计算机网络

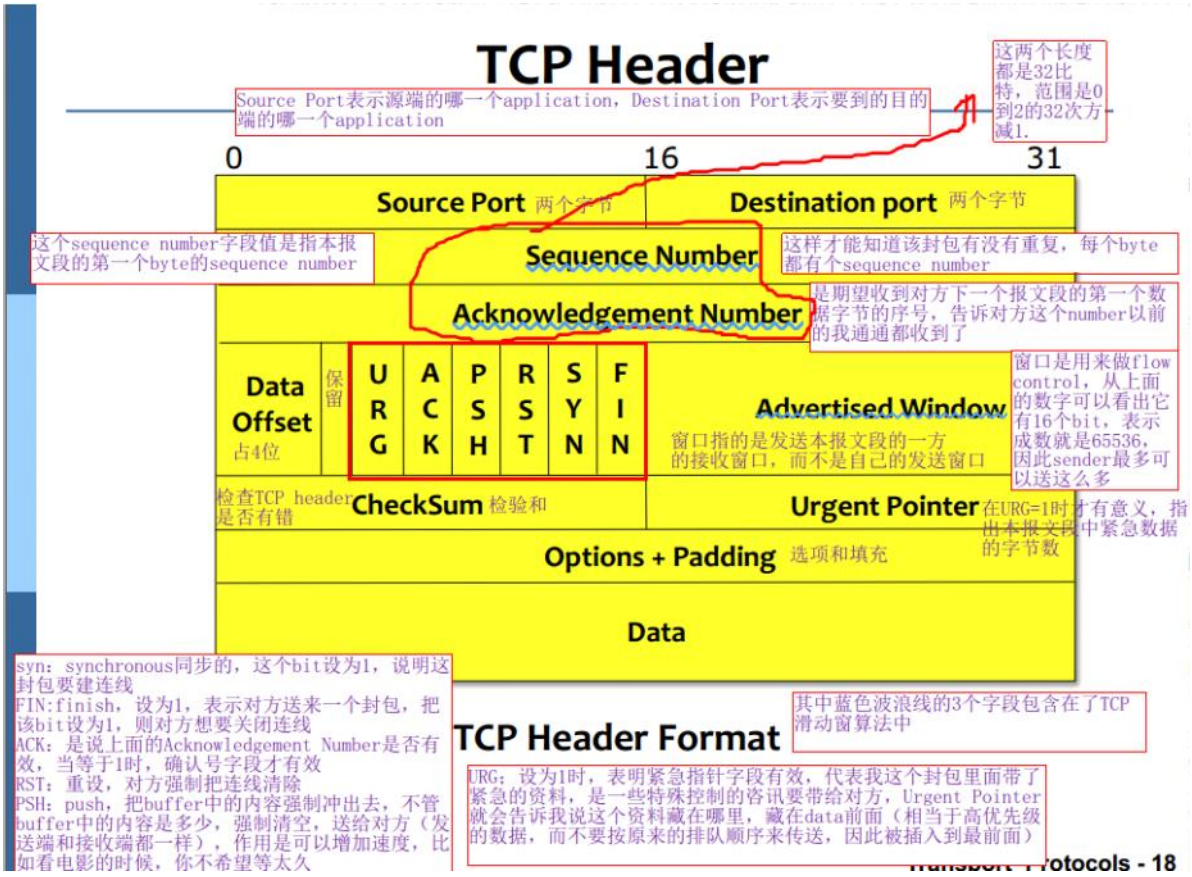
2018年6月14日 16:19

1、TCP报头格式

①TCP的特点主要有3个：（1）可靠的（2）面向连接的（3）字节流服务

②一个TCP报文段分为首部和数据两部分，而TCP的全部功能都体现在它首部的各字段的作用

③TCP报文段首部的前20个自己是固定的，因此TCP首部的最小长度是20字节



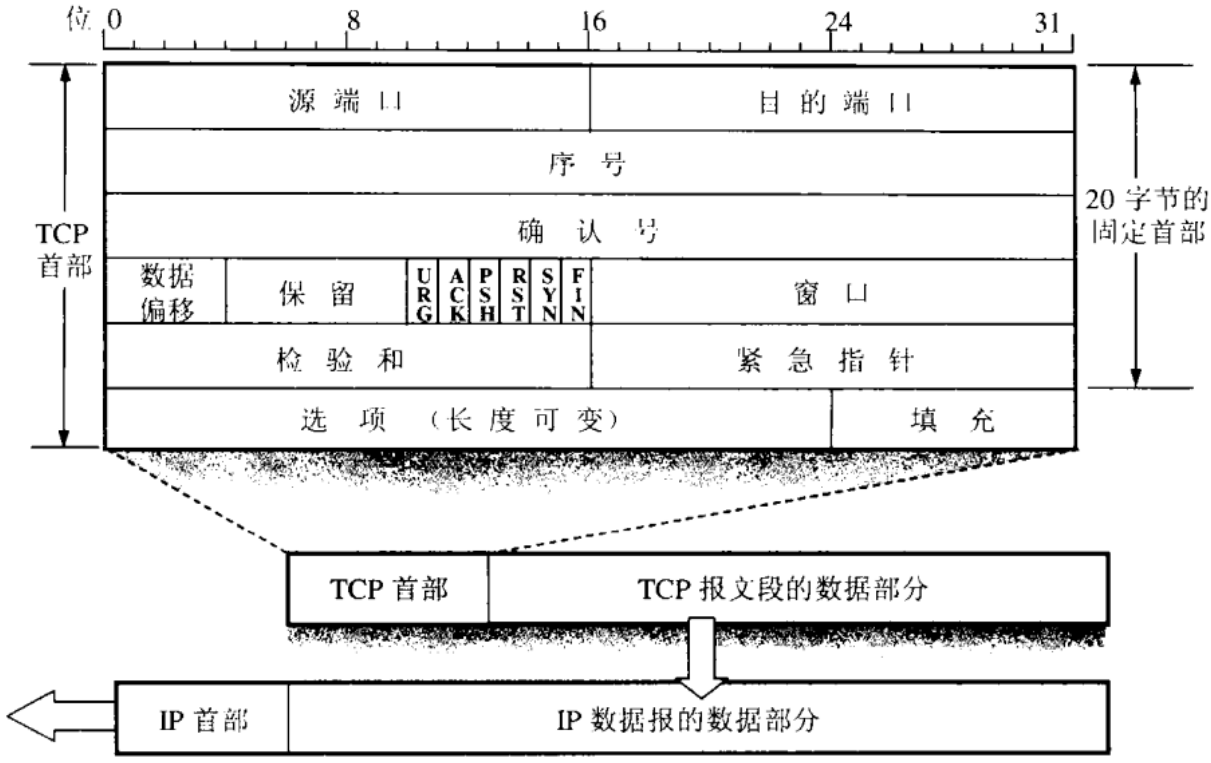


图 5-14　TCP 报文段的首部格式

（1）源端口和目的端口分别占两个字节，源端口表示源端的application，目的端口表示目的端得application

（2）序号 占四个字节，TCP是面向字节流的，在TCP中传送的字节流中的每一个字节都按顺序编号，首部中的序号字段值指的是本报文段所发送的数据的第一个字节的序号。

（3）确认号，占4字节，是期望收到对方下一个报文段的第一数据字节的序号，告诉对方这个number之前的所有数据都已经正确收到

（4）数据偏移 ，占4位，它指的是TCP报文段数据的起始处距离TCP报文的起始处有多远，这个字段实际上是TCP报文段的首部长度

（5）保留，占6位，为今后使用

（6）紧急URG，当URG=1,表明紧急指针字段有效，代表这个封包里面带了紧急的资料，是一些特殊控制的资讯要带给对方，紧急指针会告诉我说这个资料藏在哪里，藏在data的前面（相当于高优先级的数据，而不需要按原来排队的顺序来传送，因此被插入到最前面）

（7）确认ACK，ACK=1时确认字段才有效。TCP规定，在连接建立后所有传送的报文都必须把ACK置为1

（8）推送PSH，把buffer中的内容强制冲出去，不管buffer中的内容是多少，强制清空，送给对方，作用是可以增加速度，但是很少应用

（9）复位RST，重设，当RST=1时，表明TCP连接出现严重问题（主机崩溃或者其他原因，必须释放连接），然后重新建立运输连接，另外RST=1还用来拒绝一个非法报文段或拒绝打开一个连接

（10）同步SYN，当SYN=1表示这是一个连接请求或连接接受报文。连接请求报文SYN=1,ACK=0;对方同意连接请求或者连接接受报文SYN=1,ACK=1。

（11）终止FIN，用于释放一个连接，当FIN=1时，表明此报文段的发送方的数据已经发送完毕，并要求释放运输连接。

（12）窗口，占2字节。窗口作为接收方让发送方设置器发送窗口的依据，窗口字段明确表明了现在允许对方发送的数据量，窗口值是经常动态变化的。

（13）检验和，占2字节，范围包括首部和数据两个部分，在计算检验和时，要在TCP报文段前面加上12字节的伪首部。

（14）紧急指针，占2字节，只有URG=1时才有意义，指的是本报文段紧急数据的字节数

（15）选项，长度可变，最长可以达到40字节，当没有选项时,TCP首部长度是20字节。

2、UDP报头格式

UDP有两个字段：数据字段和首部字段

（1）首部字段只有8个字节，有4个字段组成，每个字段的长度都是两个字节

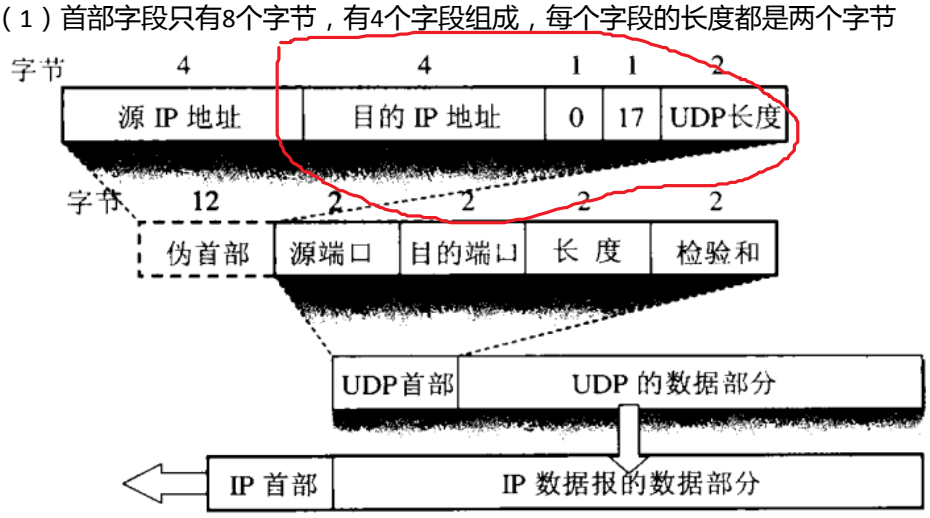


图 5-5　UDP 用户数据报的首部和伪首部

①源端口：源端口号，在需要对方回信时选用，不需要时可全用0

②目的端口号：在终点交付报文时必须要使用到

③长度：UDP用户数据报的长度，其最小值是8（仅有首部）

④校验和：检验UDP用户数据报在传输中是否有错，有错就丢弃

注意：

①UDP首部中，在计算校验和是，要在UDP用户数据报前面加12字节的伪首部

②伪首部既不向下传送也不向上提交，仅仅是为了计算校验和

③UDP的校验和是把首部和数据部分一起都校验

3.TCP和UDP的区别

TCP（Transmission Control Protocol，传输控制协议）是**基于连接**的协议，在正式收发数据前，必须和对方建立可靠的连接。一个TCP连接必须要经过三次握手才能建立起来。

2）TCP提供**可靠的数据传输**服务，通信进程能够依靠TCP无差错、有序交付所有数据。

3）TCP具有**拥塞控制**机制，该服务在发送方和接收方之间的网络出现拥塞时，抑制发送进程。这可能会导致进程通信变慢，但是对网络整体通信有好处。

UDP（User Data Protocol，用户数据报协议）是与TCP相对应的协议。

1）它是面向**非连接**的协议，它不与对方建立连接，而是直接就把数据包发送过去！（延时小）

2）UDP提供**不可靠数据传输**服务，不保证报文到达，也不保证有序到达。这种不可靠数据传输服务包括进程间的数据交付和差错检查两种服务，是运输层协议实现的最低限度服务。

3）UDP**没有拥塞控制**机制，所以UDP可以用他选定的任何速率向下层（网络层）传输数据（速度有保证）。

综合以上大致可以得出两者的适用应用：UDP适用于对**可靠性要求不高**的应用环境，但是对**数据传输速率有最小限制且对延时有要求**，例如因特网电话。TCP适用于对**数据传输可靠**性要求较高的应用，web的HTTP协议就使用TCP进行数据传输。

UDP相对TCP的优势：

（1）**无延时**。只要应用进程将数据传递给UDP，UDP就会将此数据打包进UDP报文段并立即传递给网络层。但是TCP可能会因为拥塞阻塞机制阻止运输层TCP发送方，并且一直等待，直到可以发送，这会增加时延。对实时应用，少量数据损耗并不影响，但延时不能太大，这最好使用UDP，如网络电话。

