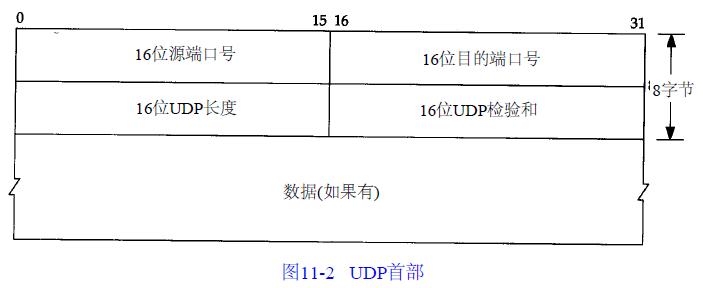
1. UDP数据报

1.UDP数据报格式



（1）端口号

UDP协议使用端口号为不同的应用保留其各自的数据传输通道。UDP和TCP协议正是采用这一机制实现对同一时刻内多项应用同时发送和接收数据的支持。数据发送一方（可以是客户端或服务器端）将UDP数据包通过源端口发送出去，而数据接收一方则通过目标端口接收数据。有的网络应用只能使用预先为其预留或注册的静态端口；而另外一些网络应用则可以使用未被注册的动态端口。因为UDP报头使用两个字节存放端口号，所以端口号的有效范围是从0到65535。一般来说，大于49151的端口号都代表动态端口。

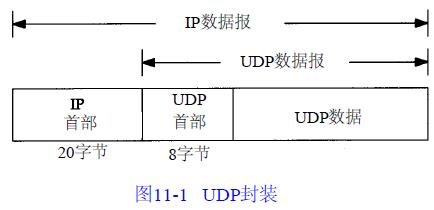
（2）UDP长度

数据报的长度是指包括报头和数据部分在内的总字节数。因为报头的长度是固定的，所以该域主要被用来计算可变长度的数据部分（又称为数据负载）。数据报的最大长度根据操作环境的不同而各异。从理论上说，包含报头在内的数据报的最大长度为65535字节。不过，一些实际应用往往会限制数据报的大小，有时会降低到8192字节。

（3）UDP校验和

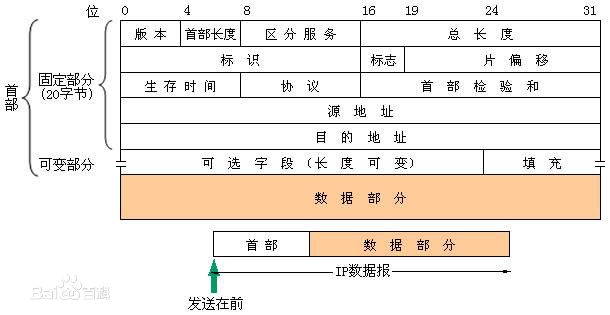
UDP协议使用报头中的校验值来保证数据的安全。校验值首先在数据发送方通过特殊的算法计算得出，在传递到接收方之后，还需要再重新计算。如果某个数据报在传输过程中被第三方篡改或者由于线路噪音等原因受到损坏，发送和接收方的校验计算值将不会相符，由此UDP协议可以检测是否出错。这与TCP协议是不同的，后者要求必须具有校验值。

2.UDP数据报在IP数据报中的位置



二.IP数据报

1.IP数据报格式



**固定部分**

(1)版本

占4位，指IP协议的版本。通信双方使用的IP协议版本必须一致。目前广泛使用的IP协议版本号为4（即IPv4）。关于IPv6，目前还处于草案阶段。

(2)首部长度

占4位，可表示的最大十进制数值是15。请注意，这个字段所表示数的单位是32位字长（1个32位字长是4字节），因此，当IP的首部长度为1111时（即十进制的15），首部长度就达到60字节。当IP分组的首部长度不是4字节的整数倍时，必须利用最后的填充字段加以填充。因此数据部分永远在4字节的整数倍开始，这样在实现IP协议时较为方便。首部长度限制为60字节的缺点是有时可能不够用。但这样做是希望用户尽量减少开销。最常用的首部长度就是20字节（即首部长度为0101），这时不使用任何选项。

(3)区分服务

占8位，用来获得更好的服务。这个字段在旧标准中叫做服务类型，但实际上一直没有被使用过。1998年IETF把这个字段改名为区分服务DS(Differentiated Services)。只有在使用区分服务时，这个字段才起作用。

(4)总长度

总长度指首部和数据之和的长度，单位为字节。总长度字段为16位，因此数据报的最大长度为2^16-1=65535字节。

在IP层下面的每一种数据链路层都有自己的帧格式，其中包括帧格式中的数据字段的最大长度，这称为最大传送单元MTU(Maximum Transfer Unit)。当一个数据报封装成链路层的帧时，此数据报的总长度（即首部加上数据部分）一定不能超过下面的数据链路层的MTU值。

(5)标识(identification)

