第五章 网络层

IP 分组

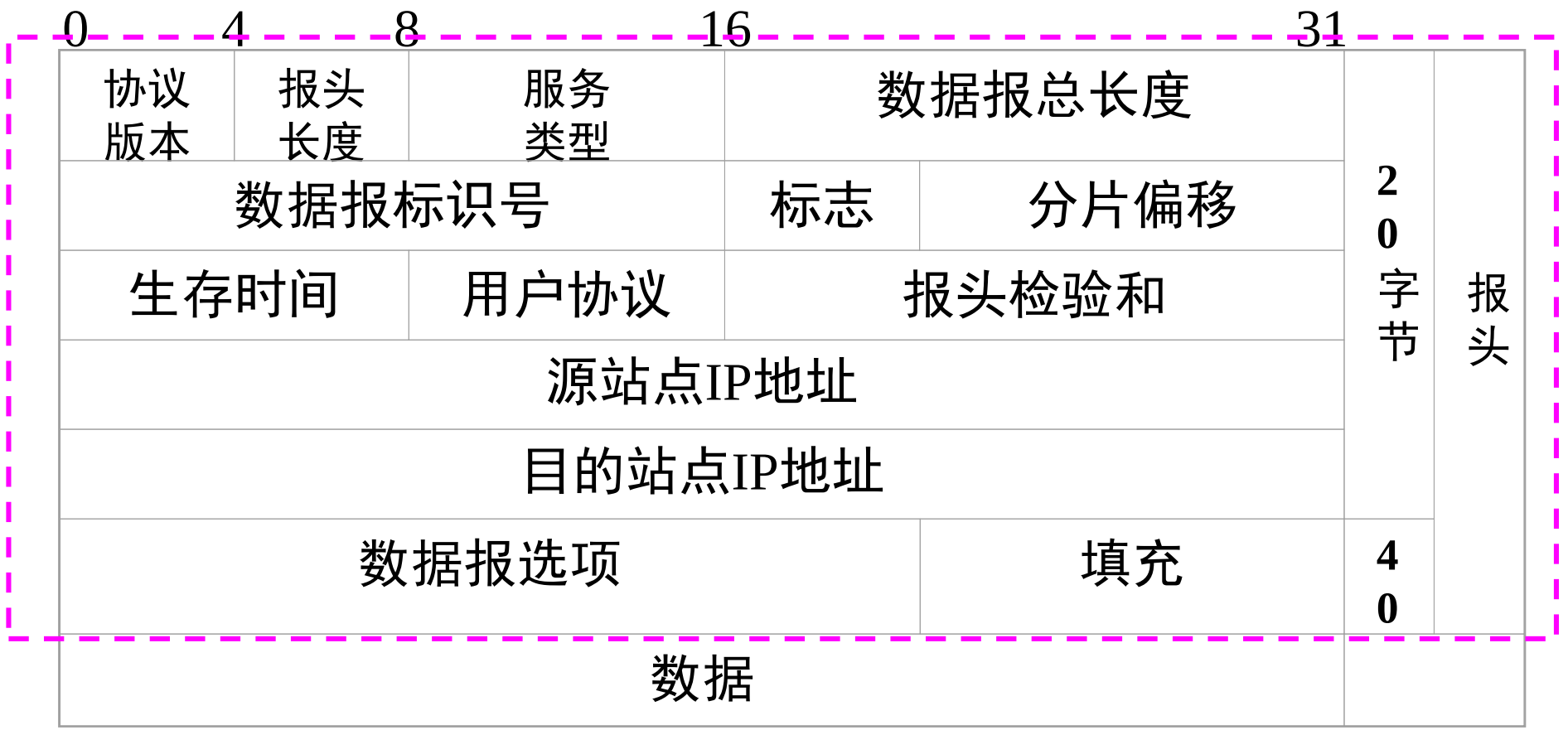
主要内容

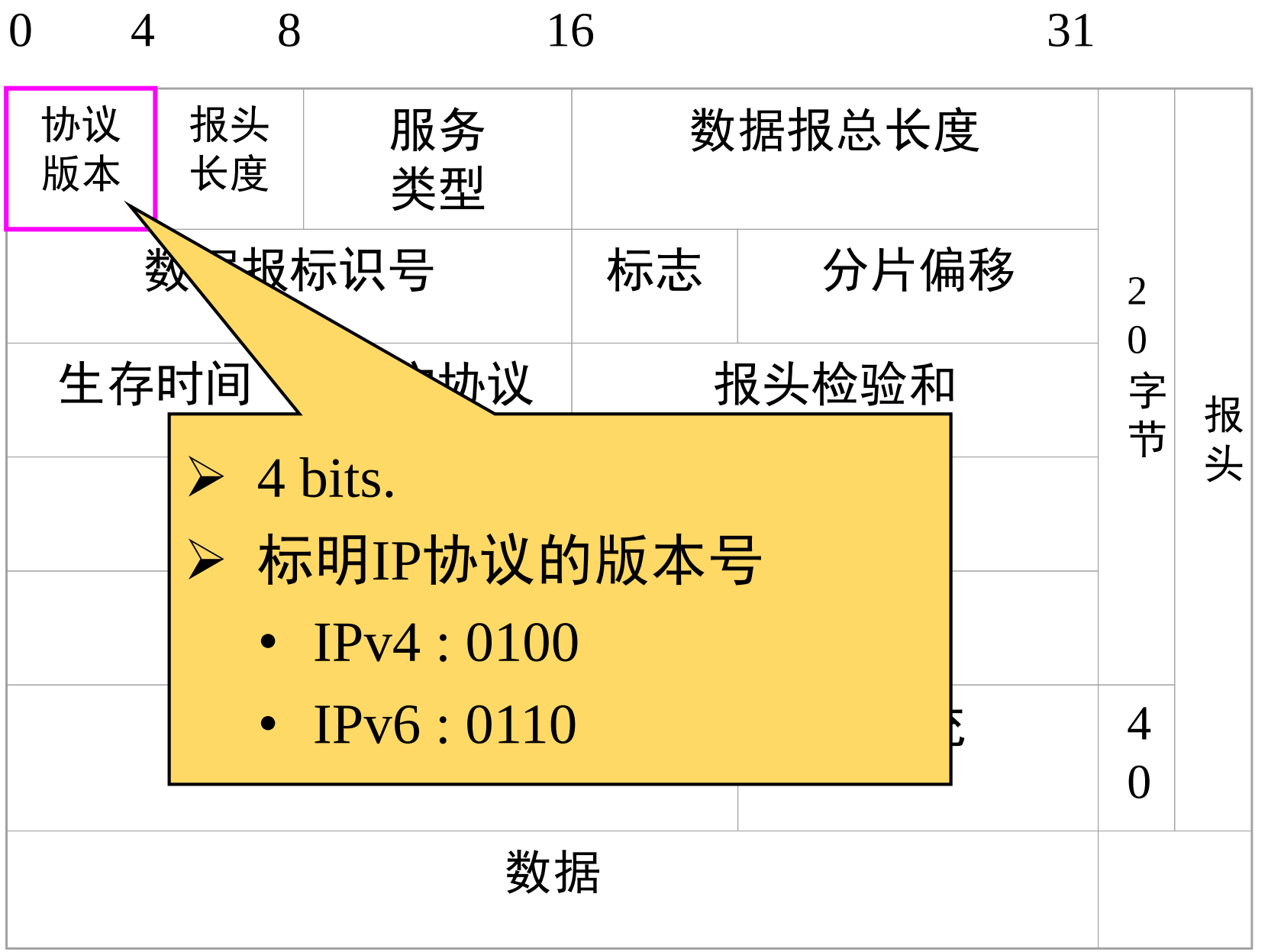
- IP分组
  - 各字段名称
  - 各字段含义
- 使用WireShark在网络上抓取真实的分组
  - 分析抓到的分组