（2）**UDP无需连接建立**，相比TCP节省了三次握手时间。DNS使用UDP协议，主要是因为UDP不需要建立连接，节省

了握手时间，如果运行在TCP上，DNS会很慢。

（3）**UDP无连接状态**，而TCP需要维护连接状态，这包括维持一些参数，因此使用UDP可以使服务器同时支持更多用户。

（4）**分组开销小**，UDP使用8字节首部开销（各两字节：源端口号、目的端口号、长度、检验和），TCP使用20字节首部开销。

常见使用**TCP协议**的应用如下：

浏览器用的HTTP

FlashFXP用的FTP

Outlook用的POP、SMTP

Putty用的Telnet、SSH

QQ文件传输

常见使用**UDP协议**的应用如下：

QQ语音、QQ视频、TFTP、DNS

表 5-1　使用 UDP 和 TCP 协议的各种应用和应用层协议

应　　用	应用层协议	运输层协议
名字转换	DNS	UDP
文件传送	TFTP	UDP
路由选择协议	RIP	UDP
IP 地址配置	BOOTP, DHCP	UDP
网络管理	SNMP	UDP
远程文件服务器	NFS	UDP
IP 电话	专用协议	UDP
流式多媒体通信	专用协议	UDP
多播	IGMP	UDP
电子邮件	SMTP	TCP
远程终端接入	TELNET	TCP
万维网	HTTP	TCP
文件传送	FTP	TCP

4.HTTP状态码（最好结合使用场景，比如缓存命中时使用的那个）（状态码一共是5类，33中）

服务器返回的响应报文的第一行为状态行，包含了状态码以及原因短语，用来告知客户端请求的结果

状态码	类别	原因短语
1XX	Informational（信息性状态码）	接收的请求正在处理
2XX	Success（成功状态码）	请求正常处理完毕
3XX	Redirection（重定向状态码）	需要进行附加操作以完成请求
4XX	Client Error（客户端错误状态码）	服务器无法处理请求
5XX	Server Error（服务器错误状态码）	服务器处理请求出错

1XX信息

100 Continue：表明目前为止都很正常，客户端可以继续发送请求或者忽略这个响应

2XX成功

200 OK
204 No Content ：请求已经成功处理，但是返回的响应报文不包含实体的主体部分。一般在只需要从客户端往服务器发送信息，而不需要返回数据时使用。
206 Partial Content ：表示客户端进行了范围请求。响应报文包含由 Content-Range 指定范围的实体内容。

3XX重定向

301 Moved Permanently ：永久性重定向

302 Found ：临时性重定向

303 See Other ：和 302 有着相同的功能，但是 303 明确要求客户端应该采用 GET 方法获取资源。

注：虽然 HTTP 协议规定 301、302 状态下重定向时不允许把 POST 方法改成 GET 方法，但是大多数浏览器都会在 301、302 和 303 状态下的重定向把 POST 方法改成 GET 方法。

304 Not Modified ：如果请求报文首部包含一些条件，例如：If-Match，If-Modified-Since，If-None-Match，If-Range，If-Unmodified-Since，如果不满足条件，则服务器会返回 304 状态码。

307 Temporary Redirect ：临时重定向，与 302 的含义类似，但是 307 要求浏览器不会把重定向请求的 POST 方法改成 GET 方法。

4XX客户端错误

400 Bad Request ：请求报文中存在语法错误。

401 Unauthorized ：该状态码表示发送的请求需要有认证信息（BASIC 认证、DIGEST 认证）。如果之前已进行过一次请求，则表示用户认证失败。

403 Forbidden ：请求被拒绝，服务器端没有必要给出拒绝的详细理由。

404 Not Found

5XX服务器错误

500 Internal Server Error ：服务器正在执行请求时发生错误。

503 Service Unavilable ：服务器暂时处于超负载或正在进行停机维护，现在无法处理请求。

2开头（请求成功）表示成功处理了请求，通常表示服务器提供了请求的网页
200（成功）服务器成功处理了请求
201（已创建） 请求成功并且服务器创建了新的资源
202（已接受）服务器已接受请求，但尚未处理
203（非授权信息）服务器已成功处理了请求，但返回的信息可能来自另一来源
204（无内容）服务器成功处理了请求，但没有返回任何内容
205（重置内容）服务器成功处理了请求，但没有返回任何内容
206（部分内容）服务器成功处理了GET请求
3开头（请求被重定向）表示要完成请求，需要进一步操作。通常这些状态代码用来重定向
300（多种选择）针对请求，服务器可执行多种操作
301（永久移动）请求的网页已永久移动到新位置。服务器返回此响应时，会自动将请求者转到新的位置
302（临时移动）服务器目前从不同位子的网页响应请求，但请求者应继续使用原有位置进行以后的请求

303（查看其它位置）请求者应当对不同的位置使用单独的GET请求来检索响应，返回此代码

304（未修改）自从上次请求后，请求网页未修改过。服务器返回此响应时，不会返回网页内容。

305（使用代理）请求者只能使用代理访问请求的网页

307（临时重定向）服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置进行以后的请求

4开头（请求错误）这些状态码表示请求可能出错，妨碍了服务器的处理

400 （错误请求） 服务器不理解请求的语法。

401 （未授权） 请求要求身份验证。 对于需要登录的网页，服务器可能返回此响应。

403 （禁止） 服务器拒绝请求。

404 （未找到） 服务器找不到请求的网页。

405 （方法禁用） 禁用请求中指定的方法。

406 （不接受） 无法使用请求的内容特性响应请求的网页。

407 （需要代理授权） 此状态代码与 401（未授权）类似，但指定请求者应当授权使用代理。

408 （请求超时） 服务器等候请求时发生超时。

409 （冲突） 服务器在完成请求时发生冲突。 服务器必须在响应中包含有关冲突的信息。

410 （已删除） 如果请求的资源已永久删除，服务器就会返回此响应。

411 （需要有效长度） 服务器不接受不含有效内容长度标头字段的请求。

412 （未满足前提条件） 服务器未满足请求者在请求中设置的其中一个前提条件。

413 （请求实体过大） 服务器无法处理请求，因为请求实体过大，超出服务器的处理能力。

414 （请求的 URI 过长） 请求的 URI（通常为网址）过长，服务器无法处理。

415 （不支持的媒体类型） 请求的格式不受请求页面的支持。

416 （请求范围不符合要求） 如果页面无法提供请求的范围，则服务器会返回此状态代码。

417 （未满足期望值） 服务器未满足"期望"请求标头字段的要求。

5开头（服务器错误）这些状态代码表示服务器在尝试处理请求时发生内部错误。 这些错误可能是服务器本身的错误，而不是请求出错。

500 （服务器内部错误） 服务器遇到错误，无法完成请求。

501 （尚未实施） 服务器不具备完成请求的功能。 例如，服务器无法识别请求方法时可能会返回此代码。

502 （错误网关） 服务器作为网关或代理，从上游服务器收到无效响应。

503 （服务不可用） 服务器目前无法使用（由于超载或停机维护）。 通常，这只是暂时状态。

504 （网关超时） 服务器作为网关或代理，但是没有及时从上游服务器收到请求。

505 （HTTP 版本不受支持） 服务器不支持请求中所用的 HTTP 协议版本。

以下3种状态行为在响应报文中是经常见到的

HTTP /1.1 202 Accepted {接受}

HTTP/ 1.1 400 Bad request {错误的请求}

HTTP/1.1 404 Not Found {找不到}

若请求的网页从 http://www.ee.xyz.edu/index.html 转移到了一个新的地址，则响应报文

的状态行和一个首部行就是下面的形式：

```
HTTP/1.1 301 Moved Permanently          {永久性地转移了}
Location: http://www.xyz.edu/ee/index.html    {新的 URL}
```

常见状态码

100 Continue 继续，一般在发送post请求时，已发送了http、header之后服务端将返回此信息，表示确认，之后发送具体参数信息

200 OK 正常返回信息

201 Created 请求成功并且服务器创建了新的资源

301 Moved Permanently 请求的网页已永久移动到新位置。

400 Bad Request 服务器无法理解请求的格式，客户端不应当尝试再次使用相同的内容发起请求。

404 Not Found 找不到如何与 URI 相匹配的资源。

500 Internal Server Error 最常见的服务器端错误。

详细

1xx - 信息提示

这些状态代码表示临时的响应。客户端在收到常规响应之前，应准备接收一个或多个 1xx 响应。

· 100 - Continue 初始的请求已经接受，客户应当继续发送请求的其余部分。（HTTP 1.1新）

· 101 - Switching Protocols 服务器将遵从客户的请求转换到另外一种协议（HTTP 1.1新）

2xx - 成功

这类状态代码表明服务器成功地接受了客户端请求。

· 200 - OK 一切正常，对GET和POST请求的应答文档跟在后面。

· 201 - Created 服务器已经创建了文档，Location头给出了它的URL。

· 202 - Accepted 已经接受请求，但处理尚未完成。

· 203 - Non-Authoritative Information 文档已经正常地返回，但一些应答头可能不正确，因为使用的是文档的拷贝，非权威性信息（HTTP 1.1新）。

· 204 - No Content 没有新文档，浏览器应该继续显示原来的文档。如果用户定期地刷新页面，而Servlet可以确定用户文档足够新，这个状态代码是很有用的。

· 205 - Reset Content 没有新的内容，但浏览器应该重置它所显示的内容。用来强制浏览器清除表单输入内容（HTTP 1.1新）。

· 206 - Partial Content 客户发送了一个带有Range头的GET请求（分块请求），服务器完成了它（HTTP 1.1新）。

3xx - 重定向

客户端浏览器必须采取更多操作来实现请求。例如，浏览器可能不得不请求服务器上的不同的页面，或通过代理服务器重复该请求。

· 300 - Multiple Choices 客户请求的文档可以在多个位置找到，这些位置已经在返回的文档内列出。如果服务器要提出优先选择，则应该在Location应答头指明。

· 301 - Moved Permanently 客户请求的文档在其他地方，新的URL在Location头中给出，浏览器应该自动地访问新的URL。

· 302 - Found 类似于301，但新的URL应该被视为临时性的替代，而不是永久性的。注意，在HTTP1.0中对应的状态信息是“Moved Temporatily”。出现该状态代码时，浏览器能

够自动访问新的URL，因此它是一个很有用的状态代码。注意这个状态代码有时候可以和301替换使 用。例如，如果浏览器错误地请求 http://host/~user （缺少了后面的斜杠）

，有的服务器返回301，有的则返回302。严格地说，我们只能假定只有当原来的请求是GET时浏览器才会自动重定向。请参见307。

· 303 - See Other 类似于301/302，不同之处在于，如果原来的请求是POST，Location头指定的重定向目标文档应该通过GET提取（HTTP 1.1新）。

· 304 - Not Modified 客户端有缓冲的文档并发出了一个条件性的请求（一般是提供If-Modified-Since头表示客户只想比指定日期更新的文档）。服务器告诉客户，原来缓冲的

文档还可以继续使用。
· 305 - Use Proxy 客户请求的文档应该通过Location头所指明的代理服务器提取（HTTP 1.1新）。
· 307 - Temporary Redirect 和302（Found）相同。许多浏览器会错误地响应302应答进行重定向，即使原来的请求是POST，即使它实际上只能在POST请求的应答是303时 才能重
定向。由于这个原因，HTTP 1.1新增了307，以便更加清除地区分几个状态代码：当出现303应答时，浏览器可以跟随重定向的GET和POST请求；如果是307应答，则浏览器只 能跟随
对GET请求的重定向。（HTTP 1.1新）
4xx - 客户端错误
发生错误，客户端似乎有问题。例如，客户端请求不存在的页面，客户端未提供有效的身份验证信息。
· 400 - Bad Request 请求出现语法错误。
· 401 - Unauthorized 访问被拒绝，客户试图未经授权访问受密码保护的页面。应答中会包含一个WWW-Authenticate头，浏览器据此显示用户名字/密码对话框，然后在 填写合
适的Authorization头后再次发出请求。IIS 定义了许多不同的 401 错误，它们指明更为具体的错误原因。这些具体的错误代码在浏览器中显示，但不在 IIS 日志中显示：
· 401.1 - 登录失败。
· 401.2 - 服务器配置导致登录失败。
· 401.3 - 由于 ACL 对资源的限制而未获得授权。
· 401.4 - 筛选器授权失败。
· 401.5 - ISAPI/CGI 应用程序授权失败。
· 401.7 – 访问被 Web 服务器上的 URL 授权策略拒绝。这个错误代码为 IIS 6.0 所专用。
· 403 - Forbidden 资源不可用。服务器理解客户的请求，但拒绝处理它。通常由于服务器上文件或目录的权限设置导致。禁止访问：IIS 定义了许多不同的 403 错误，它们指
明更为具体的错误原因：
· 403.1 - 执行访问被禁止。
· 403.2 - 读访问被禁止。
· 403.3 - 写访问被禁止。
· 403.4 - 要求 SSL。
· 403.5 - 要求 SSL 128。
· 403.6 - IP 地址被拒绝。
· 403.7 - 要求客户端证书。
· 403.8 - 站点访问被拒绝。
· 403.9 - 用户数过多。
· 403.10 - 配置无效。
· 403.11 - 密码更改。
· 403.12 - 拒绝访问映射表。
· 403.13 - 客户端证书被吊销。
· 403.14 - 拒绝目录列表。
· 403.15 - 超出客户端访问许可。
· 403.16 - 客户端证书不受信任或无效。
· 403.17 - 客户端证书已过期或尚未生效。
· 403.18 - 在当前的应用程序池中不能执行所请求的 URL。这个错误代码为 IIS 6.0 所专用。
· 403.19 - 不能为这个应用程序池中的客户端执行 CGI。这个错误代码为 IIS 6.0 所专用。
· 403.20 - Passport 登录失败。这个错误代码为 IIS 6.0 所专用。
· 404 - Not Found 无法找到指定位置的资源。这也是一个常用的应答。

