网络路由传输数据报文:（数据传输时间远大于连接建立时间）
1.电路交换：从起点终端、中间路由节点、目标终端，始终占用连接带宽
2.报文交换：相邻节点完成传输即断开连接，继续进行下一个节点的传输
3.分组交换：将报文分组进行传输，相邻节点每次传输一个组

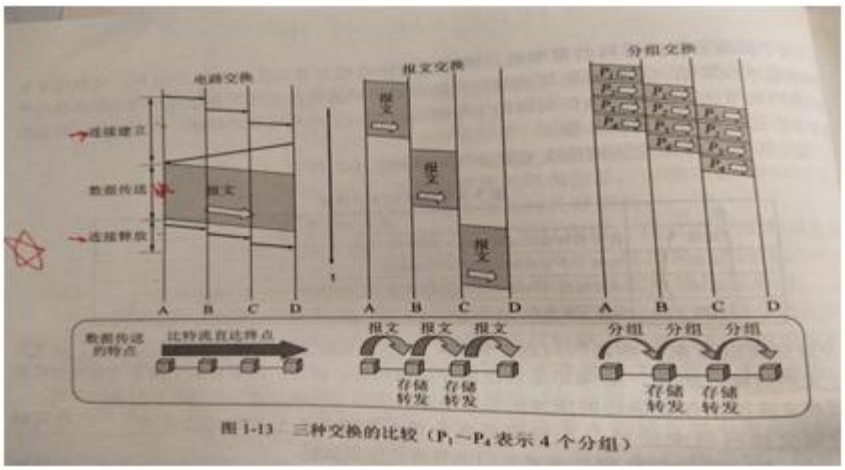


图 1-13 三种交换的比较（P_1—P_4 表示 4 个分组）

物理层：调制信号（波形）
调制解调器
信道复用

数据链路层：封装成帧，透明传输，差错检测（帧的传输）
1.点对点信道：一对一，常用于广域网，使用 PPP 协议
2.广播信道：一对多，常用于局域网，使用 CSMA/CD 协议
MAC 地址
适配器、转发器、集线器、网桥、以太网交换机

封装成帧：
帧的数据部分（IP 数据报，分组）、帧首部、帧尾部（用来验证是否为一个完整的帧）。
透明传输：
处理数据部分，使其中不会出现控制字符（帧首部和帧尾部）。

在数据部分出现控制字符时，使用字节（符）填充来解决，即在对应字符前面插入转义字符“ESC”（16 进制：1B，二进制：00011011），接收端接收后将“ESC”删除后再送往网络层。
差错检测：
比特差错：指比特在传输过程中可能会产生的差错，如 0 变成 1。

为了处理比特差错，广泛的使用了循环冗余检验 CRC 的检错技术，即在发送端计算出冗余码（称为帧检验序列 FCS）添加在数据后，接收端接受到数据后进行 CRC 检验。
FCS 的生成及 CRC 检验都是由硬件完成，速度快，不会延误数据的传输。

CRC 检错仅能做到对帧的无差错接受，无法处理帧丢失、帧重复、帧失序等情况。

对于通信线路质量较差的链路（无线传输），数据链路层增加了帧编号、确认和重传机制（收到正确的帧后向发送端发送确认，发送端在一定时间未收到确认消息，则重新发送），以数据链路层来向上提供可靠传输的服务；对于通信线路质量良好的链路，改正错误的任务就由上层协议（如 TCP 协议）完成。

