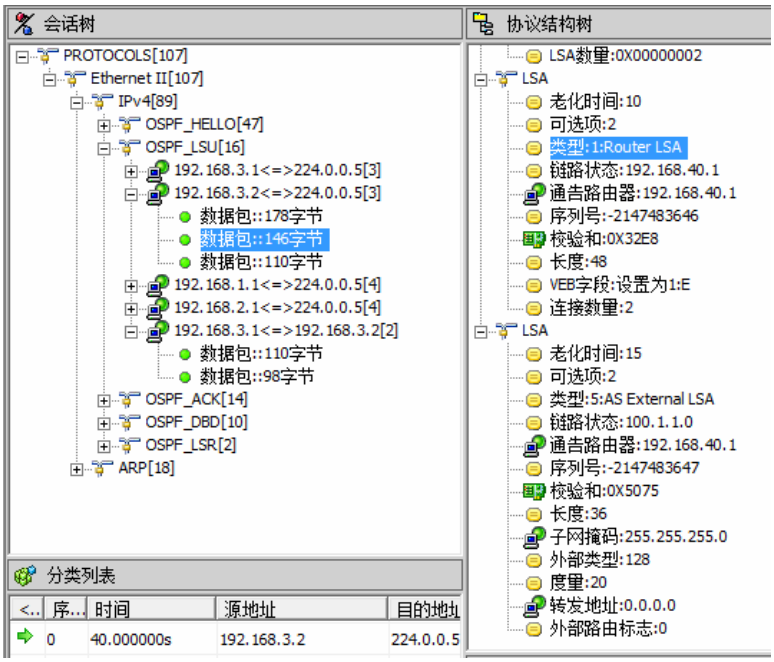

图 6-131 类型 5LSA 报文

路由器 RD 上配置了 RIPv2 路由协议，并重分发到 OSPF 路由协议中，路由器 RD 会向邻居发送一个 5 类 LSA。在 LSA 头部的选项中设置了 E 位，这说明本路由器是一台 ASBR 路由器，路由器发送的报文类型为 5 类 LSA，通告路由器 ID 为 192.168.40.1，外部路由类型是 E2 路由，转发地址是 0.0.0.0，那么数据包将被转发到始发 ASBR 上，度量值为 20。

同时路由器 RA 同样会向邻居发送一个 5 类的 LSA 报文，其度量值为 20，因为其用的是 E2 路由，并且还发送一个 4 类 LSA 报文告诉邻居去往 ASBR 的路由信息，如下图所示：

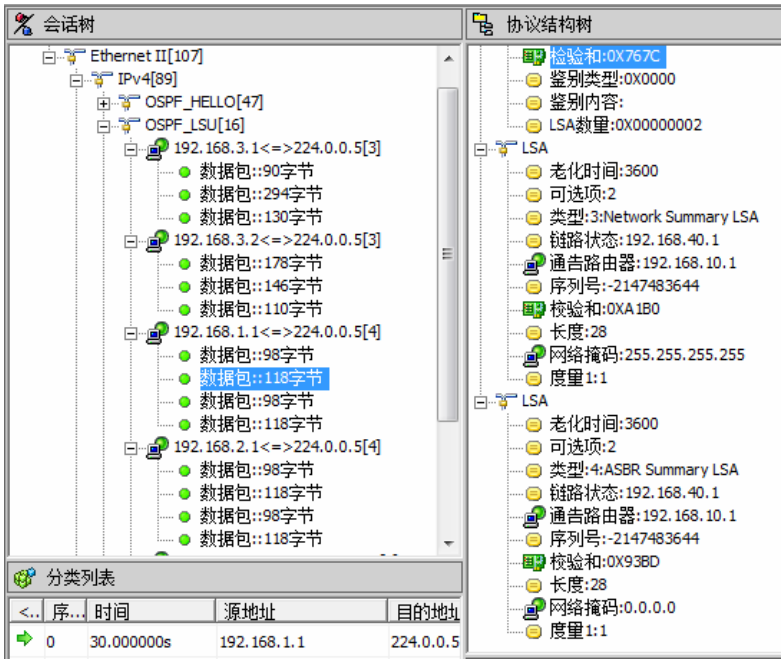

图 6-132 类型 5LSA 报文

在 4 类 LSA 中，Link state ID 设置为所通告的 ASBR 路由器的路由器 ID。网络掩码则被设置为 0.0.0.0。Metric 是到达目的地的路由代价为 1。