· 404.0 -（无）– 没有找到文件或目录。
· 404.1 - 无法在所请求的端口上访问 Web 站点。
· 404.2 - Web 服务扩展锁定策略阻止本请求。
· 404.3 - MIME 映射策略阻止本请求。
· 405 - Method Not Allowed 请求方法（GET、POST、HEAD、DELETE、PUT、TRACE等）对指定的资源不适用，用来访问本页面的 HTTP 谓词不被允许（方法不被允许）（HTTP 1.1
新）
· 406 - Not Acceptable 指定的资源已经找到，但它的MIME类型和客户在Accpet头中所指定的不兼容，客户端浏览器不接受所请求页面的 MIME 类型（HTTP 1.1新）。
· 407 - Proxy Authentication Required 要求进行代理身份验证，类似于401，表示客户必须先经过代理服务器的授权。（HTTP 1.1新）
· 408 - Request Timeout 在服务器许可的等待时间内，客户一直没有发出任何请求。客户可以在以后重复同一请求。（HTTP 1.1新）
· 409 - Conflict 通常和PUT请求有关。由于请求和资源的当前状态相冲突，因此请求不能成功。（HTTP 1.1新）
· 410 - Gone 所请求的文档已经不再可用，而且服务器不知道应该重定向到哪一个地址。它和404的不同在于，返回407表示文档永久地离开了指定的位置，而404表示由于未知的
原因文档不可用。（HTTP 1.1新）
· 411 - Length Required 服务器不能处理请求，除非客户发送一个Content-Length头。（HTTP 1.1新）
· 412 - Precondition Failed 请求头中指定的一些前提条件失败（HTTP 1.1新）。
· 413 – Request Entity Too Large 目标文档的大小超过服务器当前愿意处理的大小。如果服务器认为自己能够稍后再处理该请求，则应该提供一个Retry-After头（HTTP 1.1
新）。
· 414 - Request URI Too Long URI太长（HTTP 1.1新）。
· 415 – 不支持的媒体类型。
· 416 – Requested Range Not Satisfiable 服务器不能满足客户在请求中指定的Range头。（HTTP 1.1新）· 417 – 执行失败。
· 423 – 锁定的错误。

5xx - 服务器错误

服务器由于遇到错误而不能完成该请求。
· 500 - Internal Server Error 服务器遇到了意料不到的情况，不能完成客户的请求。
· 500.12 - 应用程序正忙于在 Web 服务器上重新启动。
· 500.13 - Web 服务器太忙。
· 500.15 - 不允许直接请求 Global.asa。
· 500.16 – UNC 授权凭据不正确。这个错误代码为 IIS 6.0 所专用。
· 500.18 – URL 授权存储不能打开。这个错误代码为 IIS 6.0 所专用。
· 500.100 - 内部 ASP 错误。
· 501 - Not Implemented 服务器不支持实现请求所需要的功能，页眉值指定了未实现的配置。例如，客户发出了一个服务器不支持的PUT请求。
· 502 - Bad Gateway 服务器作为网关或者代理时，为了完成请求访问下一个服务器，但该服务器返回了非法的应答。亦说Web 服务器用作网关或代理服务器时收到了无效响应
。
· 502.1 - CGI 应用程序超时。
· 502.2 - CGI 应用程序出错。
· 503 - Service Unavailable 服务不可用，服务器由于维护或者负载过重未能应答。例如，Servlet可能在数据库连接池

已满的情况下返回503。服务器返回503时可以提供一个
Retry-After头。这个错误代码为 IIS 6.0 所专用。
· 504 - Gateway Timeout 网关超时，由作为代理或网关的服务器使用，表示不能及时地从远程服务器获得应答。（HTTP 1.1新）。
· 505 - HTTP Version Not Supported 服务器不支持请求中所指明的HTTP版本。（HTTP 1.1新）

5.HTTP协议（一些报头字段的作用，如cace-control、keep-alive）

Http有两类报文：
（1）请求报文------从客户端向服务端发送请求的报文
（2）响应报文-----从服务器到客户的回答

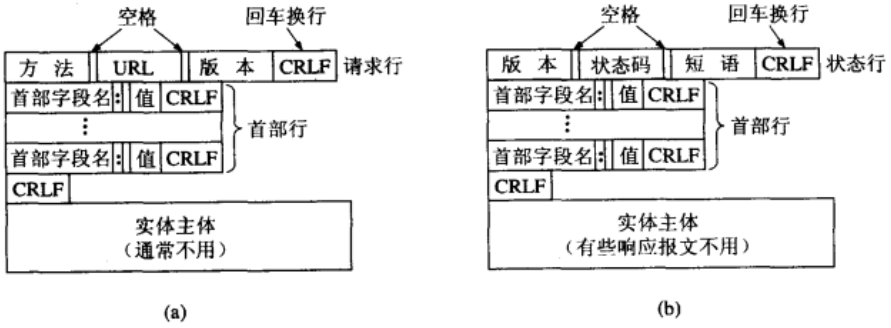


图 6-12 HTTP 的报文结构：(a) 请求报文；(b) 响应报文

Http是面向文本的
Http的请求报文和响应报文都是由3部分组成
（1）开始行，用来区分是请求报文还是响应报文，最后的“CR"代表”回车“，”LF"表示“换行”
（2）首部行，用来说明浏览器、服务器或报文主体的一些信息，可以有一行或者多行，每一行结束的地方都要有“回车”或“换行”。整个首部行结束时，还有一空行将首部行和后面的实体主体分开
（3）实体主体，在请求报文段中一般不用这个字段，而在响应报文中也可能没有这个字段
①Http请求报文的特点：
（一）请求报文的第一行“请求行”只有3个内容：即方法、请求资源的URL，以及HTTP的版本

表 6-1 HTTP 请求报文的一些方法

方法（操作）	意 义
OPTION	请求一些选项的信息
GET	请求读取由 URL 所标志的信息
HEAD	请求读取由 URL 所标志的信息的首部
POST	给服务器添加信息（例如，注释）
PUT	在指明的 URL 下存储一个文档
DELETE	删除指明的 URL 所标志的资源
TRACE	用来进行环回测试的请求报文
CONNECT	用于代理服务器

对于我们在图 6-9 中的例子，即要链接到“清华大学院系设置”的页面。HTTP 的请求报文的开始行（即请求行）应当是（请注意在 GET 后面和 HTTP/1.1 前面的空格）：

```
GET http://www.tsinghua.edu.cn/chn/yxsz/index.htm HTTP/1.1
```

下面是一个请求报文的例子：

```
GET /chn/yxsz/index.htm HTTP/1.1    {请求行使用了相对 URL}
Host: www.tsinghua.edu.cn    {此行是首部行的开始。这行给出主机的域名}
Connection: close    {告诉服务器发送完请求的文档后就可释放连接}
User-Agent: Mozilla/5.0    {表明用户代理是使用 Netscape 浏览器}
Accept-Language: cn    {表示用户希望优先得到中文版本的文档}
{请求报文的最后还有一个空行}
```

②响应报文的主要特点

每一个请求报文发出后，都能收到一个响应报文，响应报文的第一行就是状态行

状态行包括三项内容，即HTTP的版本，状态码，以及解释状态码的简单短语，状态码一共有5大类共33种；

1xx 表示通知信息的，如请求收到了或正在进行处理。

2xx 表示成功，如接受或知道了。

3xx 表示重定向，如要完成请求还必须采取进一步的行动。

4xx 表示客户的差错，如请求中有错误的语法或不能完成。

5xx 表示服务器的差错，如服务器失效无法完成请求。

下面三种状态行在响应报文中是经常见到的。

```
HTTP/1.1 202 Accepted              {接受}
HTTP/1.1 400 Bad Request           {错误的请求}
Http/1.1 404 Not Found             {找不到}
```

Keep-Alive 功能使客户端到服务器端的连接持续有效（**长连接**），当出现对服务器的后继请求时，Keep-Alive 功能避免了建立或者重新建立连接。市场上的大部分 Web 服务器，包括 iPlanet、IIS 和 Apache，都支持 HTTP Keep-Alive。对于提供静态内容的网站来说，这个功能通常很有用。但是，对于负担较重的网站来说，这里存在另外一个问题：虽然为客户保留打开的连接有一定的好处，但它同样影响了性能，因为在处理暂停期间，本来可以释放的资源仍旧被占用。当Web服务器和应用服务器在同一台机器上运行时，Keep-Alive 功能对资源利用的影响尤其突出。 这样一来，客户端和服务器之间的 HTTP 连接就会被保持，不会断开（超过 Keep-Alive 规定的时间，意外断电等情况除外），当客户端发送另外一个请求时，就使用这条已经建立的连接。

6.OSI协议、TCP/IP协议以及每层对应的协议

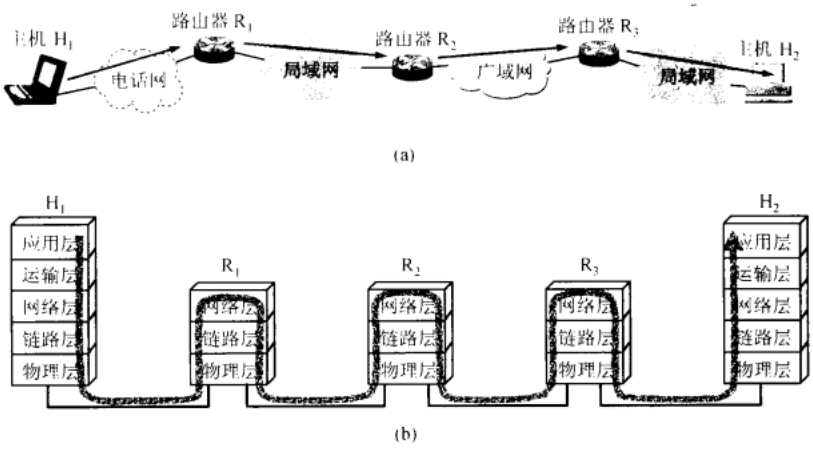


图 3-1　数据链路层的地位：(a) 主机 H_1 向 H_2 发送数据；(b) 从层次上看数据的流动

H_1 的链路层→R_1 的链路层→R_2 的链路层→R_3 的链路层→H_2 的链路层

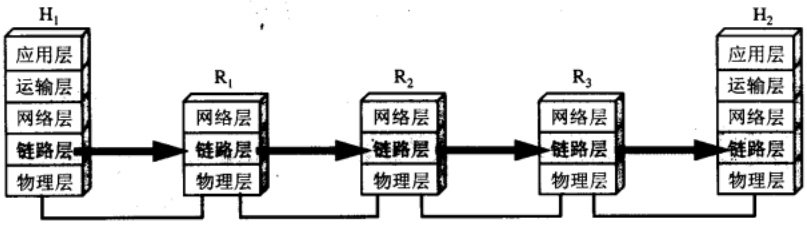
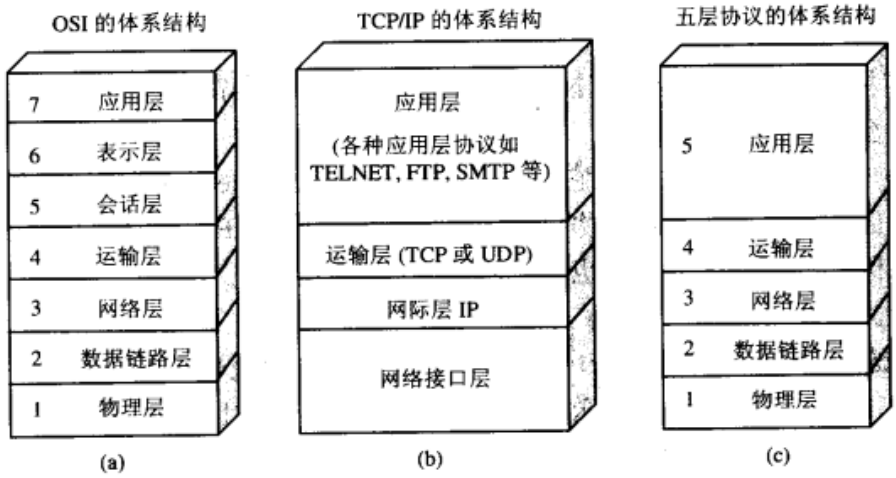


