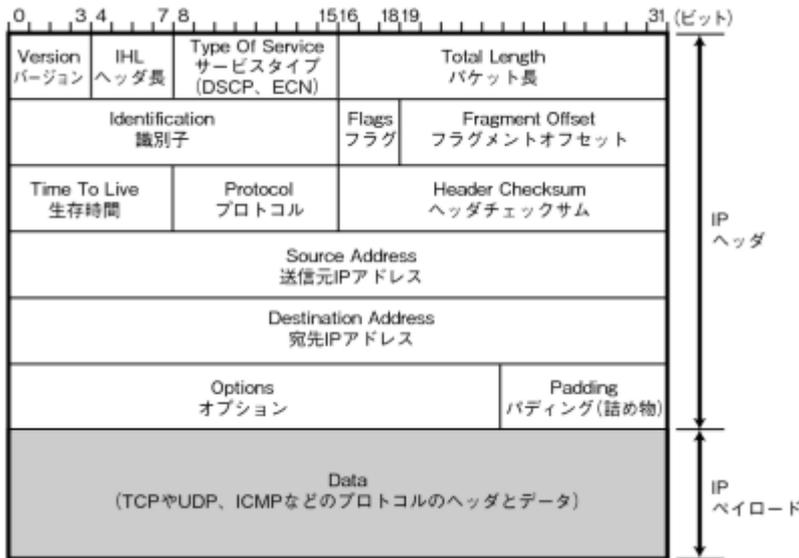


很多年前在日亚上买了这本书的电子版,现在翻来看看,把要点整理一下.

IP协议

IPv4报头

这个报头各字段我已经给学生讲过无数遍了.



不过书中给出了一些补充内容:

Version版本号

除了IPv4和IPv6之外,还有其他版本.

版本号	缩写	协议名
0~1	保留	
2~3	未分配	N/A
4	IP	Internet Protocol
5	ST	ST Datagram Mode 实验性质,可无视
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX: The Next Internet也是实现性质,可无视
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10~14	未分配	
15	保留	

官方的RFC文档如下,读一读这些协议的产生背景还是挺有意思的.



- IPv4: <https://tools.ietf.org/html/rfc791>
- ST: <https://tools.ietf.org/html/rfc1190>
- IPv6: <https://tools.ietf.org/html/rfc1752>
- TP/IX: <https://tools.ietf.org/html/rfc1475>
- PIP: <https://tools.ietf.org/html/rfc1621>

TUBA: <https://tools.ietf.org/html/rfc1347>

TUBA: TCP and UDP with Bigger Addresses

IHL: Internet Header Length 报头长度

占4比特,这个没什么好记的,单位是4字节,通常是5,表示报首长度是20字节(没有扩展项情况下)

TOS: Type of Service 服务类型

这个虽然占了8比特,分别对应优先级啊,最低延时等等特殊要求,但一般对于复杂网络来说很难实现,实际应用时经常被忽略.

DSCP和ECN

因为没有应用的余地,所以前面的TOS改为了DSCP和EDN这两个字段,DSCP是Differentiated Services Codepoint的缩写,占6个比特,如果高3位的3~5比特置0的话,则低3位的0~2比特表示优先级,000到111,数字越大优先级越高.如果5比特置1时表示实验用. ECN是Explicit Congestion Notification的缩写,当网络出现拥塞时进行通知,6比特表示通知上层(包含Layer4层以及Layer7的应用层)的协议是否要对应ECN,当ECN为1时路由器转发(即路由器要丢包时会通知 而如果发生网络拥塞时路由器会将数据包的CE位置1表示出现拥塞,先通知到接收方,接收方再将CE置1回复给发送方.

TL: Total Length 总长度

占16比特,所以最大长度为 $2^{16}=65536$ 字节,因为路由器会进行切片,要传送到Layer2只允许1500字节的Payload,所以理论最大值是达不到的.

ID: Identification 识别子

当把长的数据包切片时,到接收端要重组时,各分片需要同一个识别子才能重组.

Flags 标识位

有3个比特,0比特保留位,默认为0;1比特表示是否有分片,0表示有,1表示无;2比特表示当前片是否是最后一个分片,0表示是最后一个,1表示不是最后一个.

FO: Fragment Offset 分片偏移量

有13位,最小单位是8字节.

TTL: Time to Live 生存时间

表示数据包经过多少Hop(即路由器转发次数)会被丢弃. セキュリティポリシー：会社などの組織全体で、情報の取り扱いやセキュリティ対策についての基準や考え方などを統一し、明文化したもの。

セキュリティの構成要素 - ファイアウォール(FW) - パケットフィルタリングタイプ - アプリケーションゲートウェイタイプ

防火牆只能根据人为设置的规则Allow/Deny经过的网络流量,但无法对恶意流量进行判断.但简单的规则只是粗暴的一刀切,并不能精准打击,反而可能会殃及池鱼,所以要配合其他手段.

- IDS(侵入検知システム)

From:

<https://trident365.com/> - 三叉戟

Permanent link:

https://trident365.com/doku.php?id=resources:books:master_tcpip&rev=1732022750

Last update: **2024/11/19 22:25**