同样路由器 RB 收到 4 类和 5 类 LSA 报文后，也向其邻居发送 4 类和 5 类 LSA 报文，并且度量值 20。

步骤四：使用 RG-PATS 网络协议分析仪采集 7 类 LSA 报文

1、在路由器上配置 NSSA

修改路由器 RD 和路由器 RA 的配置：

```
RA(config)#router ospf 10
RA(config-route)#area 1 nssa
RA(config-route)#network 192.168.1.0 0.0.0.255 area 0
RA(config-route)#network 192.168.3.0 0.0.0.255 area 1
RA(config-route)#network 192.168.10.0 0.0.0.255 area 0
RD(config)#router ospf 10
RD(config-route)#redistribute connected subnets
RD(config-route)#redistribute rip metric 50 subnets
RD(config-route)#area 1 nssa
RD(config-route)#network 192.168.3.0 0.0.0.255 area 1
RD(config-route)#network 192.168.40.0 0.0.0.255 area 1
RD(config)#router rip
RD(config-route)#version 2
RD(config-route)#network 100.0.0.0
RD(config-route)#no auto-summary
RD(config-route)#redistribute ospf metric 4
```

2、采集 7 类 LSA 报文

下图是使用 RG－PATS 采集到的 7 类 LSA 报文：

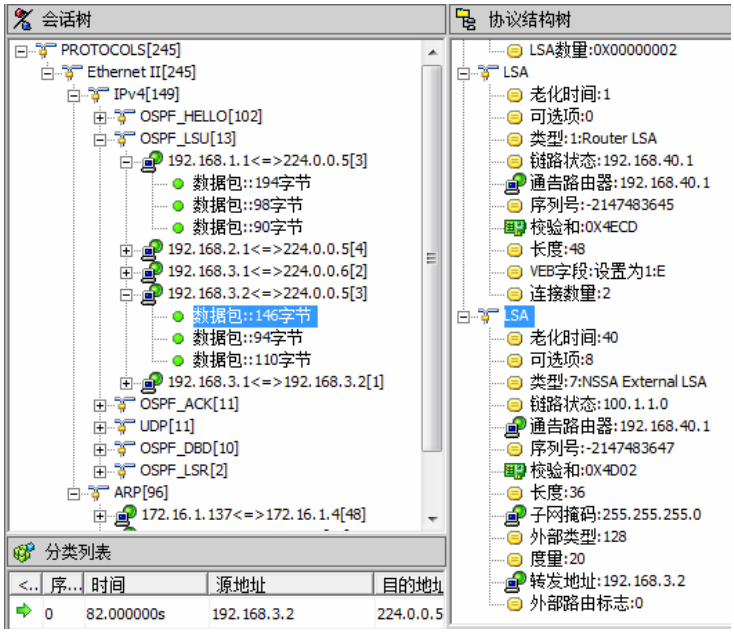

图 6-133 类型 7LSA 报文

在可选项字段中设置了 P 位，说明将告诉一个非完全末稍区域中的 ABR 路由器将类型 7 的 LSA 转换成类型 5 的 LSA。

而在转发地址字段中设置了 192.168.3.2，如果网络是在一个 NSSA ASBR 路由器和邻接的自治系统之间是作为一条内部路由通告的，那么这个转发地址就是指这个网络的下一跳地址。如果网络不是作为一条内部路由通告的，那么这个转发地址将是 NSSA ASBR 路由器的路由器 ID。