图 3-2　只考虑数据在数据链路层的流动



16　计算机网络体系结构：(a) OSI 的七层协议；(b) TCP/IP 的四层协议；(c) 五层协议

（1）应用层，体系结构中的最高层，应用层协议的定义是**应用进程间通信和交互的规则。**应用层的协议有很多

TFTP、HTTP、SNMP、FTP、SMTP、DNS 、Telnet

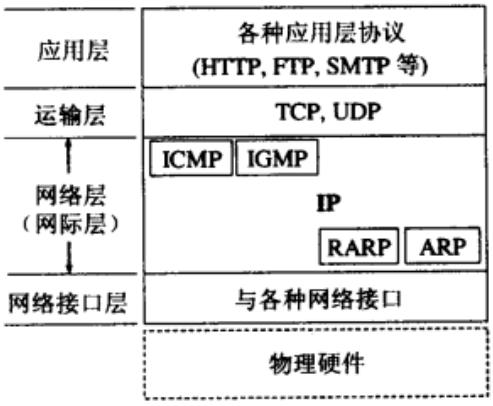
（2）运输层，任务是**负责向两个主机中的进程之间的通信提供通用的数据传输服务。**运输层主要使用以下两种协议：

传输控制协议（TCP）-----提供面向连接的、可靠的数据传输服务，其数据传输单位是**报文段**

和用户数据报协议（UDP）----提供无连接的、尽最大努力的数据传输服务（不保证传输的可靠性），其传输的基本单位是**用户数据报**

（3）网络层，主要负责**为分组交换网上的不同主机提供通信服务。**在发送数据时，网络层将运输层产生的报文段或用户数据报封装成**分组或包**进行传送，分组也称IP数据报或者数据报（和UDP的用户数据报不同）。协议有：

IP、ICMP、ARP、RARP、OSPF、IPX、RIP、IGRP



（4）数据链路层（链路层），将网络层交下来的IP数据报组装成帧，在相邻结点间的链路上传送，每一帧包括数据和必要的控制信息（如同步信息、地址信息、差错控制等）。协议：PPP、FR、HDLC、VLAN、MAC（网桥，交换机）

（5）物理层，在物理层上传输的数据单位是**比特。**协议：RJ45 、CLOCK、 IEEE802.3（中继器，集线器，网关）

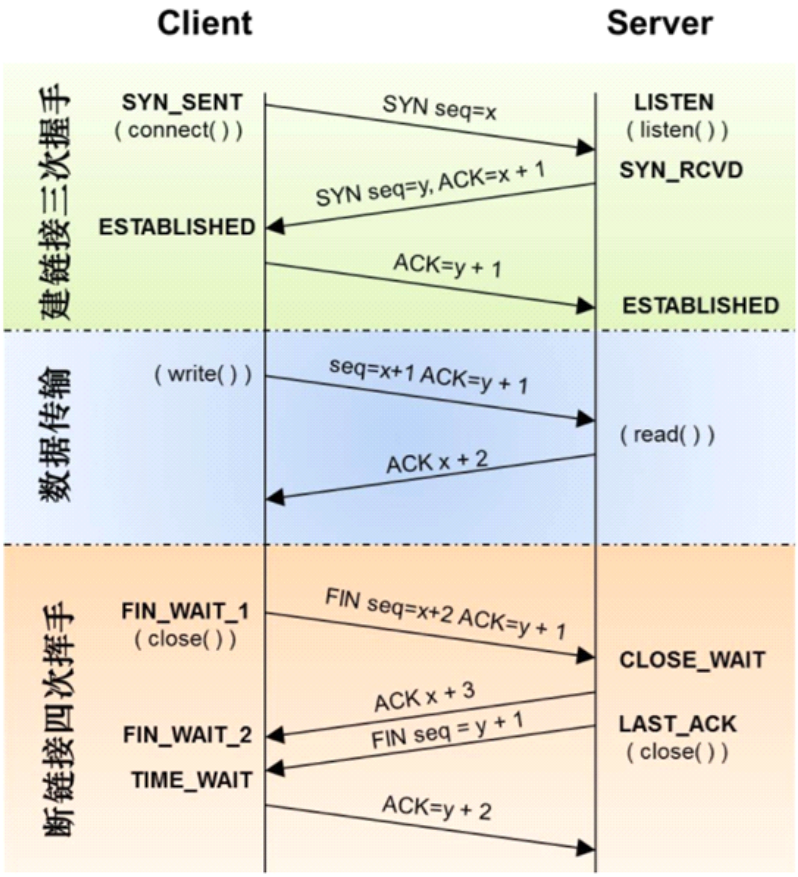
7.SESSION机制、cookie机制

（1）Http协议是无状态的，Cookie主要是为了让HTTP协议尽可能简单，使他能够处理大量事务。HTTP/1.1引入

Cookies来保存状态信息。
Cookie是服务器发送到用户浏览器并保存在本地的一小块数据，它会在浏览器下次想同一服务器再发起请求时被携带并发送到服务器上。它用于告知服务端两个请求是否来自同一浏览器，并保持用户的登录状态。
用途：①会话状态管理（如用户登录状态、购物车、游戏分数或其他需要记录的信息）
②个性化设置（如用户自定义设置、主题等）③浏览器行为跟踪（如跟踪分析用户行为）
Cookie曾一度用于客户端数据的存储，因为当时并没有其他合适的存储办法而作为唯一的存储手段，但现在随着现代浏览器开始支持各种各样的存储方式，Cookie渐渐被淘汰。由于服务器指定Cookies后，浏览器每次请求都会携带Cookie数据，会带来额外的性能开销（尤其是在移动环境下）。新的浏览器的API已经允许开发者直接蒋书记存储到本地，如使用Web storage API（本地存储 和会话存储）或IndexedDB
（2）除了可以将用户信息通过Cookie存储在用户浏览器中，也可以利用Session存储在服务器端，存储在服务器端的信息更加安全
Session可以存储在服务器上的文件、数据库或者内存中，现在最常见的是将Session存储在内存型数据库中，比如Redis。
使用Session维护用户登录的过程如下：
①用户进行登录时，用户体检包含用户名和密码的表单，放入HTTP请求报文中；
②服务器验证该用户名和密码
③如果正确则把用户信息存入Redis中，它在Redis中的ID称为Session ID
④服务器返回的响应报文的Set-Cookie首部字段包含了这个Session ID，客户端收到响应报文之后将该Cookie值存入浏览器中
⑤客户端之后对同一个服务器进行请求时会包含该Cookie值，服务器收到之后提取Session ID，从Redis中取出用户信息，继续之后的业务操作
应该注意到Session ID的安全性问题，不能让它被恶意攻击装轻易获取，那么就不能产生一个同一被猜到的Session ID值。此外，还需要经常重新生成Session ID。在对安全性要求极高的场景下，例如转账等操作，除了使用Session管理用户状态之外，还需要对用户进行重新验证，比如重新输入密码，或者短信验证码等方式。
（3）Cookie与Session选择
①Cookie只能存储ASCII码字符串，而Session则可以存储任意类型的数据，因此考虑数据复杂性时首选Session
②Cookie存储在浏览器中，容易被而已查看。如果非要将一些隐私数据存在Cookie中，可以将Cookie值进行加密，然后存储在服务器进行解密
③对于大型网站，例如用户所有信息都存储在Session中，那么开销是非常大的，因此不建议将所有用户信息都存储在Session中

8.TCP三次握手、四次挥手（这个问题真的是要回答吐了，不过真的是面试官最喜欢问的，建议每天手撸一遍，而且不仅是每次请求的过程，各种FIN_WAIT、TIME_WAIT状态也要掌握）

三次握手的过程：



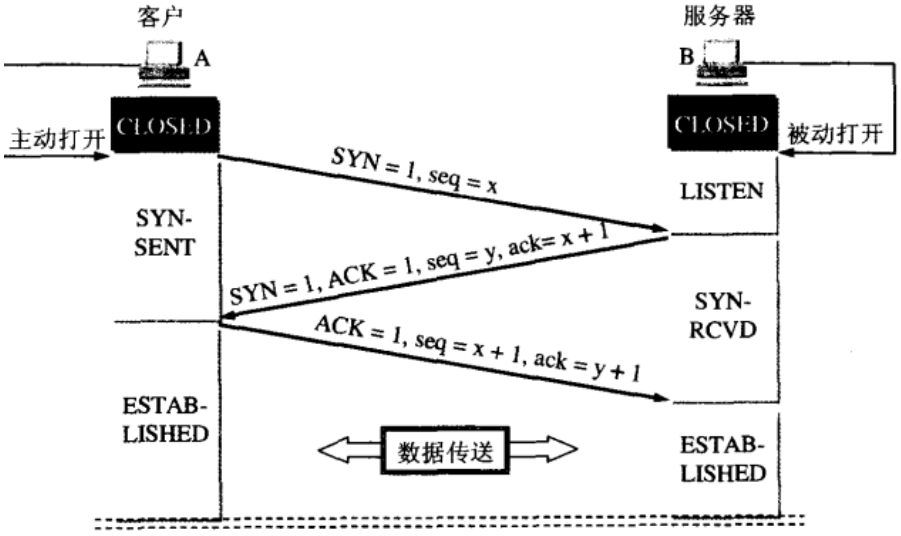


图 5-31　用三次握手建立 TCP 连接

（1）三次握手的过程

假设主机A是TCP客户程序，B是运行服务器程序，最开始两个服务器程序都是除以CLOSED状态，A主动打开连接,B被动打开连接

B的TCP服务器进程先创建传输控制模块TCB，准备接收客户进程的连接请求，然后服务进程就处于LISTEN（收听）状态，等待客户的连接请求，如果A有请求，即作出响应。

①A的客户进程也是首先创建传输控制模块TCB,然后向B 发送连接请求报文段，此时首部的同步位SYN=1,初始序列号seq=x，此时A进入SYN-SENT（同步已发送）状态；

②B收到连接请求报文段后，如果同意建立连接，则向A发送确认。在确认报文段中SYN=1,ACK=1,确认号ack=x+1,初始序列号seq=y。此时B的进程进入SYN-RCVD（同步收到）状态。

③A进程收到B的确认后，还要向B给出确认。确认报文段ACK=1,确认号ack=y+1，序列号seq=x+1。这时TCP连接已

经建立，A进入ESTABLISHED（已建立连接）状态；当B收到A的确认后，也进入ESTABLISHED状态。

为什么要用“三次握手”而不使用“二次握手”？

主要是为了防止已失效的连接请求报文段突然有传到了B，因而产生错误；“已失效的连接请求报文段”是这样产生的，A发出连接请求，但是因连接请求报文丢失而未收到确认。于是A再重传一次连接请求，后来收到了确认，建立了连接。数据传输完毕后，就释放了连接。A共发送了两个连接请求报文段，其中第一个丢失，第二个到达了B。没有“已失效的连接请求报文段”。假设出现一种异常，即A发出第一个连接请求并没有丢失，而是某些网络结点长时间滞留了，以致延误连接释放以后的某个时间才到达B。本来是一个早就失效的报文段。但B收到此失效的连接请求保温断后，就误以为是A又发出了新的连接请求，于是就向A发出确认报文段，同意建立连接，假设不采用三次握手，那只要发出确认，新的连接就建立了，由于只采用两次握手，A不会理睬B的确认，也不会向B发送数据，但B却以为新的运输连接已经建立了，并一直等待A发来的数据，B的许多资源就这样这样白白浪费了。

（2）四次挥手

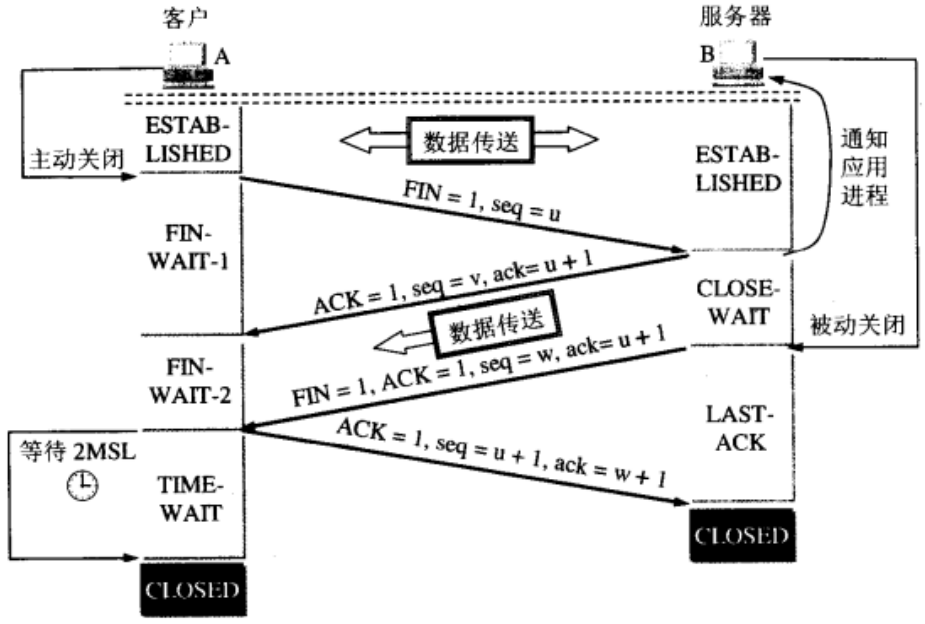


图 5-32　TCP 连接释放的过程

数据传输结束后，通信双方都可以释放连接。现在A和B都处于ESTABLISHED状态。A的应用进程先向其TCP发出连接释放报文段，并停止再发送数据，主动关闭TCP连接。