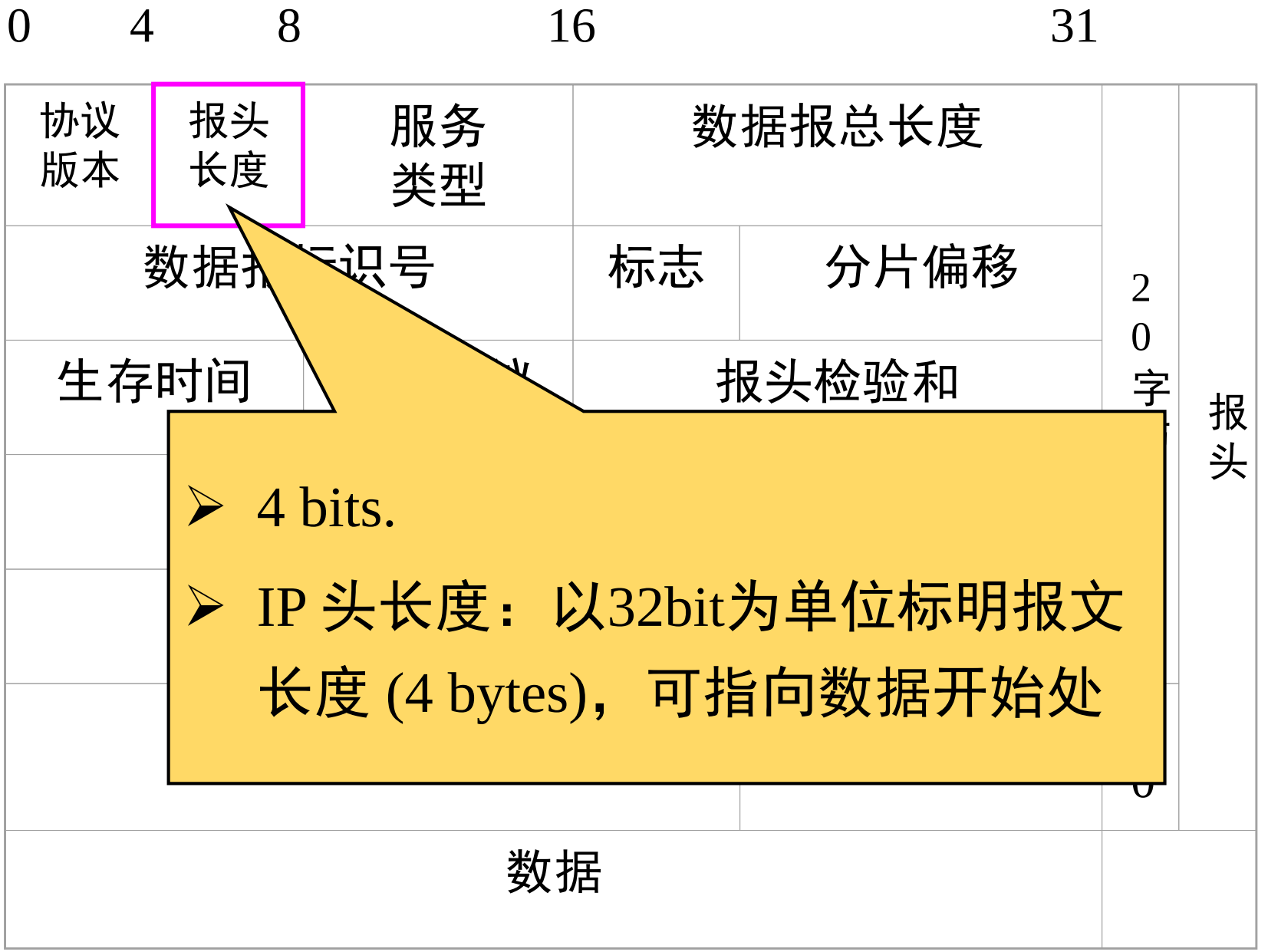
互联网协议IP（Internet protocol）

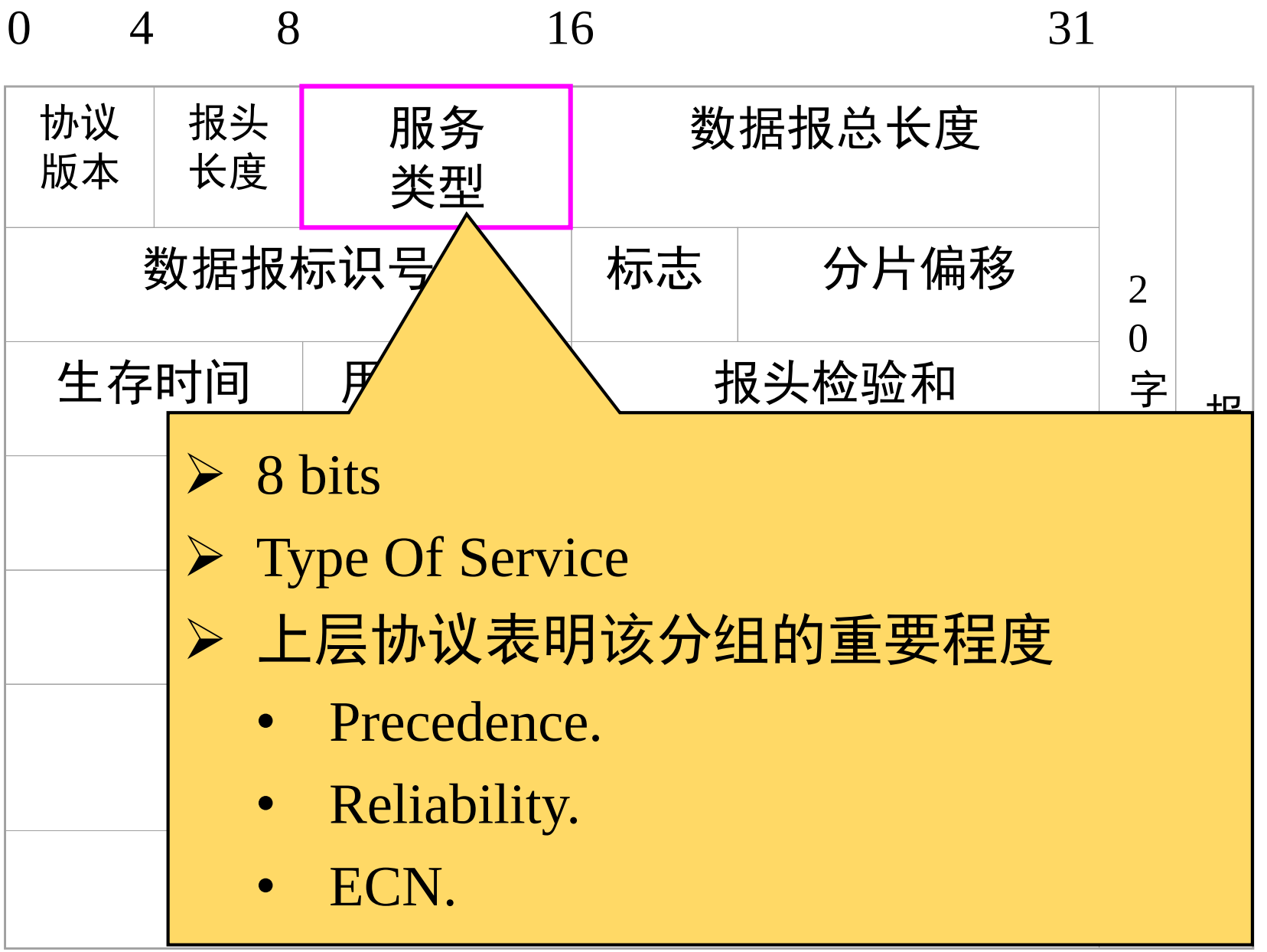
- IP 提供一个尽力而为（ Best-Efforts ）的方式，将数据从源送达目的。
  - 被路由协议
- Internet Protocol
  - 分组格式
  - 编址