PPP 协议：

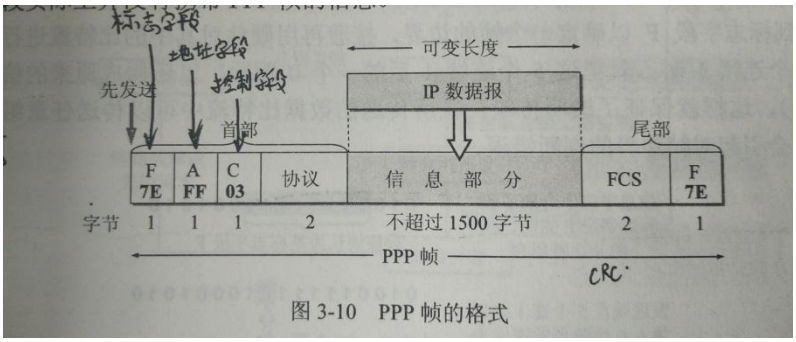


图 3-10 PPP 帧的格式

CSMA/CD 协议（以太网协议）：

广泛应用于总线网（另外有星形网、环形网两种）拓扑结构的局域网。

不可靠交付。

多点接入：多台计算机连接在一根主线；载波监听：发送前&发送中必须时刻检测信道，信道空闲时才可发送；碰撞检测：因为传播速率的因素，可能出现两个站同时在发送数据，若检测到此情况（通过总线的电压变化幅度）则需要等待随机事件后再次发送。

以太网在传输数据时以帧为单位，并且在传输时各帧之间必须有一定间隙，检测到总线上没有电压变化时就知道帧的传输已经结束,所以以太网只需要帧开始界定符，而不需要帧结束界定符，也不需要字节插入来保证透明传输。

以太网的扩展：

在物理层扩展：使用光纤连接两个以太网。由于电信号的衰减，以太网的主机之间的距离不能太远。

但是主机多了以后，碰撞域扩大了，即在任一时刻，碰撞域中只能有一个站点在发送数据。

在数据链路层扩展：使用网桥连接以太网。网桥中会缓存 MAC 地址对应的网段（以太网），网桥在收到帧时，先检查其目的 MAC 地址来确定将帧转发到哪个网段，或丢弃。

多接口的网桥-->交换机

网络层：

网际控制报文协议 ICMP、网际组管理协议 IGMP，向运输层服务。

地址解析协议 ARP，向数据链路层服务。

ARP 协议：

通过 IP 地址获取目标终端 MAC 地址（适配器/网卡的唯一标识）。

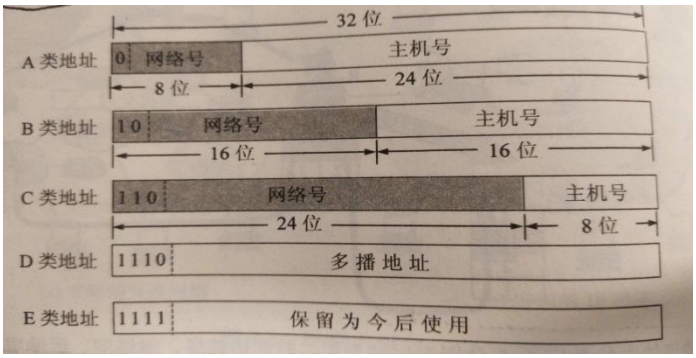
适配器收到的帧分为：1.单播帧（一对一），收到帧的 MAC 地址与自身相同；2.广播帧（一对全体），发送给本局域网所有站点的帧（全 1 地址）；3.多播帧（一对多），给本局域网上一部分站点的帧。

所有适配器至少能识别单播帧及广播帧。

ARP 协议使用广播帧将目标 ip 地址发送到本局域网下所有站点，站点对比接收到的 ip 地址和本机 ip 地址，若相同则将本机 MAC 地址返回。

通过 ip 地址及其掩码判断，当目标终端处于同一局域网时，通过 ARP 协议获取目标适配器 MAC 地址，然后广播帧，该局域网下的所有终端（其适配器）收到帧后对比 MAC 地址，若相同则收下，否则丢弃（这样不会浪费主机的处理机及内存资源）。

IP 地址：网络号+主机号



有的网络上主机很多，有的网络上主机少，所以对 IP 地址进行分类。
A 类地址：可指派的网络号 2^7-2 个，每个网络中的最大主机个数 2^24-2 个；
B 类地址：可指派的网络号 2^14-1 个，每个网络中的最大主机个数 2^16-2 个；
C 类地址：可指派的网络号 2^21-2 个，每个网络中的最大主机个数 2^8-2 个；