①A的应用进程先向其TCP发出连接释放报文段，并停止再发送数据，主动关闭TCP连接。A把连接释放报文段首部的FIN置为1，序列号seq=u，这个序列号等于前面传送过的数据的最后一个字节序列号加1。这时A进入FIN-WAIT-1（终止等待）状态，等待B的确认。（TCP规定，FIN报文段即使不携带数据，它也消耗掉一个序号）

②B收到连接释放报文段即发出确认，确认号是ack=u+1,序列号seq=v,（此序列号等于前面已传送过的数据的最后一个字节的序号加1），然后B进入CLOSE-WAIT（关闭等待）状态。TCP服务器进程这时应通知高层应用进程，因而从A到B这个方向的连接就释放了，这时TCP连接处于半关闭状态，即A已经没有数据要发送了，但若B若发送数据，A仍要接收，就是说从B到A这个方向的连接并未关闭，这个连接可能会持续一段时间。

③A收到来自B的确认后进入FIN-WAIT-2（终止等待2）状态，等待B发出的连接释放报文段。如果B已经没有要向A发送的数据，则应用进程就通知TCP释放连接，这时B发出的连接释放报文段必须使FIN=1。假设B的序号是w（在半关闭状态B可能又发送了一些数据）。B还必须重复上次已发送过的确认号ack=u+1,这时B就进入了LAST-ACK（最后确认状态），等待A的确认。

④A收到B的连接释放的报文段后，必须对此发出确认。再确认报文段：ACK=1,确认号ack=w+1，自己的序号seq=u+1，然后进入TIME-WAIT（时间等待）状态。但是此时TCP连接还没有释放掉，必须经过时间等待计时器（TIME-WAIT timer）设置的时间2MSL后，A才能进入CLOSED状态。

为什么A要在TIME_WAIT状态必须等待2MSL的时间？（原因有两个）

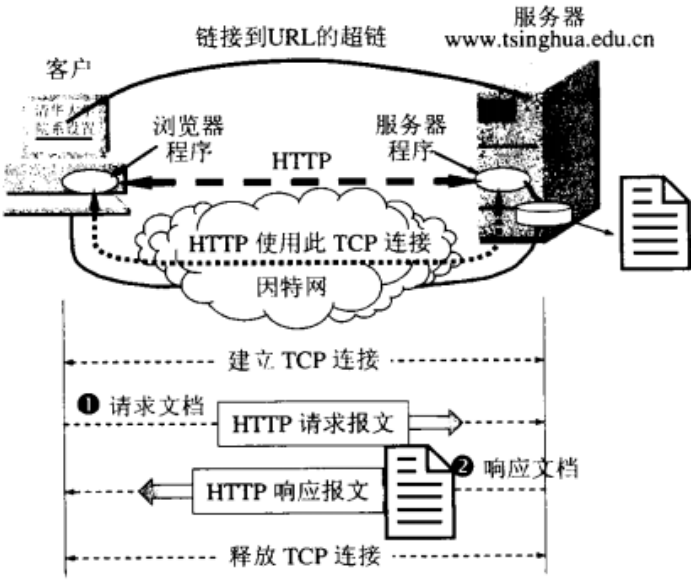
第一，为了保证A发送的最后一个ACK报文段能够到达B，这个ACK报文段有可能丢失，因而使处在LAST-ACK状态的B

收不到对已发送的FIN+ACK报文段的确认。

第二，防止“已失效的连接请求报文段”出现在本连接中。

9.打开网页到页面显示之间的过程（涵盖了各个方面，DNS解析过程，Nginx请求转发，连接建立和保持的过程，浏览器内容渲染过程，考虑的越详细越好）

HTTP协议定义了浏览器怎样向万维服务器请求万维网文档，以及服务器怎样把文档传给浏览器，**从层次上来说HTTP协议是面向事务的应用层协议，**



（一）当输入http://www.tsinghua.edu.cn/chn/yxsz/index.htm用Http/1.0更具体地说明接下来发生的事件：

（1）浏览器分析链接指向页面的URL

（2）浏览器向DNS请求解析www.tsinghua.edu.cn的IP地址

（3）域名解析系统DNS解析出清华大学的服务器的IP地址为166.111.4.100

（4）浏览器与服务器建立TCP连接（在服务器端IP地址是166.111.4.100，端口是80）

（5）向浏览器发出取文件命令：GET /chn/yxsz/index.htm

（6）服务器www.tsinghua.edu.cn给出响应，把文件index.htm发送给浏览器

（7）释放TCP连接

（8）浏览器显示“清华大学院系设置”文件index.htm中的所有文本

（二）

DNS解析----------》》建立连接

发送数据包----------》》服务器响应请求

返回浏览器----------》》浏览器渲染程序页面

（1）DNS解析

在浏览器中输入一个URL地址，但URL中服务器地址是一个域名而不是一个指定的IP地址，路由器并不知道你想要查找的地址，那么DNS域名解析系统会将该域名解析成ip，而IP地址是唯一的，每一个IP地址对应网络上的一台计算机。

（2）建立网络连接，发送数据包

由于1的努力，已经能够根据ip和端口号与网络上对应的服务器建立连接，浏览器这边会向服务器发送一个数据包，里面包含了大量的信息，但这个数据包有一定的格式。就像我给你邮个快递，也得遵循邮递公司的一些规则吧！我得写上我的身份信息、寄的物品、标明邮递地址....道理是一样的，到了网络中这些规则就是“Http协议(网络协议)”。

HTTP是一个属于应用层的面向对象的协议，HTTP 协议一共有五大特点：1、支持客户/服务器模式（C/S模式）；2、简单快速；3、灵活；4、无连接；5、无状态。

（3）服务器响应请求，返回浏览器

服务器会分解你的数据包，例如你查找的是一个文档，那么服务器可能会返回一个doc文档或者zip压缩资源给你；如果你访问的是一个链接页面，那么服务器相应的返回一个包含HTML/CSS标记文档，这些请求和响应都有一个通用的写

法，这些规则也就是前面提到的"http协议"。

客户端向服务器请求资源时，除了告诉服务器要请求的资源，同时还会附带一些其他的信息，这部分信息放在"header"部分（服务器响应请求也一样！），主要有请求头(略)和响应头，这里以响应头部信息为例：

（4）浏览器渲染呈现

浏览器拿到响应的页面代码，将其解析呈现在用户面前，至于为什么会是看到的这个样子，有时又是另外的一些页面效果，这里就涉及到web标准了，也就是我们经常提到的w3c标准。根据资源的类型，在网页上呈现给用户，这个过程叫网页渲染。解析和呈现的过程主要由浏览器的渲染引擎实现，浏览器的渲染引擎质量就决定了浏览器的好坏（引擎这一块已经超出了我的理解范围了）。

但实际上输入URL到页面呈现这背后涉及的内容远远不止这些，例如后台web服务器、双向的网络数据传输、http缓存策略等

（5）**涉及协议：**

①应用层HTTP(www访问协议)，DNS（域名解析服务）

②传输层TCP（为HTTP提供可靠的数据传输），UDP（DNS使用UDP传输）

③网络层：IP（IP数据包传输和路由选择），ICMP（提供网络传输过程中的差错检测），ARP（将本机的默认网关IP地址映射成物理MAC地址）

（6）若有客户打不开网站，分析原因排错

OSI参考模型的基础知识：

1、OSI模型每一层都为上一层提供服务

2、网络出现故障从底层往高层一项项的逐步检查

①物理层，物理层故障：查看连接状态，查看发送和接收的数据包的具体情况（网线没有接上（断开）、网线的水晶头该重新置换，没有接触良好）

②数据链路层，MAC地址冲突、ADSL拨号上网欠费、网速没有办法协商一致、计算机连接到错误的VLAN

③网络层，配置错误IP地址，子网掩码/配置错误的网关，路由器没有配置，到达不了目标网络的路由器

④应用层，应用程序配置错误

10.http和https区别，https在请求是额外的过程，https是如何保证数据安全的

超文本传输协议HTTP被用于在WEB浏览器和网站服务器之间传递信息，HTTP协议以明文的方式发送内容，不提供任何方式的数据加密，如果攻击者截取了Web浏览器和网站服务器之间的传输报文，就可以直接读懂其中的意思，所以HTTP不适合传输一些敏感信息，比如银行卡号，密码等支付信息。为了解决HTTP的这一缺陷，需要使用另一种协议：安全套接字层超文本传输协议HTTPS，为了数据传输的安全性，HTTPS在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

（1）HTTP和HTTPS的基本概念

HTTP：互联网上应用最为广泛的一种网络协议，用于从WWW服务器传输超文本到本地浏览的传输协议，它可以是浏览器更加高效。使网络传输减少。

HTTPS：是以安全为目标的HTTP通道，简单的讲就是HTTP的安全版，即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL；其主要作用可以分为两种：一种是建立一个信息安全通道，来保证数据传输的安全性；另一种是确认网站的真实性。

（2）HTTP和HTTPS的区别

简单的说，HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http安全

详细的说分为四点：

①https协议需要到ca申请证书，一般免费证书比较少，因而需要一定费用

②http是超文本传输协议，信息是明文传输；https则是具有安全性的ssl加密传输协议

③http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443

④http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的进行加密传输、身份认证的网络传输协议，比http安全

（3）HTTPS的工作原理

①客户端发起HTTPS请求，就是用户在浏览器中输入一个https网址，然后连接到server443端口

②服务端的配置，采用HTTPS协议的服务器必须要有一套数字证书，可以自己制作，也可以向组织申请。这套证书其实驾驶一对公钥和私钥。如果对公钥和私钥不太理解，可以想象成一把钥匙和一个锁头，只是全世界只有你一个人有这把钥匙，你可以把锁头给别人，别人可以用这个锁把重要的东西锁起来，然后发给你，因为只有你一个人有这把钥匙，所以只有你才能看到被这把锁锁起来的东西。

③传送证书，这个证书就是公钥，只是包含了很多信息，如证书的颁发机构，过期时间等等

④客户端解析证书

这部分工作是有客户端的TLS来完成的，首先会验证公钥是否有效，比如颁发机构，过期时间等等，如果发现异常，则会弹出一个警告框，提示证书存在问题。如果证书没有问题，那么就生成一个随机值，然后用证书对该随机值进行加密，就好像上面说的，把随机值用锁头锁起来，这样除非有钥匙，不然看不到被锁住的内容。

⑤传送加密信息，这部分传送的是用证书加密后的随机值，目的就是让服务端得到这个随机值，以后客户端和服务端的通信就可以通过这个随机值来进行加密解密了。

⑥服务端解密信息，服务端用私钥解密后，得到了客户端传过来的随机值（私钥），然后将内容通过改值进行对称加密，所谓对称加密就是将信息和私钥通过某种算法混合在一起，这样除非知道私钥，不然无法获取内容，而正好客户端和服务端都知道这个私钥，所以只要加密算法够彪悍，私钥够复杂，数据就够安全