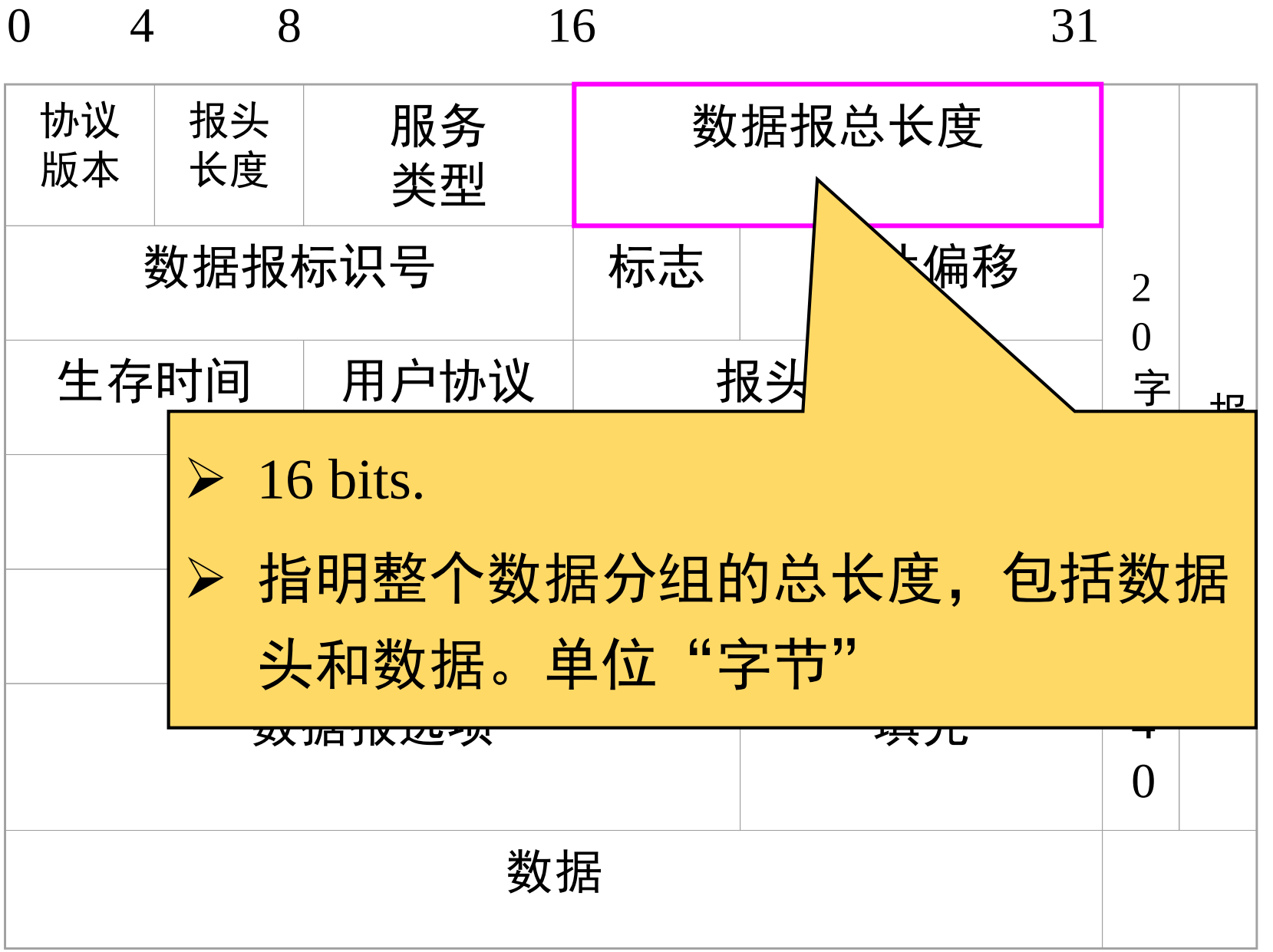
IP 分组格式

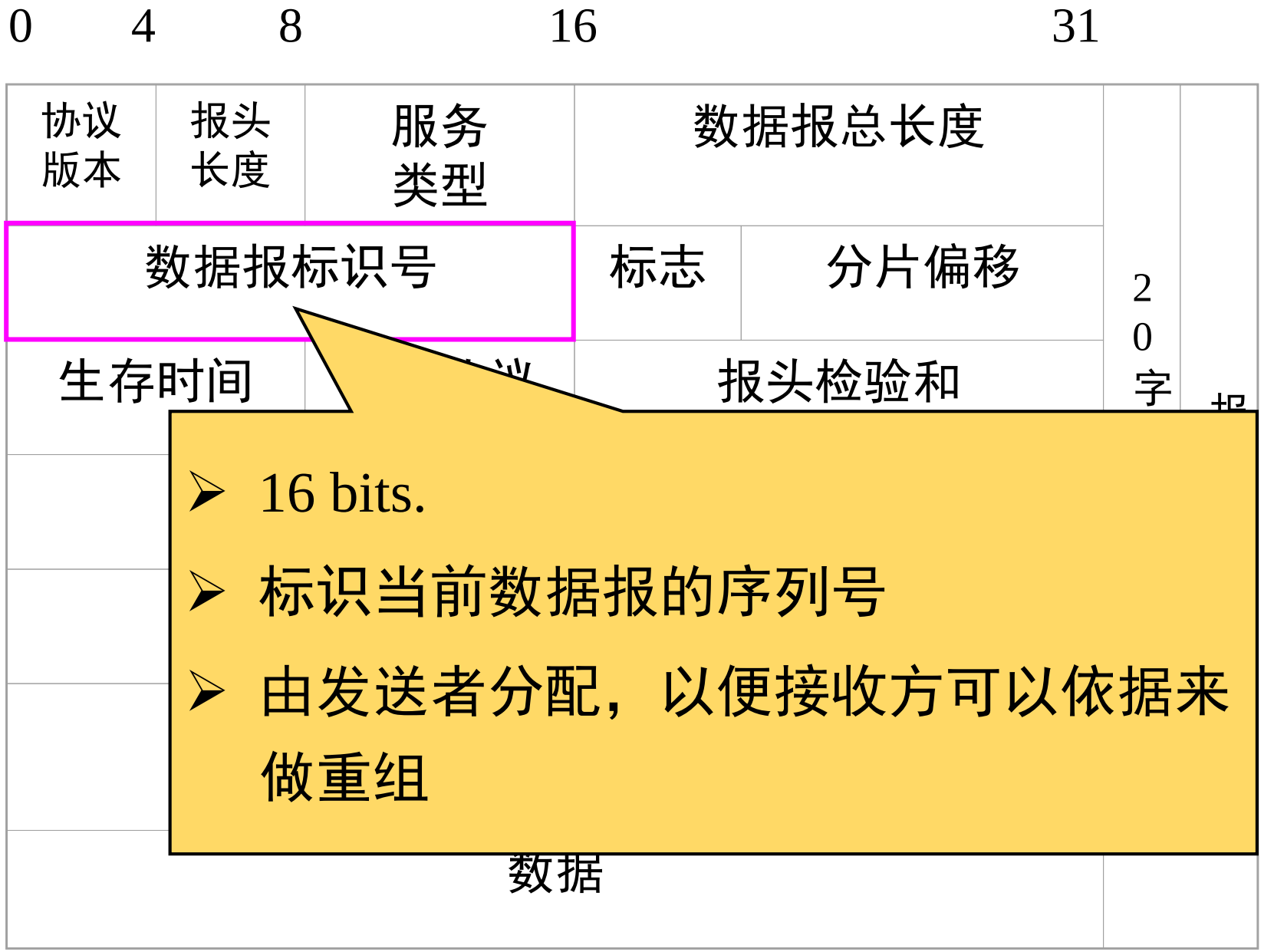

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
用户协议
报头检验和
源站点IP地址
目的站点IP地址
数据报选项
填充