步骤五：使用 RG-PATS 网络协议分析仪编辑并发送 Hello 报文

打开 RG－PATS 网络协议分析仪的数据包发生器，编辑 OSPF Hello 报文，模拟路由器 RD 向邻居发送 OSPF Hello 报文，

在 RG-PATS 协议仪上打开数据包发生器，编辑一个 OSPF Hello 数据包。首先点击菜单栏“添加”，如下图所示：

图 6-134 添加报文

添加一个 OSFP Hello 协议模板，点击确认添加，如下图所示：

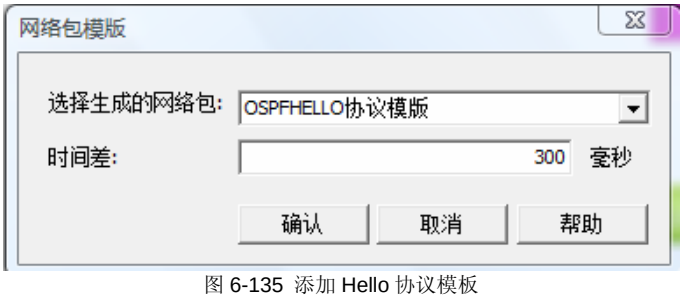

图 6-135 添加 Hello 协议模板

修改协议模板的每个值：

Ethernet II 封装：

- 目标物理地址设置为 224.0.0.4 的组播 MAC 地址 01-00-5E-00-00-05
- 原物理地址设置为路由器 RD 的 fa0/0 接口 MAC 地址 00-D0-F8-6B-38-32
- 类型：0800

IP 封装：

- 版本信息：4
- IP 头长度：5
- 服务类型：C0
- 总长度：68

- 标识：002
- 标志：0
- 生存时间：1
- 协议类型：89
- 发送 IP 地址：192.168.3.2
- 目标 IP 地址：224.0.0.5

OSPF Hello 封装：

- 版本：2
- 类型：1
- 报文长度：48
- 路由 IP：192.168.401
- 区域 ID：0.0.0.1
- 鉴别类型：0
- 鉴别内容：0
- Hello 时延：10
- 选项：2（设置为 E 位，其为十六进制）
- 优先级：1
- 路由时延：00000028 （设置为失效时间，其为十六进制）
- 指定路由器：0.0.0.0
- 备份指定路由器：0.0.0.0
- OSPF 数据：添加邻居
- 点击编辑数据，在弹出的对话框中添加邻居的 IP 地址，邻居 IP 地址为 192.168.10.1，然后点击添加，如下图所示：

图 6-136 添加邻居

编辑完成数据包后，需要点击菜单栏的校验和，进行数据检验，如下图所示：

图 6-137 计算校验和

下图是编辑完成并经过校验的数据包：

图 6-138 编辑完成的 Hello 报文

这时，在路由器 RA 上使用 debug ip ospf packet hello recv 命令，打开 debug 信息测试，再使用 RG-PATS 协议仪的协议数据发生器发送刚编辑好的数据包，点击协议数据发器的菜单栏的“发送”键，如下图所示：

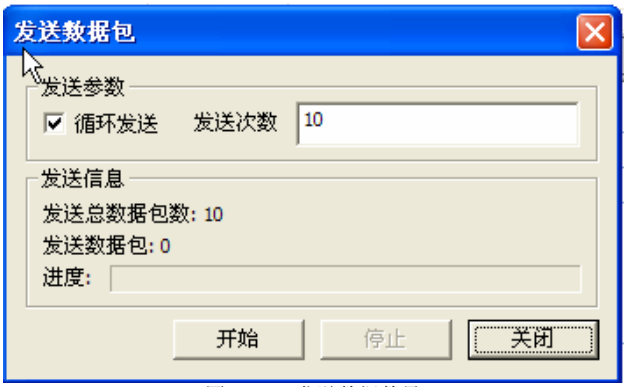

图 6-139 发送数据数量

选择循环发送，发送次数为 10，点击“开始”按键开始发送。这时路由器 RA 上显示如下信息：

```
May 27 04:55:50 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:50 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:50 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:51 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:52 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:52 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:53 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 04:55:58 RA %7:RECV[Hello]: From 192.168.20.1 via FastEthernet 0/0:192.168.1.1 (192.168.1.2 -> 224.0.0.5)
May 27 04:56:00 RA %7:RECV[Hello]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
```