⑦传输加密后的信息，这部分信息是服务段用私钥加密后的信息，可以在客户端被还原。

⑧客户端解密信息，客户端用之前生成的私钥解密服务段传过来的信息，于是获取了解密后的内容，整个过程第三方即使监听到了数据，也束手无策。

11.IP地址子网划分

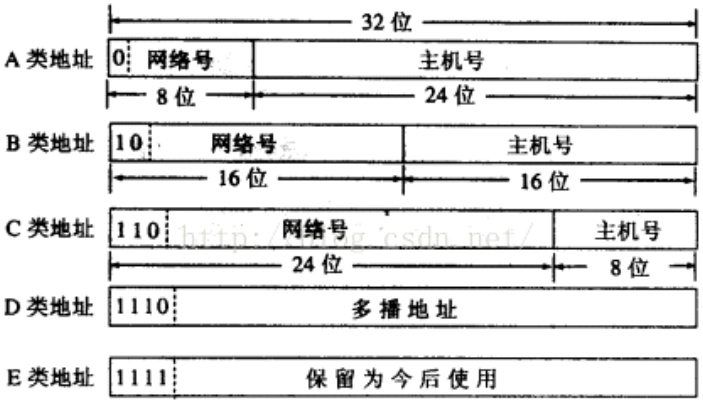


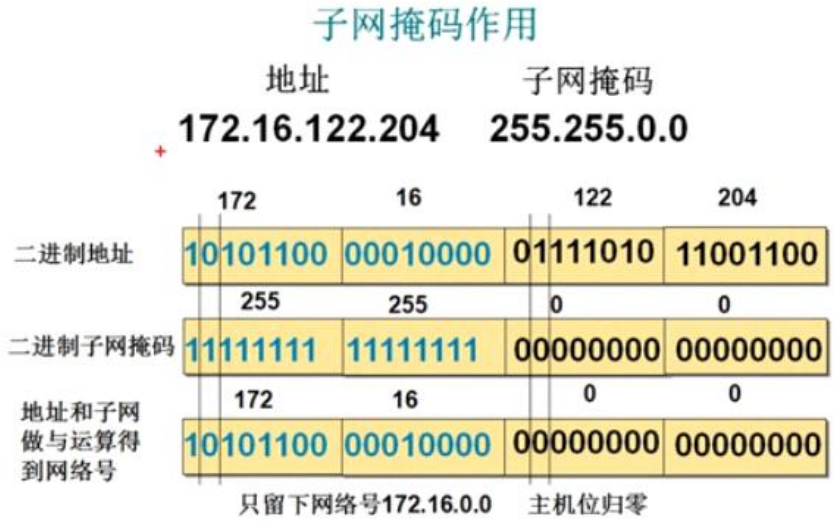
图 4-6　IP 地址中的网络号字段和主机号字段

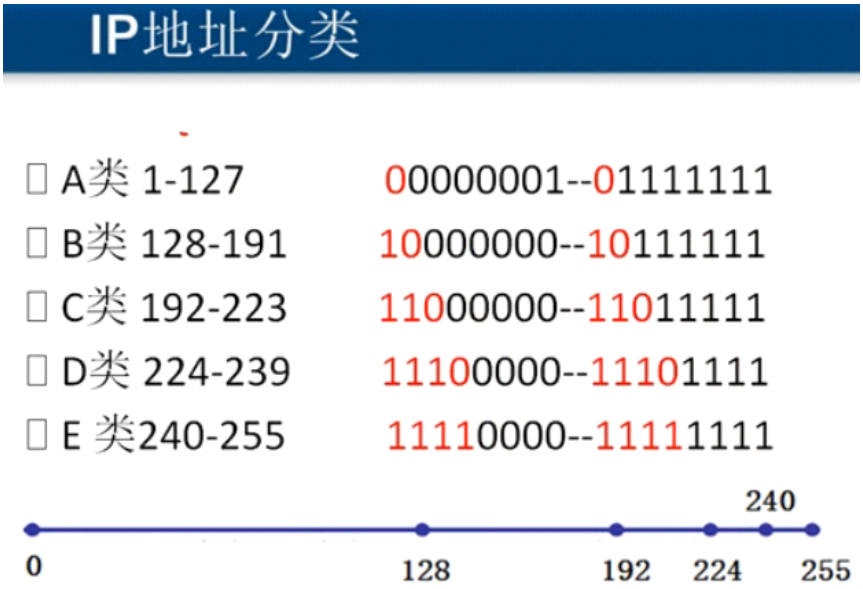
表 4-2　IP 地址的指派范围

网络类别	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中的最大主机数
A	126 (2^7-2)	1	126	16777214
B	16383 ($2^{14}-1$)	128.1	191.255	65534
C	2097151 ($2^{21}-1$)	192.0.1	223.255.255	254

表 4-3　一般不使用的特殊 IP 地址

网络号	主机号	源地址使用	目的地址使用	代表的意思
0	0	可以	不可	在本网络上的本主机（见 6.6 节 DHCP 协议）
0	host-id	可以	不可	在本网络上的某个主机 host-id
全 1	全 1	不可	可以	只在本网络上进行广播（各路由器均不转发）
net-id	全 1	不可	可以	对 net-id 上的所有主机进行广播
127	非全 0 或全 1 的任何数	可以	可以	用作本地软件环回测试之用





（一）IP地址会给Internet上每一个主机分配一个网络地址，由32位的标志符组成，将32位的IP地址分成若干固定的类，每一类地址都是由两个固定长度的字段组成，其中第一个字段是网络号，标志主机连接到的网络；第二个是主机号。一个IP地址在整个Internet上是唯一的。

（1）A类，B类，C类地址的网络号字段分别由1个字节、2个字节和3个字节长，在网络号字段最前面有1~3位是固定的，其数值分别是0，10,110。

（2）A类，B类，C类地址的主机号字段分别是由3个字节、2个字节和1个字节的长度组成的

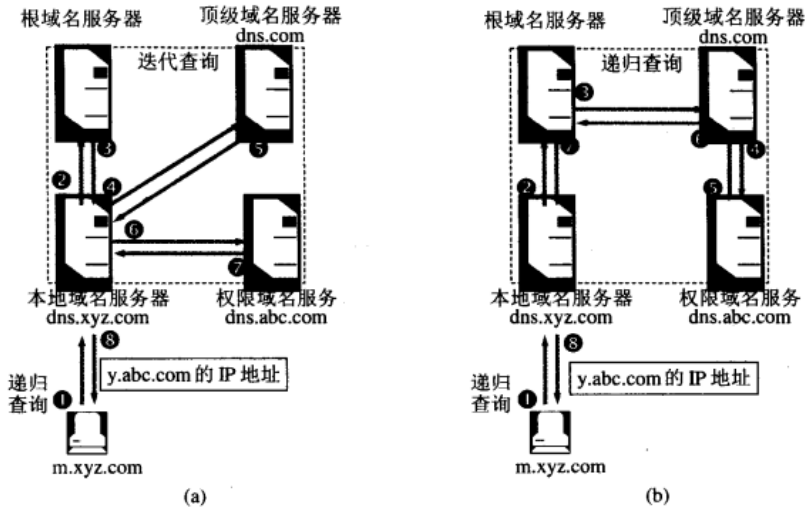
（3）D类地址的前4位是1110，用于多播（一对多通信）
（4）E类地址保留为以后使用
（二）保留的私有地址和特殊地址
私有地址是上面IP分类（ABC类）中取其中的一段
A：10.0.0.0
B：172.12.0.0----172.31.0.0（16个B类）
C：192.168.0.0----192.168.255.0（255个C类）
（三）一些特殊的IP地址
①主机为全为0：代表网络位，本网段
②主机为全为1：代表所有主机，（广播地址）
③169.254.0.0没有DHCP，未获得地址
（四）子网掩码
默认的子网掩码，不是所有的网络都需要子网
A类IP地址的默认子网掩码为255.0.0.0;
B类IP地址的为255.255.0.0；
C类的为255.255.255.0；

12.POST和GET区别

（1）get是从服务器上获取数据，post是向服务器传送数据。
（2）在客户端，Get方式在通过URL提交数据，数据在URL中可以看到；POST方式，数据放置在HTML HEADER内提交。
（3）对于get方式，服务器端用Request.QueryString获取变量的值，对于post方式，服务器端用Request.Form获取提交的数据。
（4）GET方式提交的数据最多只能有1024字节，而POST则没有此限制。
（5）安全性问题。正如在（1）中提到，使用 Get 的时候，参数会显示在地址栏上，而 Post 不会。所以，如果这些数据是中文数据而且是非敏感数据，那么使用 get；如果用户输入的数据不是中文字符而且包含敏感数据，那么还是使用 post为好。
注：所谓的安全意味着该操作用于获取信息而非修改信息。幂等的意味着对同一 URL 的多个请求应该返回同样的结果。完整的定义并不像看起来那样严格。换句话说，GET 请求一般不应产生副作用。从根本上讲，其目标是当用户打开一个链接时，她可以确信从自身的角度来看没有改变资源。比如，新闻站点的头版不断更新。虽然第二次请求会返回不同的一批新闻，该操作仍然被认为是安全的和幂等的，因为它总是返回当前的新闻。反之亦然。POST 请求就不那么轻松了。POST 表示可能改变服务器上的资源的请求。仍然以新闻站点为例，读者对文章的注解应该通过 POST 请求实现，因为在注解提交之后站点已经不同了（比方说文章下面出现一条注解）。

13.DNS解析过程

域名解析的过程，要注意以下两点：
（1）主机向本地域名服务器的查询一般都采用**递归查询**
（2）本地域名服务器向根域名服务器的查询通常采用**迭代查询**



DNS 查询举例：(a) 本地域名服务器采用迭代查询；(b) 本地域名服务器采用递归查询

假设域名为m.xyz.com的主机想知道另一个主机（域名为y.abc.com）的IP地址，例如m.xyz.com打算发邮件给主机y.abc.com，这时必须知道主机y.abc.com的IP地址，下面以下查询步骤：

（1）主机m.xyz.com先向本地域名服务器dns.xyz.com进行递归查询

（2）本地域名服务器采用迭代查询，先向一个根域名服务器查询

（3）根域名服务器告诉本地域名服务器，下一次应该查询的顶级域名服务器dns.com的IP地址

（4）本地域名服务器向顶级域名服务器dns.com进行查询。

（5）顶级域名服务器dns.com告诉本地域名服务器，下一次应查询的权限域名服务器dns.abc.com的IP地址

（6）本地域名服务器向权限域名服务器dns.abc.com进行查询

（7）权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的IP地址

（8）本地域名服务器最后把查询结果告诉m.xyz.com

14. TCP如何保证数据的可靠传输的（这个问题可以引申出很多子问题，拥塞控制慢开始、拥塞避免、快重传、滑动窗口协议、停止等待协议、超时重传机制，最好都能掌握）

TCP/IP协议族之运输层协议（UDP, TCP)

在某段时间内，若对网络中某一资源的需求超过了该资源所能提供的可用部分，网络的性能就要变坏，这种情况就叫做拥塞。

从大的方面来看，拥塞控制可分为**开环控制**和**闭环控制**两种方法。开环控制方法就是在设计网络时事先将有关发生拥塞的因素考虑周到，力求网络在工作时不产生拥塞。但一旦整个系统运行起来，就不再中途进行改正了。**闭环控制是基于反馈环路**的概念。属于闭环控制的有以下几种措施：

（1）监测网络系统以便检测到拥塞在何时、何处发生。

（2）把拥塞发生的信息发送到可采取行动的地方。

（3）调整网络系统的运行以解决出现的问题。

拥塞控制与流量控制

拥塞控制就是**防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。**拥塞控制所要做的都有一个前提，就是**网络能够承受现有的网络负荷。**拥塞控制是一个**全局性**的过程，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。

流量控制往往指点对点通信量的控制，是个**端到端**的问题（接收端控制发送端）。流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。

二者被弄混的原因是，因为某些拥塞控制算法是向发送端发送控制报文，并告诉发送端，网络已出现麻烦，必须放慢发

送速率。这点和流量控制相似。

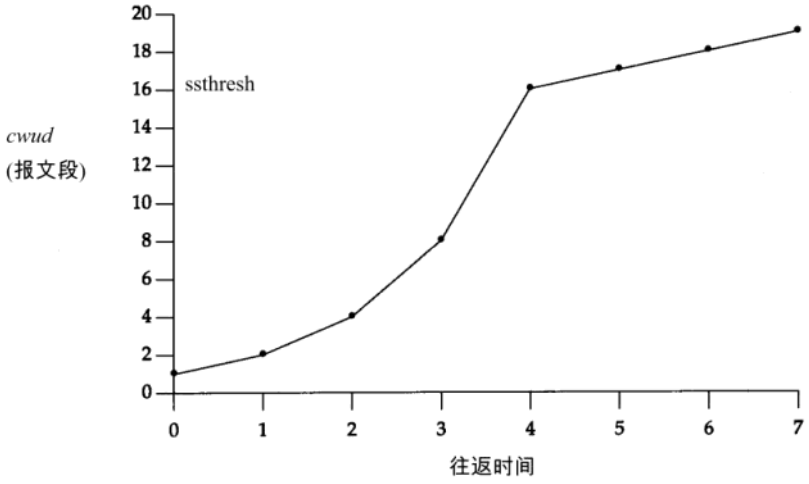
拥塞控制的方法

因特网建议标准RFC2581定义了进行拥塞控制的四种算法，即**慢开始**（Slow-start)，**拥塞避免**（Congestion Avoidance)，**快重传**（Fast Restrangsmit)和**快恢复**（Fast Recovery）。我们假定

1）数据是单方向传送，而另外一个方向只传送确认。

2）接收方总是有足够大的缓存空间，因为发送窗口的大小由网络的拥塞程度来决定。

下图是慢启动和拥塞避免的一个可视化描述。我们以段为单位来显示cwnd和ssthresh，但它们实际上都是以字节为单位进行维护的。



拥塞窗口概念：发送报文段速率的确定，既要根据接收端的接收能力，又要从全局考虑不要使网络发生拥塞，这由接收窗口和拥塞窗口两个状态量确定。接收端窗口（Reciver Window)又称通知窗口（Advertised Window),是接收端根据目前的接收缓存大小所许诺的最新窗口值，是来自接收端的流量控制。拥塞窗口cwnd（Congestion Window)是发送端根据自己估计的网络拥塞程度而设置的窗口值，是来自发送端的流量控制。

（1）**慢启动原理**

1）当主机开始发送数据时，如果立即将较大的发送窗口的全部数据字节都注入到网络中，那么由于不清楚网络的情况，有可能引起网络拥塞

2）比较好的方法是试探一下，即**从小到达逐渐增大发送端的拥塞控制窗口数值**

3）通常在刚刚开始发送报文段时可先将拥塞窗口cwnd(拥塞窗口)设置为一个最大报文段的MSS的数值。在每收到一个对新报文段确认后，将拥塞窗口增加至多一个MSS的数值，当rwind（接收窗口）足够大的时候，为了防止拥塞窗口cwind的增长引起网络拥塞，还需要另外一个变量---慢开始门限ssthresh