20字节
40
报头
数据

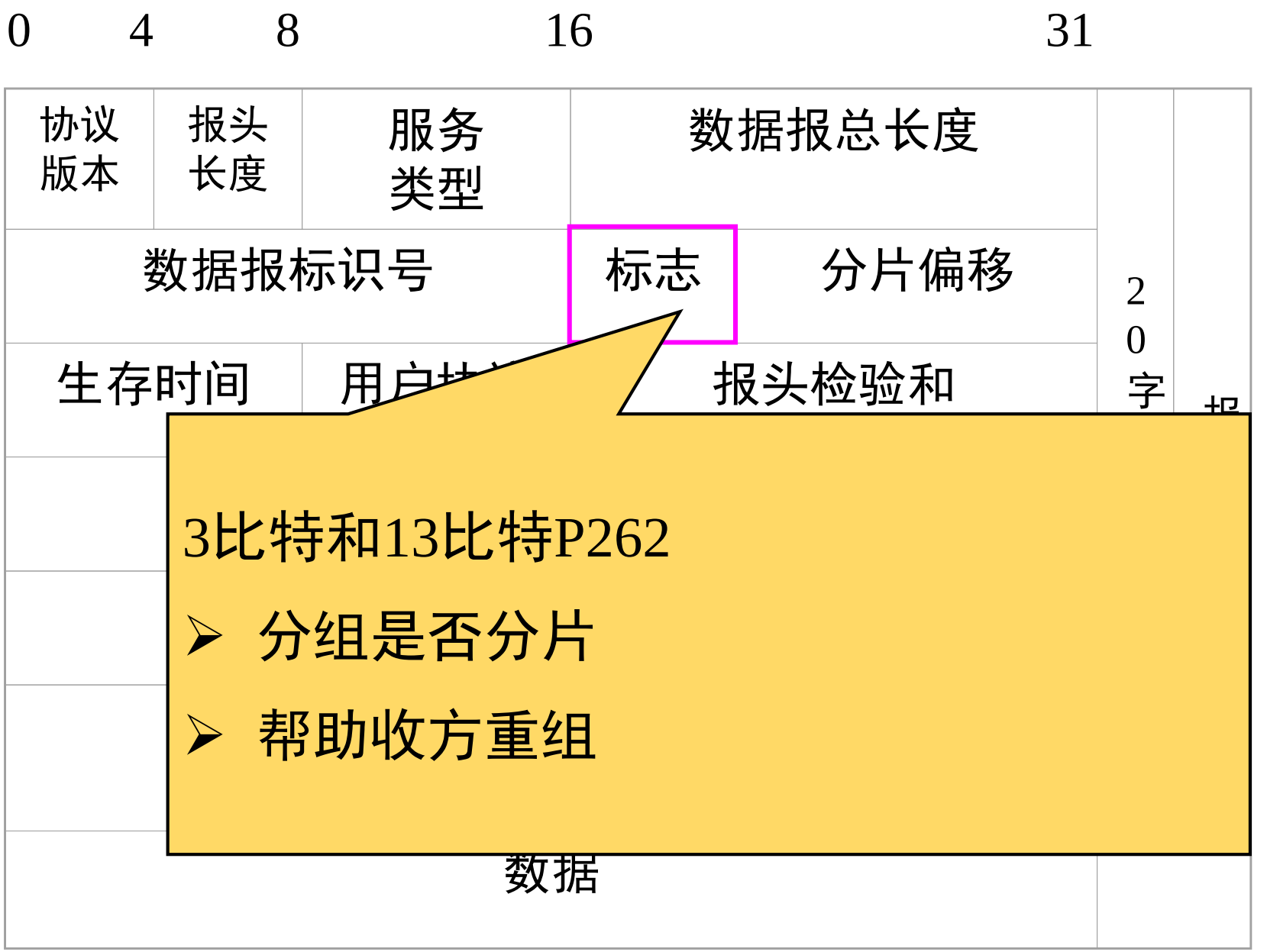

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
标志
分片偏移
生存时间
报头检验和
20字节
报头
40
数据
4 bits.
标明IP协议的版本号
IPv4 : 0100
IPv6 : 0110