图 6-140 debug 测试

步骤六：使用 RG-PATS 网络协议分析仪编辑并发送 DBD 报文

打开 RG－PATS 网络协议分析仪的数据包发生器，编辑 OSPF DBD 报文，模拟路由器 RD 向邻居发送 OSPF DBD 报文，

在 RG-PATS 协议仪上打开数据包发生器，编辑一个 OSPF DBD 数据包。首先点击菜单栏“添加”，如下图所示：

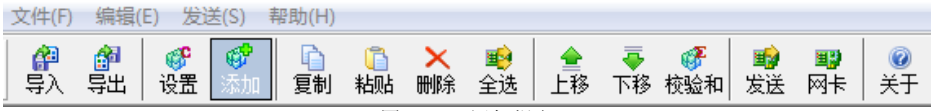

图 6-141 添加报文

添加一个 OSFP DBD 协议模板，点击确认添加，如下图所示：

图 6-142 添加 DBD 协议模板

修改协议模板的每个值：

Ethernet II 封装：

- 目标物理地址设置为路由器 A 的接口 MAC 地址 00-D0-F8-6B-38-39
- 原物理地址设置为路由器RA的fa0/0接口MAC地址00-D0-F8-6B-38-32
- 类型：0800

IP 封装：

- 版本信息：4
- IP 头长度：5
- 服务类型：C0
- 总长度：72
- 标识：006
- 标志：0
- 生存时间：1
- 协议类型：89
- 发送 IP 地址：192.168.3.2
- 目标 IP 地址：192.168.3.1

OSPF DBD 封装：

- 版本：2
- 类型：2
- 报文长度：52
- 路由 IP：192.168.401
- 区域 ID：0.0.0.1
- 鉴别类型：0
- 鉴别内容：0
- 接口 MTU：1500 （输入十六进制）
- 可选项：66（设置为 E 位，其为十进制）
- Flag：7（设置为 I、M、MS）
- DD 序列号：0000004A
- OSPF 数据：添加 LSA 头部信息，
- 点击编辑数据，在弹出的对话框中添加各种 LSA 头部信息，如下图所示：
-