（2）**拥塞控制**

具体过程为：

1）TCP连接初始化，将拥塞窗口设置为1

2）执行 慢开始算法：cwind按指数规律增长，直到cwind == ssthress开始执行**拥塞避免算法：cwnd按线性规律增长**

3）当网络发生拥塞，把ssthresh值更新为拥塞前ssthresh值的一半，cwnd重新设置为1，按照步骤（2）执行。

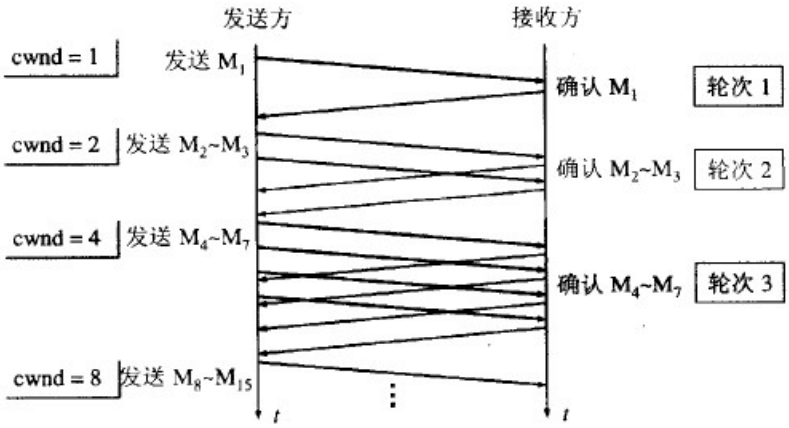


图 5-24　发送方每收到一个确认就把窗口 cwnd 加 1

（3）**快重传和快恢复**

一条TCP连接有时会因等待重传计时器的超时而空闲较长的时间，慢开始和拥塞避免无法很好的解决这类问题，因此提出了快重传和快恢复的拥塞控制方法。

快重传算法并非取消了重传机制，它要求接收方每收到一个失序的报文段后就立即发出重复确认，如果当发送端接收到三个重复的确认ACK时，则断定分组丢失，立即重传丢失的报文段，而不必等待重传计时器超时。

例如：M1，M2，M3 -----> M1,M3,缺失M2，则接收方向发送方持续发送M2重复确认，当发送方收到M2的三次重复确认，则认为M2报文丢失，启动快重传机制，重传数据，其他数据发送数据放入队列，待快重传结束后再正常传输。

快恢复算法有以下两个要点：

1）当发送方连续收到接收方发来的三个重复确认时，就执行“乘法减小”算法，把慢开始门限减半(ssthresh = ssthresh/2)，这是为了预防网络发生拥塞。

2）由于发送方现在认为网络很可能没有发生拥塞，因此现在不执行慢开始算法，而是把cwnd(拥塞窗口)值设置为慢开始门限减半后的值（cwnd=ssthresh/2），然后开始执行拥塞避免算法，使拥塞窗口缓慢地线性增大。

15.地址解析协议

地址解析协议（ARP）作用是已知一个机器（主机或路由器）的IP地址。需要找出其对应的硬件地址，即为了解决网络层使用的IP地址解析出在数据链路层使用的硬件地址。但是解决这个问题的难点在于，第一,IP地址有32位，而硬件地址有48位，两者之间不是简单地一对一映射关系；第二，在网络上，可能经常有新的主机要加进来，或撤走一些主机。ARP解决这些问题的方法是在主机ARP高速缓存中存放一个从IP地址到硬件地址的映射表，并且这个映射表还经常动态更新（新增或超时删除）。

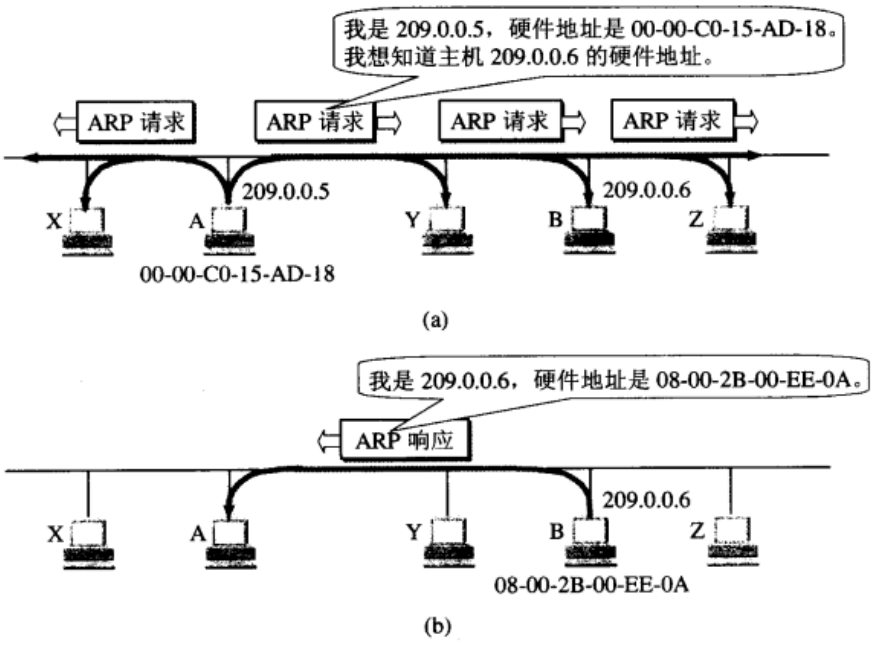


图 4-12　地址解析协议 ARP 的工作原理

(a) 主机 A 广播发送 ARP 请求分组；(b) 主机 B 向 A 发送 ARP 响应分组

当主机A要向本局域网上的某个主机B发送数据报时，就先在其ARP高速缓存中查看有无主机B的IP地址。如果有，就在ARP高速缓存中查出对应的硬件地址，再把这个硬件地址写入MAC帧，然后通过局域网把该MAC帧发往此硬件地址。也有可能查不到主机B的IP地址项目，原因可能是主机B才入网或者主机A刚刚加电，高速缓存还是空的。在这种情况下，主机A就自行运行ARP，按照以下步骤找出主机B的硬件地址

（1）ARP进程在本局域网上广播发送一个ARP请求分组，主要内容表明“我的IP地址是209.0.0.5，硬件地址是00-00-C0-15-AD-18,我想知道IP地址为209.0.0.6的主机的硬件地址”

（2）在本局域网上的所有主机运行的ARP进程都收到此ARP请求分组

（3）主机B在ARP请求分组中见到自己的IP地址，就向主机A发送ARP响应分组，并写入自己的硬件地址，其余主机都不理睬这个ARP请求分组。ARP响应分组的主要内容是“我的IP地址是209.0.0.6，我的硬件地址是08-00-2B-00-EE-0A“。注意：虽然ARP请求分组是广播发送的，但是ARP响应分组是普通的单播，即从一个源地址发送到一个目的地址

（4）主机A收到主机B的ARP响应分组后，就在其APR高速缓存中写入主机B的IP硬件地址到硬件地址的映射。

16.交换机和路由器的区别

17.TCP是如何实现可靠传输的

1、确认和重传：接收方收到报文就会确认，发送方发送一段时间后没有收到确认就重传。

2、数据校验

3、数据合理分片和排序：

UDP：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.这样就会多做许多事情,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.

tcp会按MTU合理分片，接收方会缓存未按序到达的数据，重新排序后再交给应用层。

4、流量控制：当接收方来不及处理发送方的数据，能提示发送方降低发送的速率，防止包丢失。

5、拥塞控制：当网络拥塞时，减少数据的发送。

1.使用网桥的好处：过滤通信量，增大吞吐量；扩大物理范围；提高可靠性。

2.适合交互式通信的交换技术：分组；电路；虚电路分组。报文不适合。

3.透明网桥转发表的建立是基于：所转发的帧的源MAC地址。

4.TCP/IP参考模型中的主机-网络层对应于OSIRM中的：物理层与数据链路层

5.关于ADSL(非对称数字用户线路)技术描述：上行和下行的传输速率可以不同；数据传输可利用现有电话线；适用于家庭用户使用

6.在OSI模型（目前被TCP/IP协议淘汰的一个协议）中，第N层和其上的第N+1层的关系是：第N层为第N+1层提供服务。处理路径选择的是网络层；

7.IP报文的分片发生在路由器上，分组发生在主机上。

8.Top Level Domain 顶级域名 它是一个因特网域名的最后部分，也就是任何域名的最后一个点后面的字母组成的部分。最早的顶级域名。com（公司和企业）;.net（网络服务机构）;.org（非赢利性组织）;.edu（教育机构）;.gov（美国专用的政府部门）;.int（国际组织）；等等。TLD 由因特网号码分配机构（IANA）分配。现今分为三种类型：通用顶级域名（也叫一般顶级域名）：（gTLD）；国家顶级域名：（nTLD）；国际顶级域名：（iTLD）。

Top Level Domain 顶级域名它是一个因特网域名的最后部分，也就是任何域名中，名字后面的字母组成的部分。最早的顶级域名.com（公司和企业）;.net（网络服务机构）;.org（非赢利性组织）;.edu（教育机构）;.gov（美国专用的政府部门）;.int（国际组织）；等等。

TLD 由因特网号码分配机构（IANA）分配。现今分为三种类型：通用顶级域名（也叫一般顶级域名）：（gTLD）；国家顶级域名：（nTLD）；国际顶级域名：（iTLD）。

按照机构区分的域名原来有 7个 ：com（商业机构）、net（网络服务机构）、gov（政府机构）、mil（ 军事 机构）、org（非盈利性组织）、edu（教育部门）、int（国际机构）。

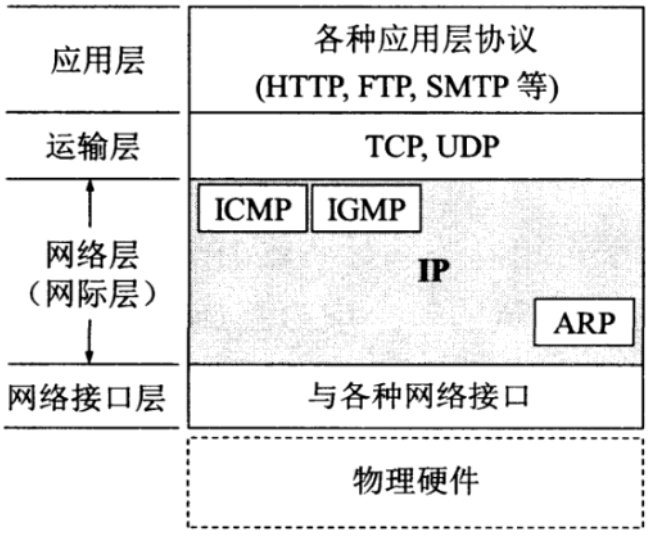
1997年又新增7个最高级标准域名：firm（企业和公司）、store（商业企业）、web（从事与WEB相关业务的实体）、arts（从事文化娱乐的实体）、REC（从事休闲娱乐业的实体）、info（从事信息服务业的实体）、nom（从事个人活动的个体、发布个人信息）。

9.理想低通信道的最高码元传输速率是2WBaud。

10.每个IP地址都可以有一个主机名，通过主机名得到该主机对应的IP地址的过程叫做**域名解析。**

11.ATM信元由53个字节组成，信头包含5个字节。

12.