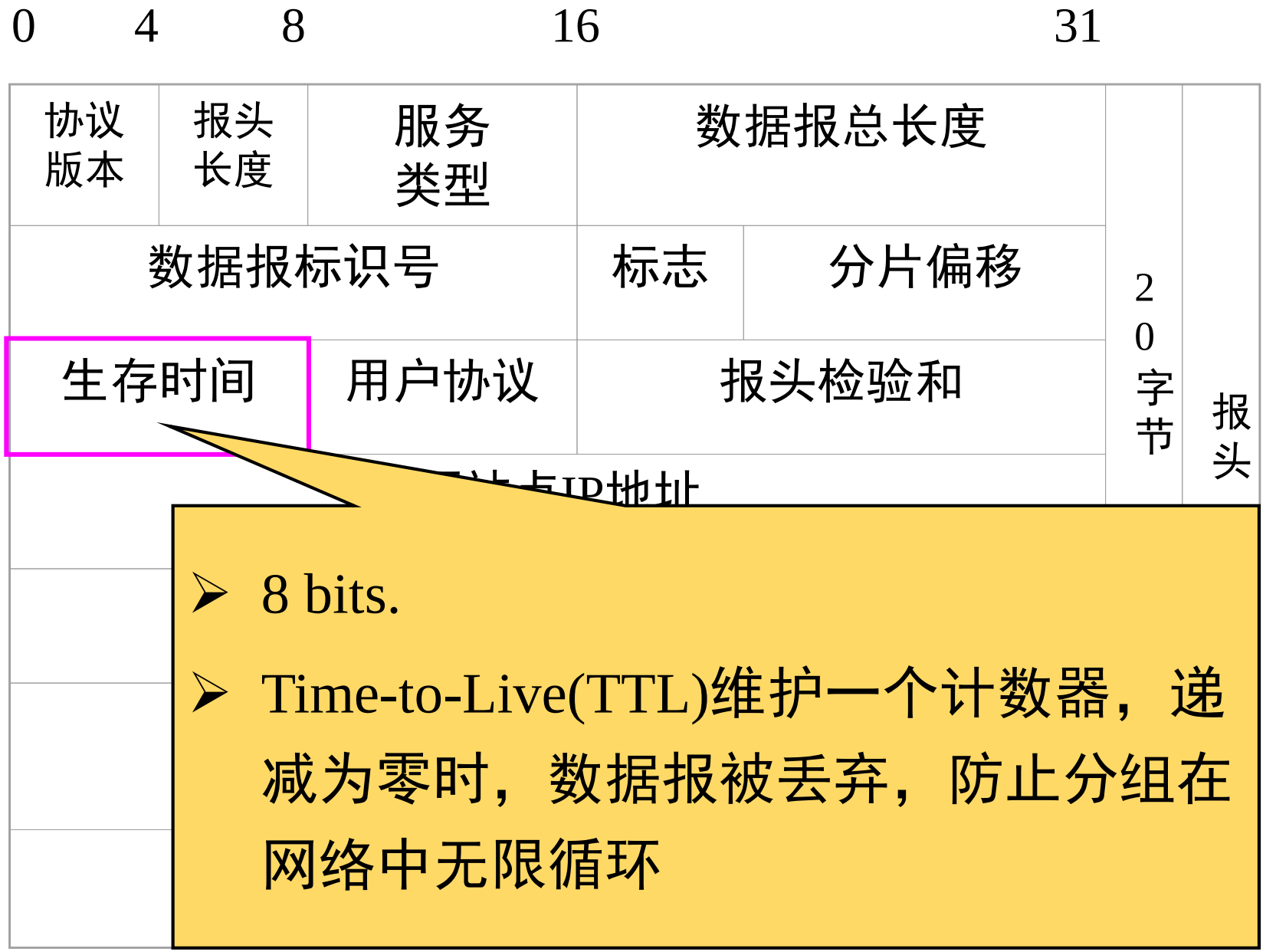

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
标志
分片偏移
生存时间
报头检验和
20字节
报头
数据
4 bits.
IP 头长度：以32bit为单位标明报文长度 (4 bytes)，可指向数据开始处

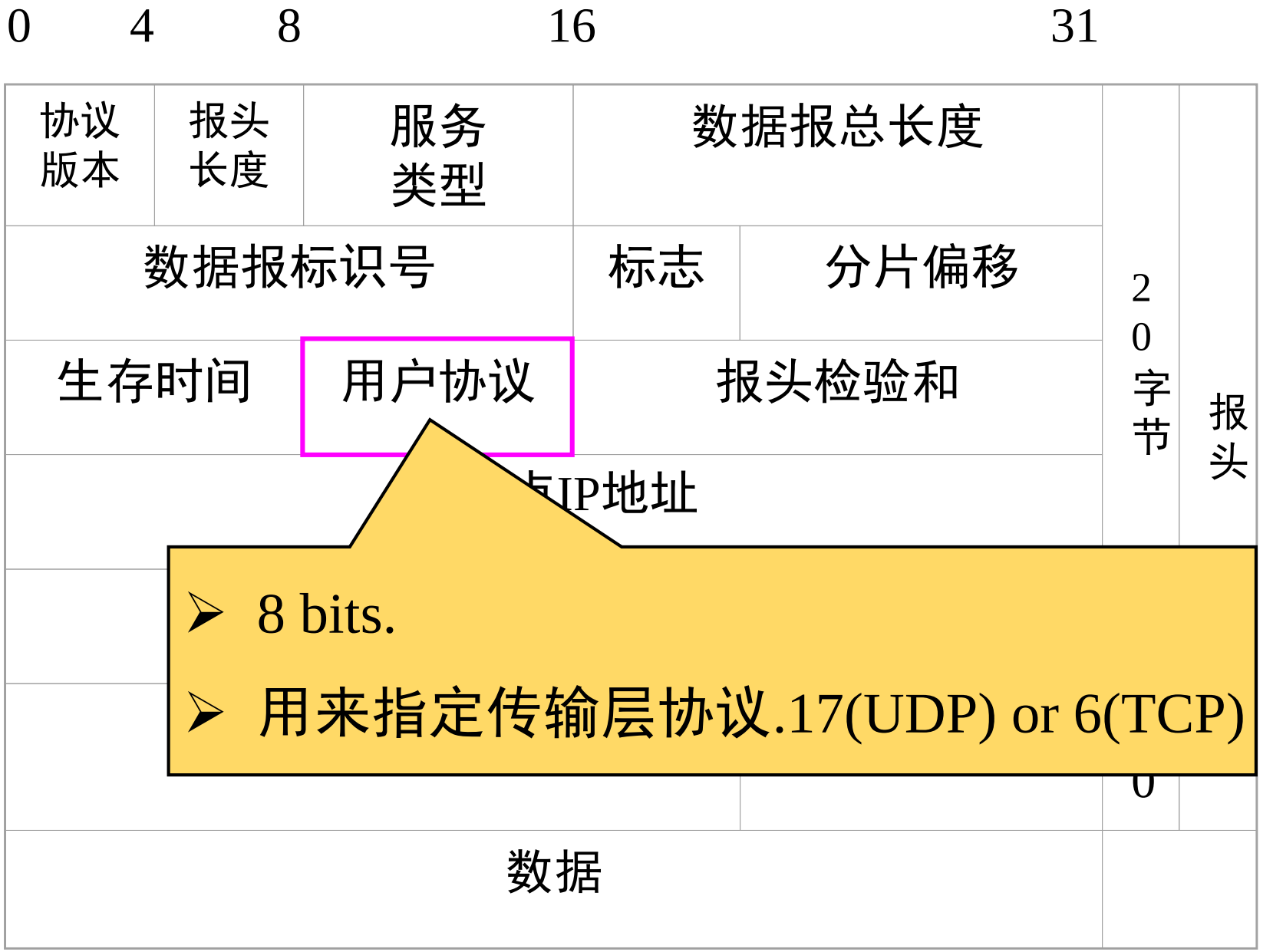

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
报头检验和
20字
8 bits
Type Of Service
上层协议表明该分组的重要程度
Precedence.
Reliability.
ECN.