1.IP 管理机构在分配 IP 地址时，只需分配网络号，主机号由得到网络号的单位自行分配。
2.路由器仅根据网络号来转发分组，减少了路由表所占的存储空间及查找路由表的时间。
3.拥有不同网络号的局域网必须使用路由器连接。所以路由器至少连接到两个网络，所以路由器至少拥有两个不同的 IP 地址。

IP 数据报的发送：（分组转发算法）

1.主机 A 将 IP 数据报发送到该网络的路由器，路由器从数据报的首部获取到目的主机的 IP 地址 D 和其网络地址 N。
2.若 N 就是与此路由器直接相连的某个网络地址，则直接进行交付（从 ARP 高速缓存中获取目的主机的 MAC 地址，将数据报封装成 MAC 帧进行发送）。否则执行 3。
3.若路由表中有目的地址为 D 的特定主机路由，则把数据报传给该路由器。否则执行 4。
4.若路由表中有到达 N 的路由，则把数据报传送给该路由器。否则执行 5。
5.若路由表中有默认路由，则把数据报传送给该默认路由器。否则执行 6。
6.报告转发分组出错。

划分子网：

IP 地址 = 网络号 + 子网号 + 主机号

对于拥有主机个数很多的网络（如 A 类 B 类 IP 地址）来说，可以从主机号中“借用”若干位作为子网号。这样，对内来说已经将本网络划分为了若干个网络，但对外来说仍然表现为一个网络。

划分子网降低了路由器的负担（减少了路由表的项目数），增强了网络性能。

子网掩码：通过子网掩码来获取网络号（如 C 类地址的默认子网掩码为 255.255.255.0）。

无分类编址 CIDR（构成超网）：

由于 ipv4 地址的地址空间有限，引出了 CIDR，消除了传统 A/B/C 类地址及划分子网的概念。

IP 地址 = 网络前缀 + 主机号

网络前缀通过地址掩码（也可称作子网掩码）来获取。

最长匹配前缀：路由器在匹配 ip 地址时，可能匹配到不止一个结果（如：206.0.71.130 可以匹配到 206.0.68.0/22 和 206.0.71.128/25），此时，应选择匹配的地址中更具体的一个，即网络前缀更长的地址。

网际控制报文协议 ICMP：

允许主机或路由器报告差错情况和提供有关异常情况的报告。

重要应用之一：ping 命令，用来测试两个主机之间的连通性。应用层直接使用网络层 ICMP，而没有通过运输层的 TCP 或 UDP。

二：traceroute（windows 为 tracert）命令。用来跟踪一个分组从源点到终点路径，即经过的主机。

路由选择协议：得到路由表中的数据

因特网将整个互联网划分为许多较小的自治系统，在自治系统内部使用内部网关协议 IGP（如 RIP 和 OSPF），在自治系统之间使用使用外部网关协议 EGP（如 BGP）。

……

IP 多播：

与单播相比，在一对多通信中（如直播、消息推送等），多播可以大大节约网络资源。

能够运行多播协议的路由器称为多播路由器（普通单播 IP 数据报也可转发），服务器将数据分组当做多播数据报来发送，多播路由器在转发时会先将分组复制，然后转发到所有目标地址。当分组到达目的局域网时，由于局域网具有硬件多播功能，因此不需要复制分组。