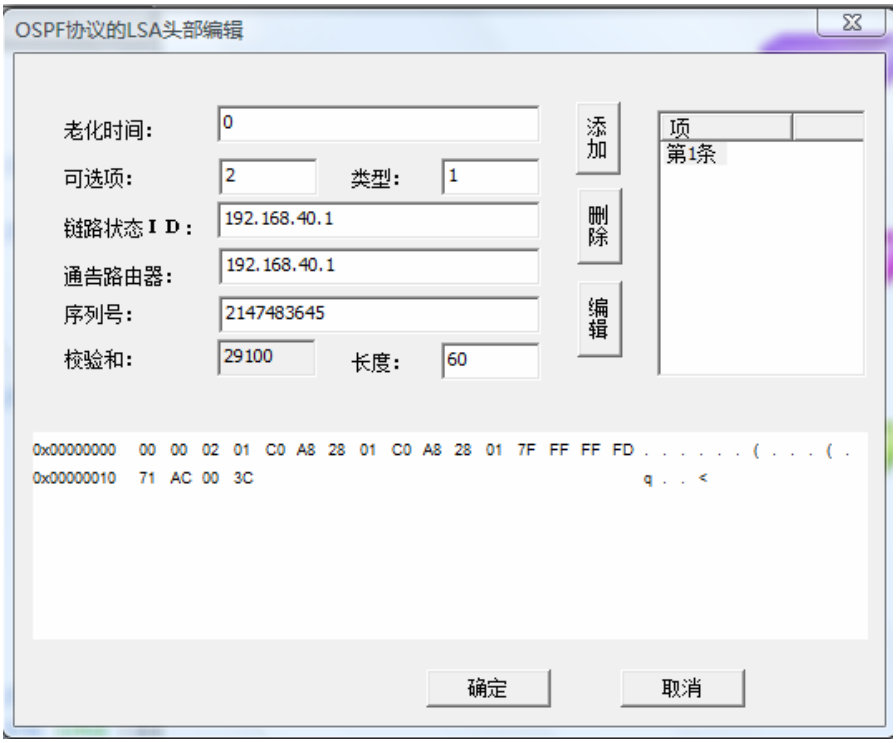

图 6-143 编辑数据

- 老化时间：0
- 可选项：2
- 类型：1
- 链路状态 ID：192.168.40.1
- 通告路由器：192.168.40.1
- 长度：60
- 点击添加，完成 LSA 头部编辑，如果有多条信息可以继续添加。

编辑完成数据包后，需要点击菜单栏的校验和，进行数据检验，如下图所示：

图 6-144 计算校验和

下图是编辑完成并经过校验的数据包：

图 6-145 编辑完成 DBD 报文

这时，在路由器 RA 上使用 debug ip ospf packet dd recv 命令，打开 debug 信息测试，再使用 RG-PATS 协议仪的协议数据发生器发送刚编辑好的数据包，点击协议数据发器的菜单栏的“发送”键，如下图所示：

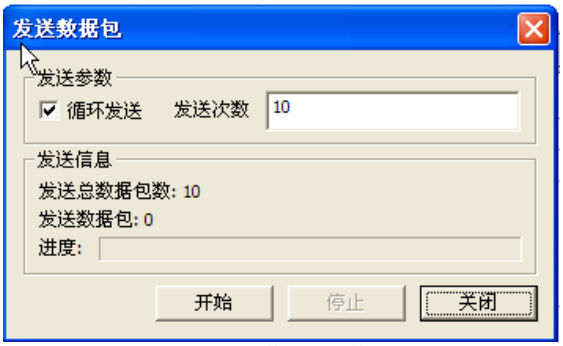

图 6-146 数据发送数量

选择循环发送，发送次数为 10，点击“开始”按键开始发送。这时路由器 RA 上显示如下信息：

```
RA#May 27 05:08:56 RA %7:RECV[DD]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:08:56 RA %7:Neighbor router[FastEthernet 0/1:192.168.3.1-192.168.40.1]: Status change Full -> ExStart
May 27 05:08:57 RA %7:RECV[DD]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:08:57 RA %7:RECV[DD]: Neighbor-RID[192.168.40.1] Self-RID[192.168.10.1] RID cmp=[30] Flag = 7 Recv seq:0x4a Self seq:0x5d
May 27 05:08:57 RA %7:RECV[DD]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1: Negotiation fails, packet discarded
May 27 05:08:57 RA %7:RECV[DD]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:08:57 RA %7:RECV[DD]: Neighbor-RID[192.168.40.1] Self-RID[192.168.10.1] RID cmp=[30] Flag = 7 Recv seq:0x4a Self seq:0x5d
May 27 05:08:57 RA %7:RECV[DD]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1: Negotiation fails, packet discarded
May 27 05:08:58 RA %7:RECV[DD]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:08:58 RA %7:RECV[DD]: Neighbor-RID[192.168.40.1] Self-RID[192.168.10.1] RID cmp=[30] Flag = 7 Recv seq:0x4a Self seq:0x5d
```