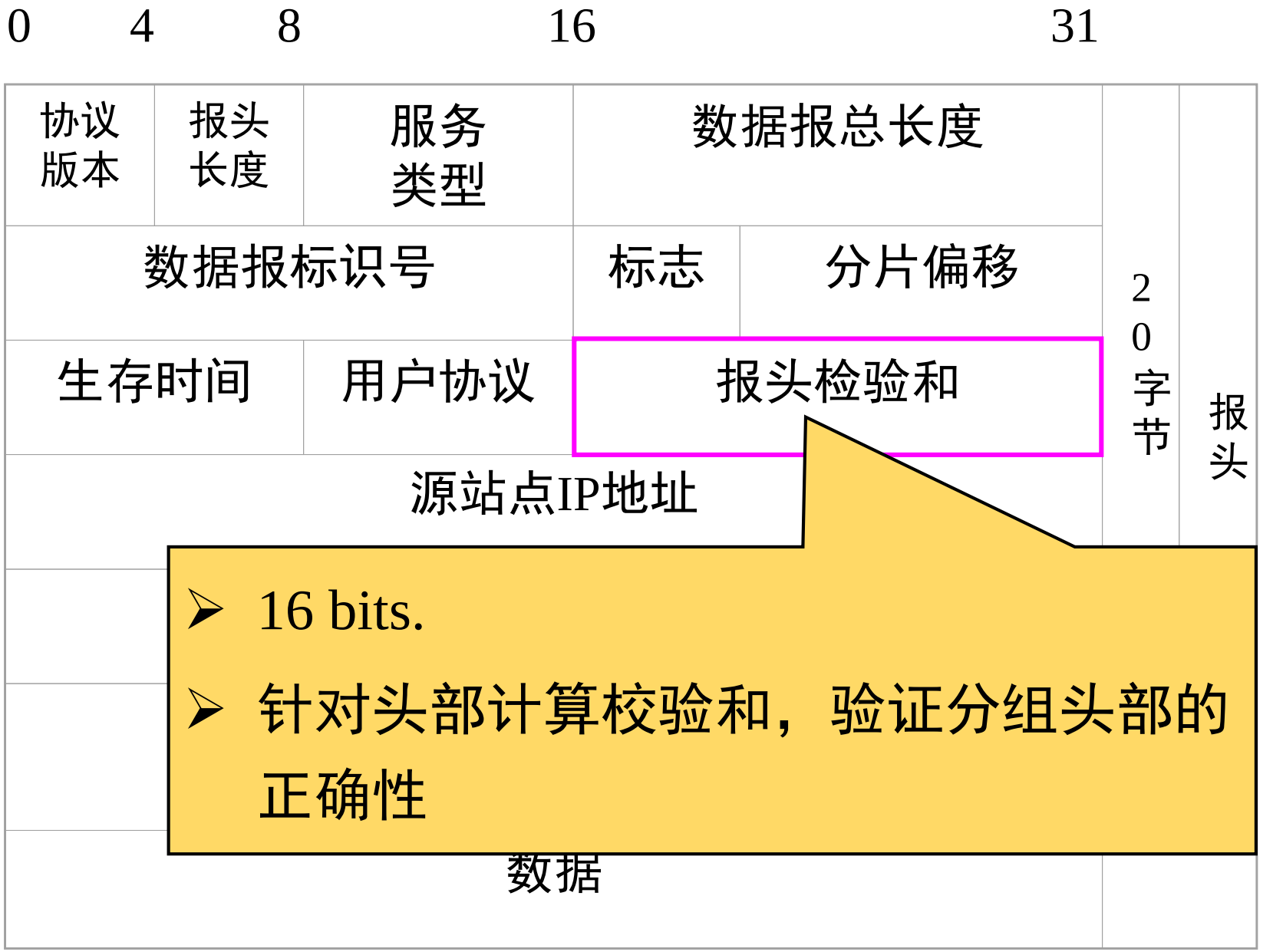

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
偏移
20字
生存时间
用户协议
报头
数据报选项
填充
40
数据
16 bits.
指明整个数据分组的总长度，包括数据头和数据。单位“字节”

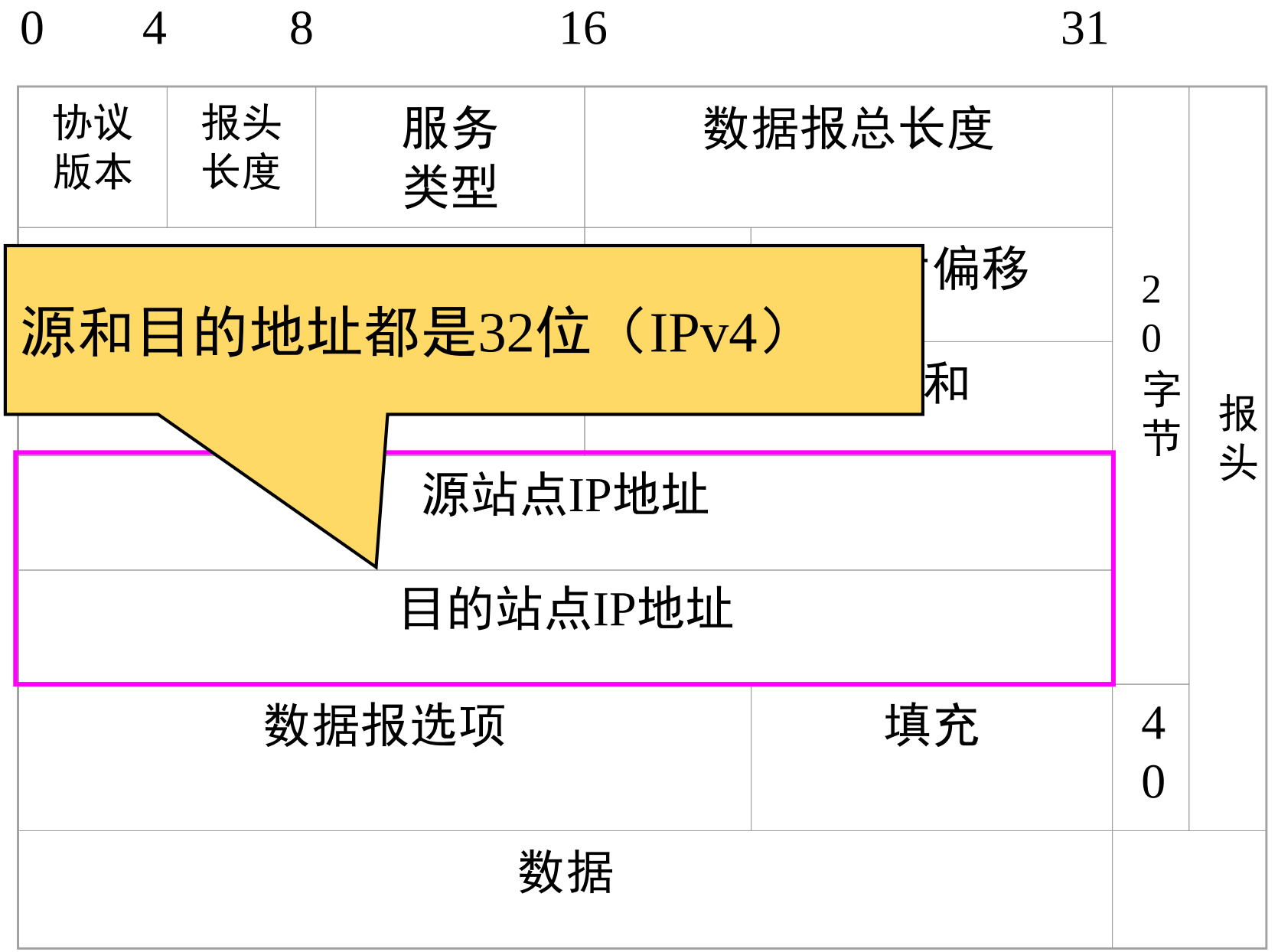

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
报头检验和
20字
数据
16 bits.
标识当前数据报的序列号
由发送者分配，以便接收方可以依据来做重组