占16位。IP软件在存储器中维持一个计数器，每产生一个数据报，计数器就加1，并将此值赋给标识字段。但这个“标识”并不是序号，因为IP是无连接服务，数据报不存在按序接收的问题。当数据报由于长度超过网络的MTU而必须分片时，这个标识字段的值就被复制到所有的数据报的标识字段中。相同的标识字段的值使分片后的各数据报片最后能正确地重装成为原来的数据报。

(6)标志(flag)

占3位，但目前只有2位有意义。

●　标志字段中的最低位记为MF(More Fragment)。MF=1即表示后面“还有分片”的数据报。MF=0表示这已是若干数据报片中的最后一个。

●　标志字段中间的一位记为DF(Don’t Fragment)，意思是“不能分片”。只有当DF=0时才允许分片。

(7)片偏移

占13位。片偏移指出：较长的分组在分片后，某片在原分组中的相对位置。也就是说，相对用户数据字段的起点，该片从何处开始。片偏移以8个字节为偏移单位。这就是说，除了最后一个分片，每个分片的长度一定是8字节（64位）的整数倍。

(8)生存时间

占8位，生存时间字段常用的的英文缩写是TTL(Time To Live)，表明是数据报在网络中的寿命。由发出数据报的源点设置这个字段。其目的是防止无法交付的数据报无限制地在因特网中兜圈子，因而白白消耗网络资源。最初的设计是以秒作为TTL的单位。每经过一个路由器时，就把TTL减去数据报在路由器消耗掉的一段时间。若数据报在路由器消耗的时间小于1秒，就把TTL值减1。当TTL值为0时，就丢弃这个数据报。后来把TTL字段的功能改为“跳数限制”（但名称不变）。路由器在转发数据报之前就把TTL值减1.若TTL值减少到零，就丢弃这个数据报，不再转发。因此，现在TTL的单位不再是秒，而是跳数。TTL的意义是指明数据报在网络中至多可经过多少个路由器。显然，数据报在网络上经过的路由器的最大数值是255.若把TTL的初始值设为1，就表示这个数据报只能在本局域网中传送。

(9)协议

占8位，协议字段指出此数据报携带的数据是使用何种协议，以便使目的主机的IP层知道应将数据部分上交给哪个处理过程。

(10)首部检验和

占16位。这个字段只检验数据报的首部，但不包括数据部分。这是因为数据报每经过一个路由器，路由器都要重新计算一下首部检验和（一些字段，如生存时间、标志、片偏移等都可能发生变化）。不检验数据部分可减少计算的工作量。

(11)源地址　占32位。

(12)目的地址　占32位。

**可变部分**

IP首部的可变部分就是一个可选字段。选项字段用来支持排错、测量以及安全等措施，内容很丰富。此字段的长度可变，从1个字节到40个字节不等，取决于所选择的项目。某些选项项目只需要1个字节，它只包括1个字节的选项代码。但还有些选项需要多个字节，这些选项一个个拼接起来，中间不需要有分隔符，最后用全0的填充字段补齐成为4字节的整数倍。

增加首部的可变部分是为了增加IP数据报的功能，但这同时也使得IP数据报的首部长度成为可变的。这就增加了每一个路由器处理数据报的开销。实际上这些选项很少被使用。新的IP版本IPv6就将IP数据报的首部长度做成固定的。

目前，这些任选项定义如下：

（1）安全和处理限制（用于军事领域）

（2）记录路径（让每个路由器都记下它的IP地址）

（3）时间戳（Time Stamp）（让每个路由器都记下IP数据报经过每一个路由器的IP地址和当地时间）

（4）宽松的源站路由（Loose Source Route）（为数据报指定一系列必须经过的IP地址）

（5）严格的源站路由（Strict Source Route）（与宽松的源站路由类似，但是要求只能经过指定的这些地址，不能经过其他的地址）

这些选项很少被使用，并非所有主机和路由器都支持这些选项。

**三.分片**

(1)UDP数据包的理论长度

udp数据包的理论长度是多少，合适的udp数据包应该是多少呢？从TCP-IP详解卷一第11章的udp数据包的包头可以看出，udp的最大包长度是2^16-1的个字节。由于udp包头占8个字节，而在ip层进行封装后的ip包头占去20字节，所以这个是udp数据包的最大理论长度是2^16-1-8-20=65507。

然而这个只是udp数据包的最大理论长度。首先，我们知道，TCP/IP通常被认为是一个四层协议系统，包括链路层、网络层、运输层、应用层。UDP属于运输层，在传输过程中，udp包的整体是作为下层协议的数据字段进行传输的，它的长度大小受到下层ip层和数据链路层协议的制约。

(2)MTU相关概念

以太网(Ethernet)数据帧的长度必须在46-1500字节之间，这是由以太网的物理特性决定的。这个1500字节被称为链路层的MTU(最大传输单元)。因特网协议允许IP分片，这样就可以将数据包分成足够小的片段以通过那些最大传输单元小于该数据包原始大小的链路了。这一分片过程发生在网络层，它使用的是将分组发送到链路上的网络接口的最大传输单元的值。这个最大传输单元的值就是MTU（Maximum Transmission Unit）。它是指一种通信协议的某一层上面所能通过的最大数据包大小（以字节为单位）。最大传输单元这个参数通常与通信接口有关（网络接口卡、串口等）。