图 6-147 debug 测试

步骤七：使用 RG-PATS 网络协议分析仪编辑并发送 LSR 报文

打开 RG－PATS 网络协议分析仪的数据包发生器，编辑 OSPF LSR 报文，模拟路由器 RD 向邻居发送 OSPF LSR 报文，

在 RG-PATS 协议仪上打开数据包发生器，编辑一个 OSPF LSR 数据包。首先点击菜单栏“添加”，如下图所示：

图 6-148 添加报文

添加一个 OSFP LSR 协议模板，点击确认添加，如下图所示：

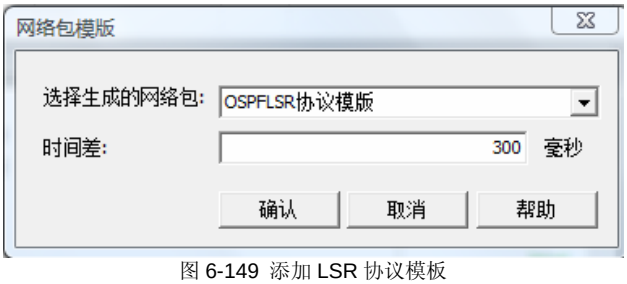

图 6-149 添加 LSR 协议模板

修改协议模板的每个值：

Ethernet II 封装：

- 目标物理地址设置为路由器 A 的接口 MAC 地址 00-D0-F8-6B-38-39
- 原物理地址设置为路由器RA的fa0/0接口MAC地址00-D0-F8-6B-38-32
- 类型：0800

IP 封装：

- 版本信息：4
- IP 头长度：5
- 服务类型：00
- 总长度：80
- 标识：09
- 标志：0
- 生存时间：1
- 协议类型：89
- 发送 IP 地址：192.168.3.2
- 目标 IP 地址：192.168.3.1

OSPF LSR 封装：

- 版本：2
- 类型：3
- 报文长度：60
- 路由 IP：192.168.401
- 区域 ID：0.0.0.1
- 鉴别类型：0
- 鉴别内容：0
- OSPF 数据：编辑 LSR 信息，
- 点击编辑数据，在弹出的对话框中添加各种 LSR 信息，如下图所示：

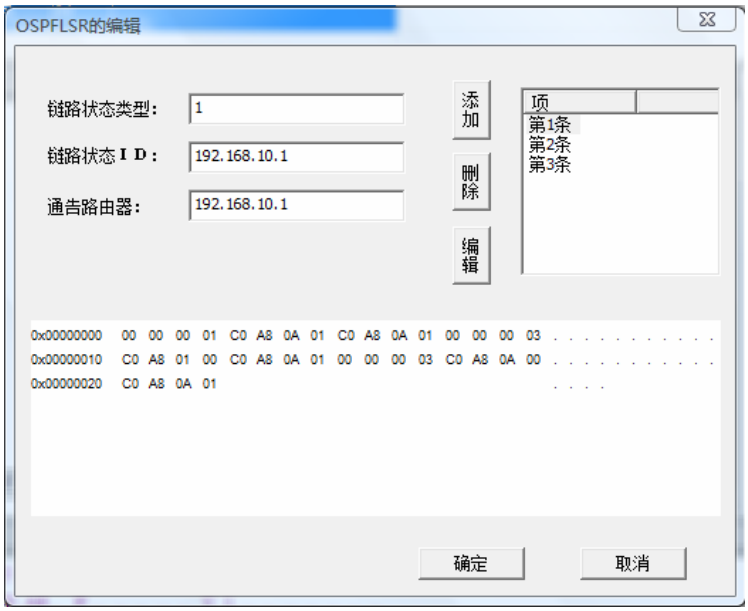

图 6-150 编辑数据

- 链路状态类型：1
- 链路状态 ID：192.168.10.1
- 通告路由器：192.168.10.1
- 点击添加，完成 LSR 信息编辑，如果有多条信息可以继续添加。

编辑完成数据包后，需要点击菜单栏的校验和，进行数据检验，如下图所示：

图 6-151 计算校验和

下图是编辑完成并经过校验的数据包：

图 6-152 编辑完成的 LSR 报文

这时，在路由器 RA 上使用 debug ip ospf packet ls-request recv 命令，打开 debug 信息测试，再使用 RG-PATS 协议仪的协议数据发生器发送刚编辑好的数据包，点击协议数据发器的菜单栏的“发送”键，如下图所示：