IP 多播传送分组需要使用 IP 多播地址，即 D 类地址，使用网际组管理协议 IGMP。

多播地址只能用于目的地址，而不能用于源地址。

对多播数据报不产生 ICMP 差错报文，所以 PING 多播地址将收不到响应。

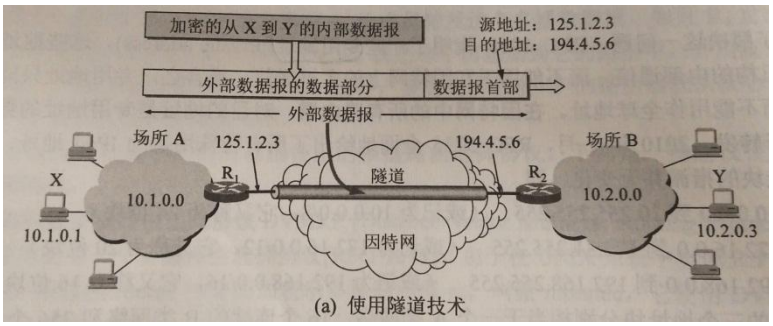
网际组管理协议 IGMP 和多播路由选择协议：

IGMP 协议是让连接在本地局域网上的多播路由器知道本局域网上是否有主机（主机上的某个进程）参加或者退出了某个多播组。
多播路由选择协议用于，连接在局域网上的多播路由器和连接在因特网上的其它多播路由器协同工作，以便付出最小的代价将多播数据报传输给所有的多播组成员。

虚拟专用网 VPN：

可重用 IP 地址，也叫作专用 IP 地址，这些地址仅作为机构内部使用的本地地址。
包括：10.0.0.0—10.255.255.255（10.0.0.0/8），172.16.0.0—172.31.255.255（172.16.0.0/12），192.168.0.0—192.168.255.255（192.168.0.0/16）。

专用网 A 和专用网 B 属于同一个机构，但不在同一个局域网下，此时可以利用因特网作为通信载体来进行通信。这样的专用网叫做虚拟专用网。
内部数据报在因特网传输前会进行加密，并作为外部数据报的数据部分再进行一次封装。



(a) 使用隧道技术

网络地址转换 NAT：

若专用网需要连接到因特网，则需要使用网络地址转换 NAT 方法。
使用 NAT 需要在专用网连接到因特网的路由器上安装 NAT 软件，路由器至少有一个有效的外部全球 IP 地址。这样，该专用网的所有主机在与因特网通信时，都要在 NAT 路由器上将其本地地址转换为全球 IP 地址。

NAT 路由器拥有 n 个全球 IP 地址时，专用网内最多可以同时有 n 个主机接入到因特网。
服务器并不知道专用网内主机的 IP 地址，需要由 NAT 路由器进行转换，所以一个主机在完成一次请求后才会“释放”对应全球 IP 地址。

现在常用的 NAT 转换表会将运输层的端口号也利用上，这种方式称为网络地址与端口号转换 NAPT。端口号的加入可以使专用网内的多个主机同时访问因特网。

运输层：

运输层提供的是主机的应用进程间的逻辑通信。两个主要协议：用户数据报协议 UDP，传输控制协议 TCP。

UDP：

UDP 是无连接的，即发送数据之前不需要建立连接，减少了开销和发送数据之前的时延。
UDP 不保证可靠交付。
UDP 是面向报文的，对于应用层交付的报文，加上 UDP 首部就往网络层发送，对于网络层交付的报文，去掉 UDP 首部就往应用层发送，不对报文做任何处理。

UDP 没有拥塞控制，在网络出现拥塞时不会使源主机的发送速率降低，这对某些实时应用是很重要的。
UDP 支持一对一、一对多、多对一、多对多的交互通信。
UDP 的首部开销小，只有 8 个字节，比 TCP20 字节的首部要短。

若接收方 UDP 发现收到的报文中的目的端口号不正确（不存在对应于该端口号的应用进程），就丢弃该报文，并由网际控制报文协议 ICMP 发送“端口不可达”差错报文给发送方。

TCP：可靠传输的原理及实现、流量控制、拥塞控制、运输连接管理

TCP 是面向连接的服务，提供可靠的运输服务，因此增加了许多开销（确认、流量控制、计时器、连接管理等），使协议数据单元的首部增大很多，还要占用许多的处理机资源。此外 TCP 不提供广播或多播服务。