在因特网协议中，一条因特网传输路径的“路径最大传输单元”被定义为从源地址到目的地址所经过“路径”上的所有IP跳的最大传输单元的最小值。

需要注意的是，loopback的MTU不受上述限制，查看loopback MTU值：

[root@bogon ~]# cat /sys/class/net/lo/mtu

65536

(3)IP分包udp数据包长度的影响

如上所述，由于网络接口卡的制约，mtu的长度被限制在1500字节，这个长度指的是链路层的数据区。对于大于这个数值的分组可能被分片，否则无法发送，而分组交换的网络是不可靠的，存在着丢包。IP 协议的发送方不做重传。接收方只有在收到全部的分片后才能 reassemble并送至上层协议处理代码，否则在应用程序看来这些分组已经被丢弃。

假定同一时刻网络丢包的概率是均等的，那么较大的IP datagram必然有更大的概率被丢弃，因为只要丢失了一个fragment，就导致整个IP datagram接收不到。不超过MTU的分组是不存在分片问题的。

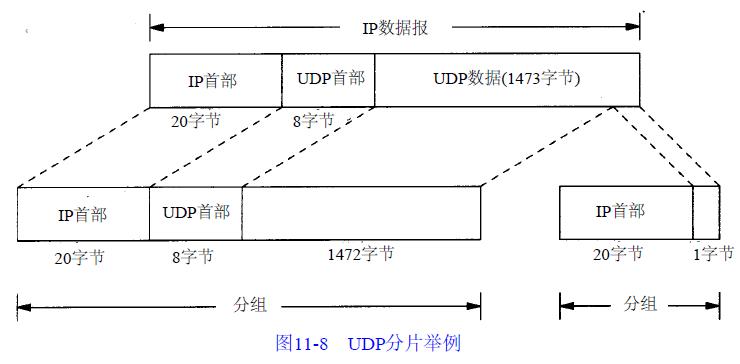
MTU的值并不包括链路层的首部和尾部的18个字节。所以，这个1500字节就是网络层IP数据报的长度限制。因为IP数据报的首部为20字节，所以IP数据报的数据区长度最大为1480字节。而这个1480字节就是用来放TCP传来的TCP报文段或UDP传来的UDP数据报的。又因为UDP数据报的首部8字节,所以UDP数据报的数据区最大长度为1472字节。这个1472字节就是我们可以使用的字节数。

当我们发送的UDP数据大于1472的时候会怎样呢？这也就是说IP数据报大于1500字节，大于MTU。这个时候发送方IP层就需要分片(fragmentation)。把数据报分成若干片，使每一片都小于MTU。而接收方IP层则需要进行数据报的重组。而更严重的是，由于UDP的特性，当某一片数据传送中丢失时，接收方便无法重组数据报。将导致丢弃整个UDP数据报。因此，在普通的局域网环境下，将UDP的数据控制在1472字节以下为好。

进行Internet编程时则不同，因为Internet上的路由器可能会将MTU设为不同的值。如果我们假定MTU为1500来发送数据的，而途经的某个网络的MTU值小于1500字节，那么系统将会使用一系列的机制来调整MTU值，使数据报能够顺利到达目的地。鉴于Internet上的标准MTU值为576字节，所以在进行Internet的UDP编程时，最好将UDP的数据长度控件在548字节(576-8-20)以内。

（4）UDP分片举例

IP数据报分片例如以下图所看到的，注意，仅仅有第一个分片有UDP头，可是每一个分片都有IP首部。



链路层的数据帧，刨除数据帧帧头，最多传输的长度为1500。也就是说，假设一个ip数据报，长度大于1500，则需要分片。

分片注意的点：

（1）在ip头中3位标志，13位片偏移，这俩字段就是用来分片的。

●　标志字段中的最低位记为MF(More Fragment)。MF=1即表示后面“还有分片”的数据报。MF=0表示这已是若干数据报片中的最后一个。除了最后一个分片为0，其余的分片都为1。

●　标志字段中间的一位记为DF(Don’t Fragment)，意思是“不能分片”。只有当DF=0时才允许分片。如果DF=1，即便IP数据报再长，也不分片，可能会将该IP数据报丢弃，并发送一个ICMP差错报文给发送端。

13位片偏移：用于表示相对于起始的偏移量，就是个offset。

（2）每一个分片都有一个独立的IP头，20个字节。

（3）IP的分片和组装都是在IP层完毕的，其对UDP/TCP网络层是透明的。

（4）假设在传输过程中，某个分片丢失，则须要重传整个IP数据报。不能单独传递某个分片，这主要是，假设是中间某个路由器做的分片，起始端也不知道怎样分片的，所以仅仅能重传整个IP数据报。

（5）至于重不重传。

TCP会丢包重传，可是UDP则不会，IP层是没有丢包重传机制的。

（6）传输单元，IP层叫IP数据报，链路层叫分组