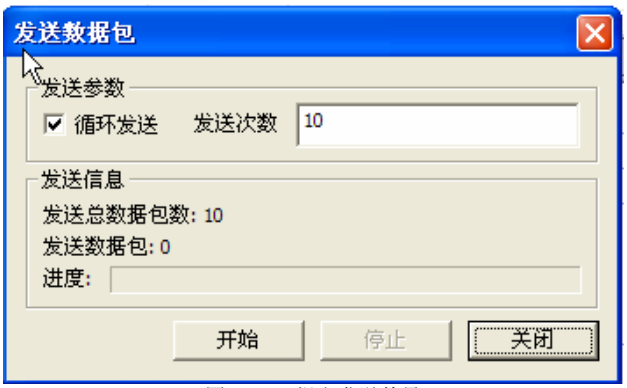

图 6-153 报文发送数量

选择循环发送，发送次数为 10，点击“开始”按键开始发送。这时路由器 RA 上显示如下信息：

```
RA#debug ip ospf packet ls-request recv
RA#May 27 05:43:40 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:19 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:20 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:20 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:21 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:22 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:22 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:23 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:23 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:24 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
May 27 05:44:25 RA %7:RECV[LS-Req]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 192.168.3.1)
```

图 6-154 debug 测试

步骤八：使用 RG-PATS 网络协议分析仪编辑并发送 LSAck 报文

打开 RG－PATS 网络协议分析仪的数据包发生器，编辑 OSPF LSAck 报文，模拟路由器 RD 向邻居发送 OSPF LSAck 报文，

在 RG-PATS 协议仪上打开数据包发生器，编辑一个 OSPF LSAck 数据包。首先点击菜单栏“添加”，如下图所示：

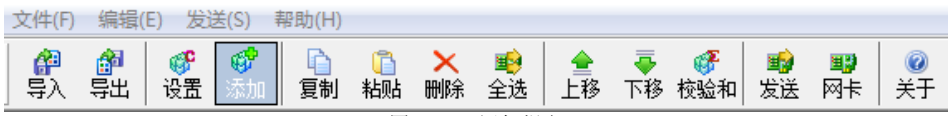

图 6-155 添加报文

添加一个 OSFP LSR 协议模板，点击确认添加，如下图所示：

图 6-156 添加 ACK 协议模板

修改协议模板的每个值：

Ethernet II 封装：

- 目标物理地址设置为组播 224.0.0.5 的 MAC 地址 01-00-5E-00-00-05
- 原物理地址设置为路由器 RA 的 fa0/0 接口 MAC 地址 00-D0-F8-6B-38-32
- 类型：0800

IP 封装：

- 版本信息：4
- IP 头长度：5
- 服务类型：00
- 总长度：64
- 标识：0
- 标志：0
- 生存时间：1
- 协议类型：89
- 发送 IP 地址：192.168.3.2
- 目标 IP 地址：224.0.0.5

OSPF LSR 封装：

- 版本：2
- 类型：5
- 报文长度：44
- 路由 IP：192.168.401
- 区域 ID：0.0.0.1
- 鉴别类型：0
- 鉴别内容：0
- OSPF 数据：编辑 LSAck 信息，
- 点击编辑数据，在弹出的对话框中添加各种 LSAck 信息，如下图所示：