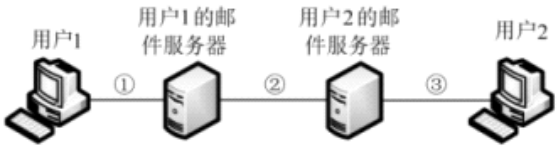
13.适用于小城市的本地网组织：端局分区

适用于中等城市的本地网组织：汇接局全覆盖

适用于大城市的本地网组织：汇接局分区

14.（POP3和SMTP的区别）

28 若用户 1 与用户 2 之间发送和接收电子邮件的过程如下图所示，则图中①、②、③阶段分别使用的应用层协议可以是（ ）。



SMTP:简单邮件传输协议，用来发送或者中转邮件。POP3是邮局协议的第3个版本，规定怎样将个人计算机连接带Intenet的邮件服务器和下载电子邮件的协议，是从服务器下载到本地的。

15.RS-485最少有2根数据信息号。

16.TCP使用多种机制来保证可靠传输，包括滑动串口、确认、序列号。

17.集线器和交换机的区别

集线器不管端口是否接入网线都一视同仁的给每个端口分配固定带宽，理论值为5Mbit/s。交换机只在有数据转发时才分配带宽给指定端口，理论值为100Mbit/s。

18.数据链路层的三个基本问题是封装成帧、透明传输和差错检测

19.与IP协议配套使用的有ICMP协议、ICGP协议，ARP协议，ICMP报文作为数据段封装在IP分组中，因此IP协议直接为ICMP服务

20.总线拓扑结构采用一个信道作为传输媒体,所有站点都通过相应的硬件接口直接连到这一公共传输媒体上,该公共传输媒体即称为总线。任何一个站发送的信号都沿着传输媒体传播,而且能被所有其它站所接收。

21.Internet是将无数局域网连接起来组成的网络。

22.RIP是基于距离向量的路由选择协议，RIP选择一个到目的网络具有最少路由器的路由（最短路由）；

OSPF最主要特征是使用分布式链路状态协议，所有的路由器最终都能建立一个链路状态数据库（全网的拓扑结构图）。

BGP-4采用路径向量路由选择协议。BGP所交换的网络可达性信息是要到达某个网络所要经过的自治系统序列。

因特网采用动态路由协议。

23.通信系统必须具备的三个基本要素：信源、通信媒体、信宿。

24.帧中继网是一种广域网。

25.攻击者使用无效IP地址，利用TCP连接的三次握手过程，连续发送会话请求，使受害主机处于开放会话的请求之中，直至连接超时，最终因耗尽资源而停止响应。这种攻击被称为**SYN Flooding攻击。**

26.HTTP 1.0,各种状态码的表示含义

302表示文件被转移

404 未找到，服务器找不到所请求的网页。

302 临时移动，服务器从不同位置的网页响应请求，请求者应继续使用原有位置进行以后的请求。

500 （服务器内部错误），服务器遇到错误，无法完成请求。

403 （禁止）服务器拒绝请求

IP address rejected为403.6

1xx（临时响应）

表示临时响应并需要请求者继续执行操作的状态代码。

2xx （成功）

表示成功处理了请求的状态代码。

3xx （重定向）

表示要完成请求，需要进一步操作。 通常，这些状态代码用来重定向。

4xx（请求错误）

这些状态代码表示请求可能出错，妨碍了服务器的处理。

5xx（服务器错误）

这些状态代码表示服务器在尝试处理请求时发生内部错误。 这些错误可能是服务器本身的错误，而不是请求出错。

27.

> 假设信道长度为1200km，其往返时间为20ms，分组长度为1200bit，发送速率为1Mb/s。若忽略处理时间和发送确认分组时间，则该信道的利用率为( )

1200bit的长度，发送速度为1mb/s，则需要1.2ms

往返时间20ms，则发送一组共需要(20+1.2)ms

利用率=1.2/21.2=0.0566

编辑于 2016-06-13 13:02:03

28.国标规定接入网的维护管理接口应该符合Q3接口

29.IP地址的编码分为网络号和主机号两部分

IP分网络号和主计划

A类IP第一字节是网络号，后三字节是主机号

B类IP前两字节是网络号，后两字节是主机号

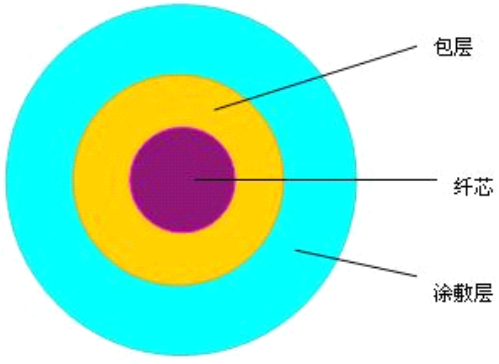
C类IP前三字节是网络号，后一字节是主机号

29.虚电路交换分为3各阶段

虚电路表示这只是一条 **逻辑上的连接** ，分组都沿着这条逻辑连接按照存储转发方式传送，而 **并不是真正建立了一条物理连接** 。包括建立连接，传输数据，拆除连接三个阶段。建立连接之后就类似于专线，所以不存在路由选择

30.在Internet域名体系中，域的下面可以划分子域，各级域名用圆点分开，按照从右到左越来越小的方式分多层排列

31.



光纤裸纤一般分为三层：

中心高折射率玻璃芯（芯径一般为50或62.5μm），

中间为低折射率硅玻璃包层（直径一般为125μm），折射率差可以保证光主要限制在纤芯里进行传输。

最外是加强用的树脂涂层，涂料的作用是保护光纤不受外来的损害，增加光纤的机械强度。。

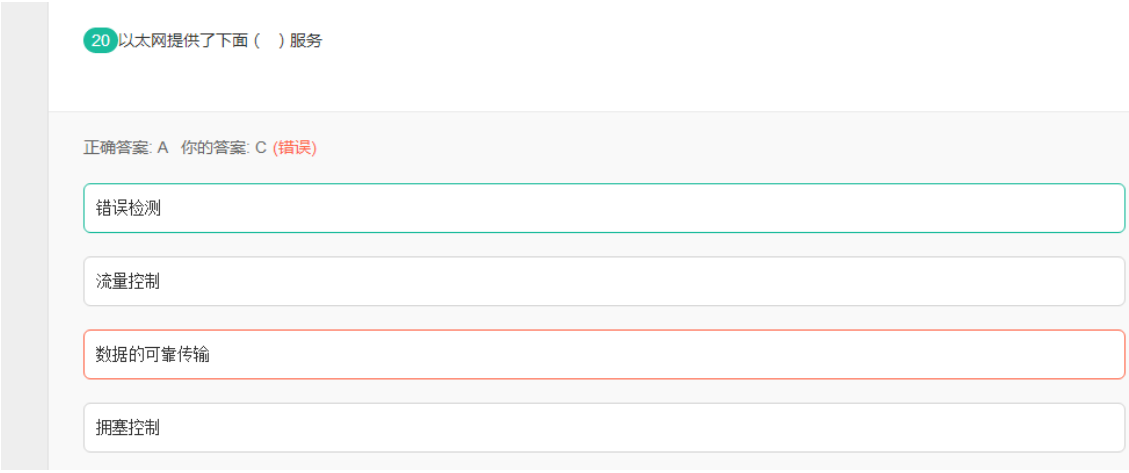
32.路由器工作于网络层，用于连接多个逻辑上分开的网络。

33.采用海明码纠正一位差错，若信息位为 4 位，则冗余位至少应为（ ）

对于纠正一位差错的海明码,必须满足如下条件：记冗余位长度为r,那么总的码长为:2^r-1,信息位长度为：2^r-r-1.所以依题设 2^r-r-1=4,r=3,即冗余位至少应为3位

34.

35.



以太网提供的服务是不可靠的交付，即尽最大努力的交付，当目的站收到有差错的数据帧时就丢弃此帧，其他什么都不做。差错的纠正右高层来决定。如果高层发现丢失了一些数据而进行重传，以太网并不知道这是一个重传的帧。

36.Ping是windows下的一个命令，在Unix和Linux下也有这个命令。ping也属于一个通信协议，是TCP/IP协议的一部分。利用ping命令可以检查网络是否联通，可以很好地帮助我们分析和判断网络故障。应用格式是Ping空格IP地址。该命令还可以加许多参数使用，具体是键入Ping按回车即可看到详细说明。Ping实际上利用的是ICMP ECHO和ICMP ECHO REPLY包来探测主机是否存在，所以Ping程序的流程十分简单：发送ICMP ECHO包---------接收ICMP ECHO REPLY包。发送ICMP ECHO包时填充Identifier为进程ID,Sequence Number为从0递增计数，data填充为发送时间。接收ICMP ECHO REPLY包时检查Identifier，Sequence Number是否正确，通过IP报头的源地址字段获得回送的主机地址是否正确。Ping使用了ICMP回送请求与回送回答报文。Ping是应用层直接使用网络层的一个例子，它没有通过传输层的TCP和UDP

37.通过计算机网络给B发送消息，说其同意签订合同，随后A反悔，不承认发送过该消息。为防止这种情况发生，在计算机网络中应采用（**数字签名**）技术。

38.SNMP 使用 udp 161 和 162 端口，则该协议属于 TCP/IP 模型中的**应用层**

39.TCP/IP是一组支持异种计算机网路互联的通信协议

40.集线器（HUB）：是局域网LAN中的重要的部件之一，它是网络连线的连接点。集线器有多个户端口，连接计算器和服务器之类的外围设备。**集线器会增大冲突域**

41.UDP首部有8个字节，TCP首部有20个字节

42.在HDLC协议中，每次发送方要发送的信息中含有5个以上连续的1时，他总要在第五个1后面插入一个冗余的0，不管第六位是0还是1，这个额外的零都要插入。例:在HDLC中，数据比特串0111101111110装帧发送出去的串为**01111011111010**

43.网卡是工作在链路层的网络组件，是局域网中连接计算机和传输介质的接口。若要将计算机与局域网连接，至少需要具有的硬件是网卡

44.

以http://mail.163.com/index.html为例进行说明：

1)http://:这个是协议，也就是HTTP超文本传输协议，也就是网页在网上传输的协议。

2)mail：这个是**服务器名(主机名)**，代表着是一个邮箱服务器，所以是mail. 【www代表一个Web（万维网）服务器】

3)163.com:这个是**域名**，是用来定位网站的独一无二的名字。

4)mail.163.com：这个是**网站名**，由服务器名+域名组成。

5)/：这个是根目录，也就是说，通过网站名找到服务器，然后在服务器存放网页的根目录

6)index.html：这个是根目录下的默认网页（当然，163的默认网页是不是这个我不知道，只是大部分的默认网页，都是index.html）

7)http://mail.163.com/index.html:这个叫做**URL**，统一资源定位符，全球性地址，用于定位网上的资源。

45.高等研究计划署网路（Advanced Research Projects Agency Neywork简称ARPnet）,是美国国防研究计划署开发的世界上第一个运营的封包交换网络，它是全球互联网的始祖。

46.

21 网络地址172.16.22.38/28 请写出此地址的子网ID以及广播地址，此地址所处子网可用主机数

正确答案: D 你的答案: 空 (错误)

172.16.22.32 172.16.22.255 12

172.16.22.32 172.16.22.47 16

172.16.22.32 172.16.22.255 15

172.16.22.32 172.16.22.47 14

32

172.16.22.38/28

此IP地址 28 表示 子网掩码的前28位作为网络号，是1， 即 1111 1111.1111 1111. 1111 1111. 1111 0000

所以可以计算该IP的网络号为:

38---> 0010 0110

& 1111 0000

32--> 0010 0000

所以可得到子网ID是 172.16.22.32

32 - 28 = 4 ,由此可计算该子网最多有 2^4 = 16 台主机，去掉网络号和广播地址是16 - 2 = 14

主机号全部为0 的主机作为网络号， 主机号全部为1的作为广播地址，

所以，可得该IP的广播地址是: 0010 1111-->47

所以广播地址是 172.16.22.47

47.

22 1 | 在如下网络拓扑结构中，具有一定集中控制功能的网络是（ ）

正确答案: B 你的答案: A (错误)

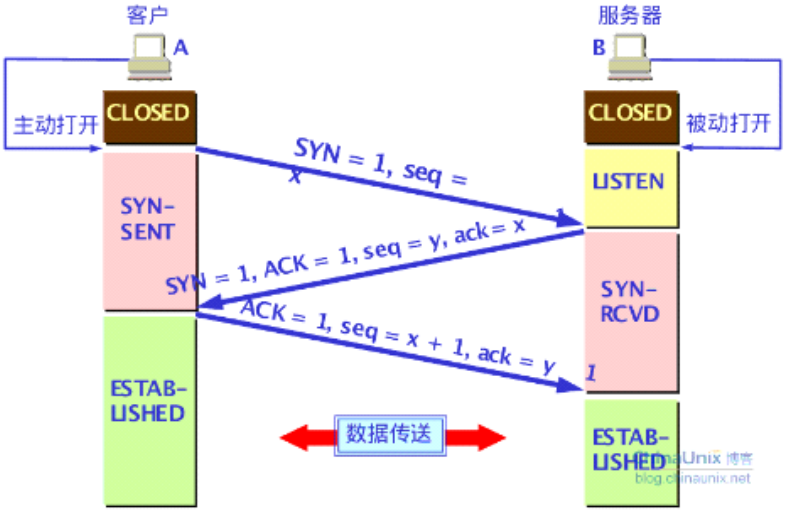
总线型网络

星型网络

环形网络

Full-mesh

48.



（此图第三次握手的ack应该等于y+1，而不是y，上面看不太清楚，但不影响解这题）

49.信元交换又叫异步传输模式，信元交换技术是一种快速分组交换技术，它结合了电路交换技术延迟小和分组交换技术灵活的优点，信元是固定长度的分组，ATM采用信元交换技术，其信元长度是53个字节，信元头是5个字节，数据是48字节。交换技术方面，经历了：电路交换-------报文交换-----分组交换------信元交换的过程

50

表示层的作用：对数据进行翻译、加密和压缩（表示协议数据单元PPDU）；

网络层的作用：负责数据包从源到宿的传递和网际互联（包）；

传输层的作用：提供端到端的可靠报文传递和错误恢复（段）；

会话层的作用：建立、管理和终止会话（会话协议数据单元）；

所以由上的各层作用就可以得道答案是表示层；

数据链路层，帧

网络层，数据报

运输层，报文段

应用层，报文

数据报diagram

在TCP/IP参考模型中，与OSI参考模型的网络层对应的是互联网络层。

MAC地址通常存储在计算机的网卡ROM中