可靠传输：

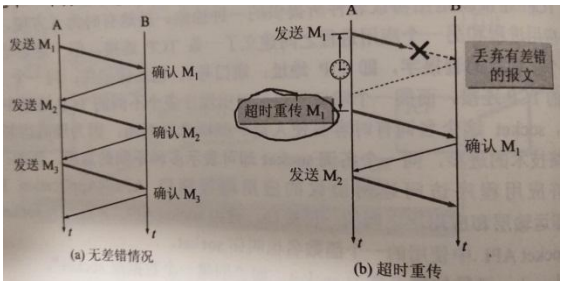
停止等待协议（A 向 B 发送数据报）：

1.A 向 B 发送分组 1，B 在收到分组 1 后就给 A 发送确认消息，A 收到确认消息后再发送下一个分组。

2.若 A 在向 B 发送分组 1 的传输过程中出现了差错，则 B 就不会向 A 发送确认信息。A 则需要设置一个超时计时器，若过了这段时间还没有收到 B 的确认，则认为刚才发送的分组 1 丢失了，此时需要重新发送分组 1。

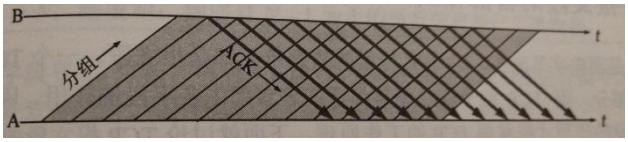
3.若 B 在向 A 发送确认消息的过程中出现了差错，A 将会重新发送分组 1，B 在收到重复分组 1 时，需要丢弃这个重复的分组 1，并且向 A 发送确认消息。

4. 若 B 在向 A 发送确认消息的过程中网络出现拥堵等情况，导致该确认消息“迟到”。此时 A 会向 B 重新发送分组 1，B 则丢弃重复的分组 1 并向 A 发送确认消息。A 在收到了确认消息后继续发送分组 2。而对于 B 向 A 第一次发送的分组 1 的确认消息，A 会收下确认消息，但什么也不做。



连续 ARQ 协议：

停止等待协议的信道利用率太低，连续 ARQ 协议是为了提升信道利用率。



以字节为单位的滑动窗口；

超时重传时间的选择（根据报文段的往返时间 RRT）；
选择确认 SACK（分组未按序到达时）；
发送方维持一个发送窗口，凡位于发送窗口内的分组都可连续发送出去，而不需要等待对方的确认。接收方一般采用累积确认，对按序到达的最后一个分组发送确认，表明这个分组为止的所有分组都已正确收到。

流量控制：控制发送方的发送速率，让接收方来得及接收。

拥塞控制：控制发送速率，防止网络中的路由器或路由过载。（需求的资源>可用资源）

运输连接管理：1.建立连接 2.数据传输 3.连接释放
1．建立连接：
所谓连接其实就是在主机的内存里保存一份对方的信息（如 ip 地址、端口号等），方便与对方传递消息。

三次握手：A 向 B 发送连接请求，B 接收后向 A 发送确认消息，A 接收到确认消息后向 B 发送确认消息。

三次握手的必要性：
说法一：（若不采用三次握手，则 A 在收到 B 的确认消息后则认为连接建立成功，而 B 在发送完确认消息后就认为连接建立成功，等待接收 A 发送的数据）假定 A 向 B 发送的连接请求，由于某种异常情况长时间滞留在了某些网络节点中。A 在超时时间内没有收到 B 的确认消息，则重新发送连接请求。在此次传输完成并释放连接后，假定第一次发送的连接请求此时到达 B 了，则 B 在发送完确认消息后就会一直等待接收 A 发来数据。但 A 并没有发出建立连接的请求，所以 A 接下到 B 的确认消息后什么也不做，造成了 B 的资源浪费。
说法二：由于通信时双向的，前两次握手只有 A 知道双向通信是正常的，而 B 并不知道从 B 到 A 的通信是不是正常的，所以 A 给 B 发送确认消息，表明 B 到 A 的通信也是正常的。

2．连接释放
四次挥手：四次挥手可以由双方任意一方发起
a． A 向 B 发送释放连接请求，表示单方面释放连接。
b． B 向 A 发送确认消息（B 只发送确认消息，因为 B 有可能还有数据没有发送完成）。
c． B 完成数据的传输工作后，向 A 发送释放连接请求。
d． A 向 B 发送确认消息，并等待 2*MSL 时间后释放连接；B 收到确认消息后马上释放连接。（因为该确认消息可能出现丢失的情况，为了在丢失之后能重新发送确认消息，需要保持连接 2*MSL 的时间）MSL:最长报文段寿命