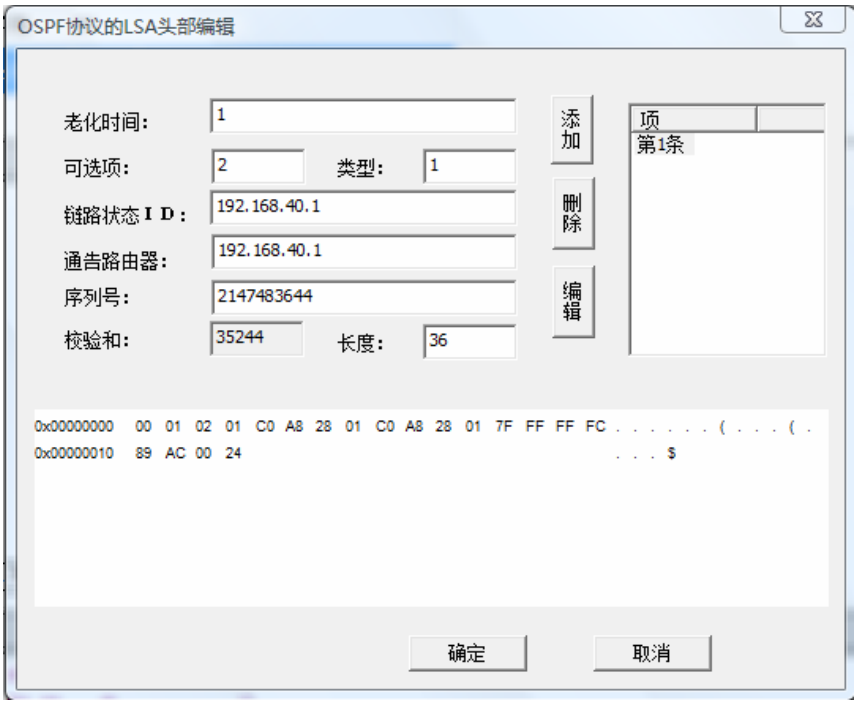

图 6-157 编辑数据

- 老化时间：1
- 可选项：2
- 类型：1
- 链路状态类型：1
- 链路状态 ID：192.168.10.1
- 通告路由器：192.168.10.1
- 长度：36
- 点击添加，完成 LSAck 信息编辑，如果有多条信息可以继续添加。

编辑完成数据包后，需要点击菜单栏的校验和，进行数据检验，如下图所示：

图 6-158 计算校验和

下图是编辑完成并经过校验的数据包：

图 6-159 编辑完成的 ACK 报文

这时，在路由器 RA 上使用 debug ip ospf packet ls-ack recv 命令，打开 debug 信息测试，再使用 RG-PATS 协议仪的协议数据发生器发送刚编辑好的数据包，点击协议数据发器的菜单栏的“发送”键，如下图所示：

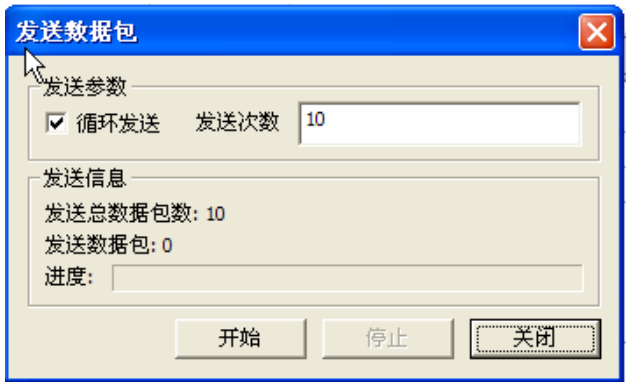

图 6-160 数据发送数量

选择循环发送，发送次数为 10，点击“开始”按键开始发送。这时路由器 RA 上显示如下信息：

```
May 27 05:59:45 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 05:59:46 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 05:59:59 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 05:59:59 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:00 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:01 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:01 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:02 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:03 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:03 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:04 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
May 27 06:00:05 RA %7:RECV[LS-Ack]: From 192.168.40.1 via FastEthernet 0/1:192.168.3.1 (192.168.3.2 -> 224.0.0.5)
```

图 6-161 debug 测试

【思考问题】

1、OSPF 使用 IP，这样做有何优点？在 Database Description 报文中，OSPF 是通过什么方式确保数据的正确传输？

2、为什么 OSPF 报文比 RIP 报文传播得更快？