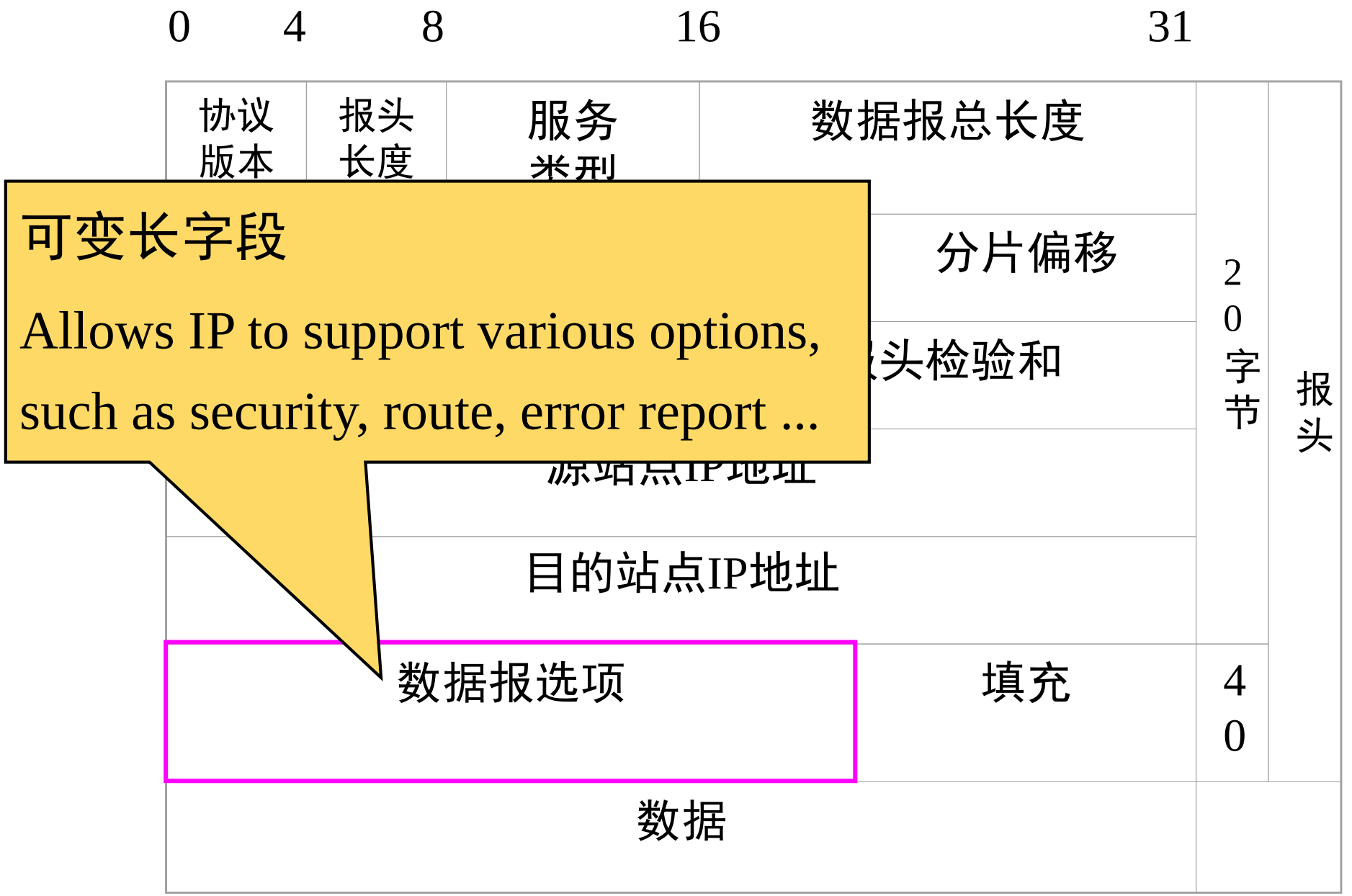

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
报头检验和
20字
数据
3比特和13比特P262
分组是否分片
帮助收方重组

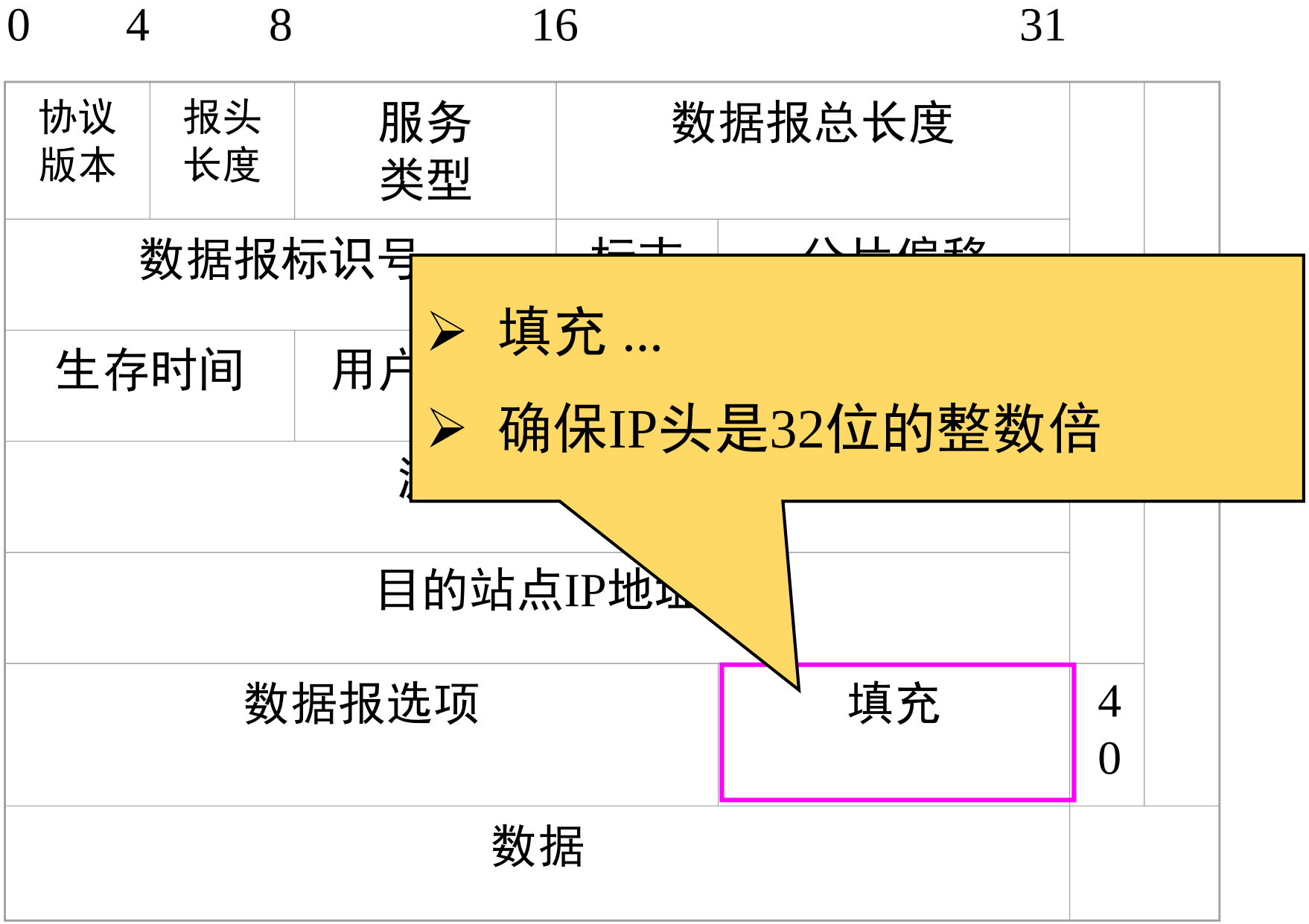

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
用户协议
报头检验和
20字节
报头
8 bits.
Time-to-Live(TTL)维护一个计数器，递减为零时，数据报被丢弃，防止分组在网络中无限循环