四次挥手的必要性：
因为释放连接请求可以在数据传输的任一时刻发起，所以会出现在数据报传输的过程中其中一台主机发起释放连接请求的情况。为了保证该数据报能传输完成，采用了四次挥手的方法，有双方主机各发送一次释放连接请求，并确认后才释放连接。

应用层：

域名系统 DNS：

因特网的域名系统 DNS 被设计成为一个联机分布式数据库系统，并采用客户-服务器方式。域名到 IP 的解析是由分布在因特网上的许多域名服务器共同完成的。

解析过程：当某一应用进程需要把主机名解析为 IP 地址时，把待解析的域名使用 UDP 报文（为了减少开销）发送给本地域名服务器，本地域名服务器在查找域名后，将对应的 IP 地址返回。若本地域名服务器无法回应该请求，则向其它域名服务器发出查询请求。

动态主机配置协议 DHCP：

自动获取主机的 IP 地址、子网掩码、默认路由 IP、域名服务器 IP。

DHCP 使用客户-服务器方式，主机广播发送发现报文，目的 IP 地址置为全 1：255.255.255.255，源地址设为全 0：0.0.0.0。由 DHCP 服务器返回 IP 地址等配置信息。

每个网络找那个至少又一个 DHCP 中继代理（通常是路由器），用来转发 DHCP 报文到 DHCP 服务器中。以此来减少 DHCP 服务器的数量。

HTTP、SMTP

网络安全：

安全威胁：被动攻击、主动攻击。

被动攻击：从网络中窃听他人通信的内容，而不干扰信息流。（数据加密）

主动攻击：1.篡改：篡改网络中的报文。

2.恶意程序。

3.拒绝服务：DDos 攻击，使用大量主机不停的发送请求，使服务器瘫痪。

数据加密：

对称加密算法：

加密解密使用相同的密钥。

优点：速度快。

缺点：涉及到密钥管理的问题，在进行通信之前需要先交换密钥，若在交换密钥的过程中密钥被窃取，则无法保证数据安全。

常用的有 DES、3DES、AES、BlowFish、IDEA、RC5、RC6。

非对称加密（公钥加密）算法：

分为公钥密钥及私钥密钥，一个进行加密，另一个进行解密。

优点：允许公钥随意发布，私钥只由自己单方保管，安全性好。（衍生出数字签名）

缺点：算法复杂，性能远远比不上对称加密。

常用的有 RSA、ElGamal、背包算法、Rabin（RSA 的特例）、ECC。DSA（数字签名）。

数字签名：

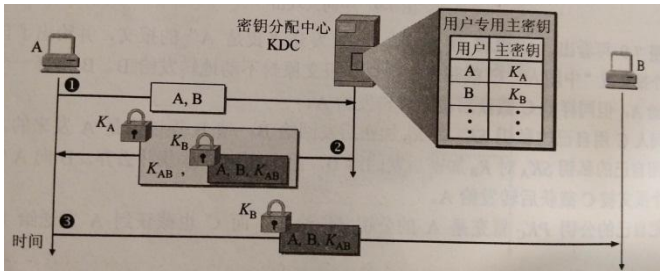
采用非对称加密（公钥加密）算法实现。

原理：用户 A 使用私钥加密数据，任何人都可以使用公钥来解密，由于私钥只由 A 拥有，所以可以肯定该数据必定来自 A。

公众可以验证该用户发布的数据或文件是否完整、是否被篡改，接收者可以信赖这条信息是来自该用户，该用户也无法抵赖。

报文鉴别：
鉴别接收到报文的真伪。
许多报文并不需要加密但却需要数字签名，以便让报文的接受者能够鉴别报文的真伪，然而对很长的报文进行数字签名会使计算机增加很大的负担。
通过报文摘要算法得到很短的报文摘要进行签名。
报文摘要（实质是散列算法）是单向的，不能通过逆计算得到原始的报文。常用的有MD5、SHA、SHA-1。