0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
用户协议
报头检验和
IP地址
数据
20字节
报头
8 bits.
用来指定传输层协议.17(UDP) or 6(TCP)

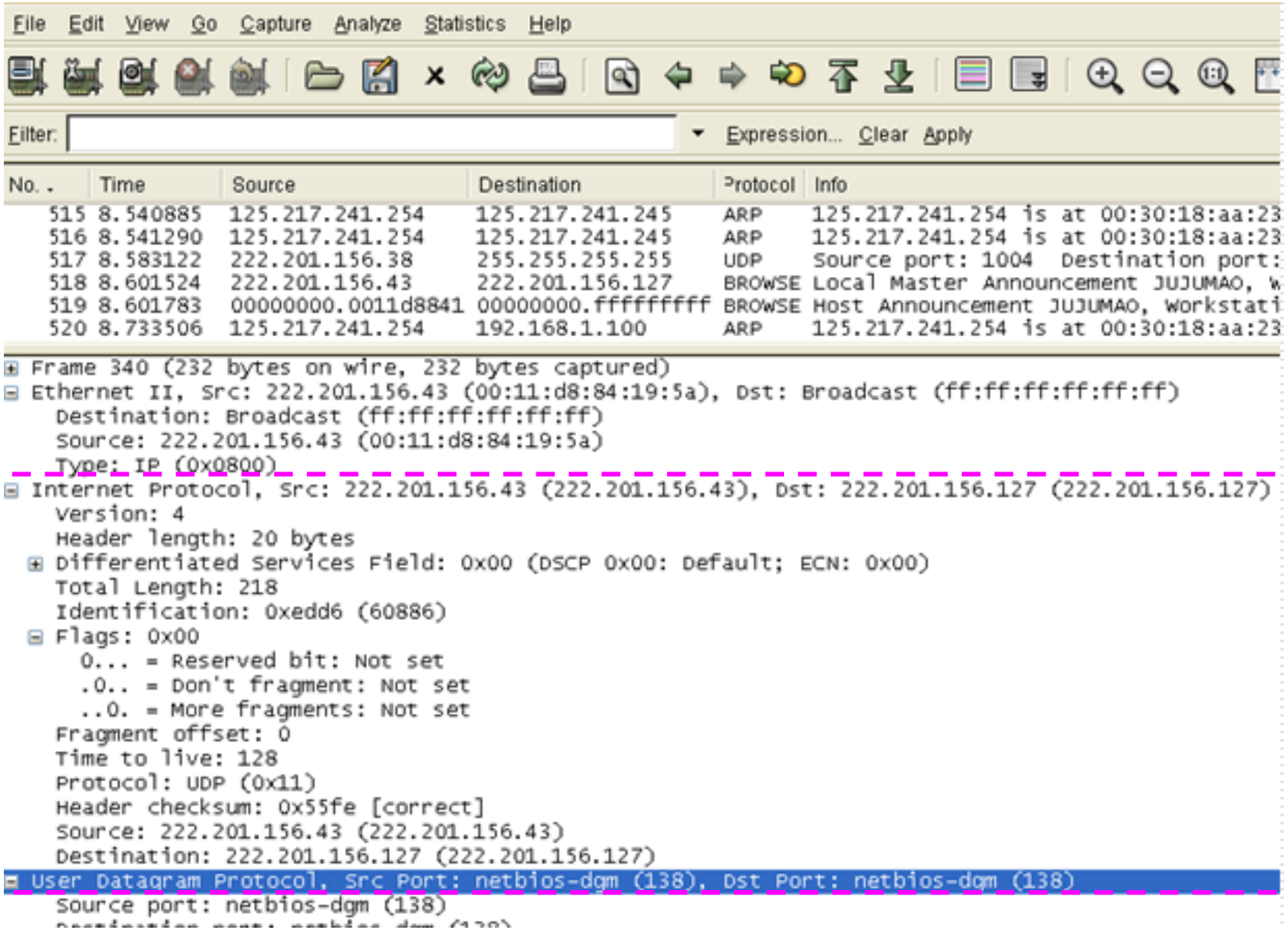

0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
标志
分片偏移
生存时间
用户协议
报头检验和
源站点IP地址
数据
20字节
报头
16 bits.
针对头部计算校验和，验证分组头部的正确性


0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
偏移
和
源和目的地址都是32位（IPv4）
源站点IP地址
目的站点IP地址
数据报选项
填充
数据
20字节
40
报头


0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
分片偏移
头检验和
源站点IP地址
目的站点IP地址
数据报选项
填充
数据
20字节
40
报头
可变长字段
Allows IP to support various options, such as security, route, error report ...


0
4
8
16
31
协议版本
报头长度
服务类型
数据报总长度
数据报标识号
生存时间
目的站点IP地址
数据报选项
填充
40
数据
填充 ...
确保IP头是32位的整数倍

抓个真的


File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
515 8.540885 125.217.241.254 125.217.241.245 ARP 125.217.241.254 is at 00:30:18:aa:23
516 8.541290 125.217.241.254 125.217.241.245 ARP 125.217.241.254 is at 00:30:18:aa:23
517 8.583122 222.201.156.38 255.255.255.255 UDP Source port: 1004 Destination port:
518 8.601524 222.201.156.43 222.201.156.127 BROWSE Local Master Announcement JUJUMAO, W
519 8.601783 00000000.0011d8841 00000000.ffffffff BROWSE Host Announcement JUJUMAO, Workstati
520 8.733506 125.217.241.254 192.168.1.100 ARP 125.217.241.254 is at 00:30:18:aa:23
Frame 340 (232 bytes on wire, 232 bytes captured)
Ethernet II, Src: 222.201.156.43 (00:11:d8:84:19:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: 222.201.156.43 (00:11:d8:84:19:5a)
Type: IP (0x0800)
Internet Protocol, Src: 222.201.156.43 (222.201.156.43), Dst: 222.201.156.127 (222.201.156.127)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 218
Identification: 0xedd6 (60886)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0x55fe [correct]
Source: 222.201.156.43 (222.201.156.43)
Destination: 222.201.156.127 (222.201.156.127)
User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
Source port: netbios-dgm (138)

小结

- IP分组的重要字段
  - 头部长度
  - TTL
  - 用户协议
  - 目的IP
- 自己抓取真实的分组来分析

思考题

- IP分组中包括哪些主要字段？
- 怎样知道IP分组的净载荷中封装的是什么数据段呢？
- 当路由器发现一个分组的TTL-1=0时，它会怎么对待这个分组？
- 怎么知道一个分组是否包含有选项呢？
- 尝试用WireShark抓取一个真实的分组，观察它的各字段值，并分析它。

谢谢观看

致谢

本课程课件中的部分素材来自于：（1）清华大学出版社出版的翻译教材《计算机网络》（原著作者：Andrew S. Tanenbaum，David J. Wetherall）；（2）思科网络技术学院教程；（3）网络上搜到的其他资料。在此，对清华大学出版社、思科网络技术学院、人民邮电出版社、以及其它提供本课程引用资料的个人表示衷心的感谢！

对于本课程引用的素材，仅用于课程学习，如有任何问题，请与我们联系！