对称密钥的分配：
设立密钥分配中心 KDC（Key Distribution Center），给需要进行秘密通信的用户临时分配一个回话密钥。
需要使用 KDC 的用户需要在 KDC 进行登记，并记录和 KDC 进行通信的主密钥。
密钥分配协议 Kerberos V5，它既是鉴别协议，同时也是 KDC。使用 AES 加密。



非对称密钥的分配：
数字证书认证机构（CA）：
是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中的公钥的合法性检验的责任。

因特网使用的安全协议：
网络层：
IP 安全协议 IPsec，包含的信息：1.32 位的连接标识符（安全参数索引 SPI）2.源点及终点（IP 地址）3.使用的加密类型 4.加密的密钥 5.完整性检查的类型 6.鉴别使用的密钥

运输层：
安全套接字层 SSL（Secure Socket Layer），运输层安全 TLS（Transport Layer Security）。
TLS 是基于 SSL3.0 设计的。
SSL/TLS 作用于应用层和运输层之间，在应用层使用 SSL/TLS 最多的就是 HTTP，但不局限于 HTTP。在发送方，SSL 接收应用层的数据，对数据进行加密，然后把加了密的数据送往 TCP 套接字。在接收方，SSL 从 TCP 套接字读取数据，解密后把数据交给应用层。

SSL 建立安全会话的简要过程：
1.协商加密算法。浏览器 A 向服务器 B 发送浏览器的 SSL 版本号和一些可选的加密算法，B 从中选定自己所支持的算法，并告知 A。

2.服务器鉴别。服务器 B 向 A 发送一个包含其 RSA 公钥的数字证书，A 使用该证书的认证机构 CA 的公开发布的 RSA 公钥对该证书进行验证。
3.会话密钥计算。由浏览器 A 随机产生一个秘密数，用服务器 B 的 RSA 公钥进行加密后发送给 B。双方根据协商的算法产生一个共享的对称会话密钥。
4.安全数据传输。双方用会话密钥加密解密它们之间传输的数据并验证其完整性。

防火墙：

1.分组过滤路由器：
根据过滤规则对进出内部网络的分组执行转发或者丢弃，过滤规则基于分组的网络层或运输层首部的信息，如：源/目的 IP、端口、协议类型等。
优点：简单高效。
缺点：不能对高层数据进行过滤，例如不能禁止某个用户对某个特定应用的某个特定操作等。
2.应用网关（代理服务器）：
所有进出网络的应用程序报文都必须通过应用网关，应用网关在应用层打开该报文，查看该请求是否合法，若合法则以客户进程的身份将请求报文转发给服务器，若不合法则丢弃。
优点：控制精确。
缺点：每种应用都需要不同的应用网关；在应用层处理和转发报文，负担较重。

无线网络和移动网络：

无线网络和移动网络的数据链路层与传统的有线因特网的数据链路层差别很大。

无线局域网 WLAN（wireless local area network）：
使用星型拓扑结构。
数据链路层使用 CSMA/CA 协议，在碰撞检测时与 CSMA/CD 协议有所不同。
CSMA/CA 协议的设计是为了尽量减少碰撞发生的概率。
……..// TODO

无线个人区域网 WPAN（wireless personal area network）：
在个人工作的地方，把属于个人使用的垫子设备用无线技术连接起来自组网络。
蓝牙、低速 WPAN、高速 WPAN。

移动通信的种类很多：蜂窝移动通信、卫星移动通信、集群移动通信、无绳电话通信等。
蜂窝移动通信网：
移动 IP：
用户在改变自身地理位置时，接入的网络也会变化，此时 IP 地址也会发生改变。移动 IP 需要解决的就是，使用户的移动性对上传的网络应用是透明的。
移动站 A 必须记录一个永久地址，接入的网络称为归属网络。当移动站 A 移动到另一个地点时，它所接入的网络称为被访网络。被访网络给为 A 创建一个转交地址。
使用代理的方式，移动站 A 访问服务器 B 时，B 将数据返回给 A 的永久地址，再由其归属网络转发到转交地址。