吴雨娟 22920192204097.

厦門大學
XIAMEN UNIVERSITY
ADD:FUJIAN XIAMEN CABLE:0633 P.C:361005

6-24

解：邮局抽收POP使用客户服务器的工作方式：在接收邮件的用户计算机中的用户代理协议运行POP3客户程序，而在收件人所连接的ISP的邮件服务器中则运行POP3服务器程序。在电子邮件中，收件人在打算收信时，就运行计算机中的用户代理，使用POP(或IMAP)协议读取发送给自己的邮件。IMAP与POP的区别：用户从POP服务器读取了邮件，POP服务器就把该邮件删除，这在某些情况下就不方便。而IMAP最大的好处就是用户可以在不同的地方使用不同的计算机，随时上网阅读和处理自己的邮件。IMAP还允许收件人只读取邮件中的某一部分。

6-30

解：因为有时对方的邮件服务器不工作，邮件就发送不出去。或者对方的邮件服务器在收到邮件后，在收件人读取前就出现了故障，也会使邮件丢失。

6-32

解：DHCP提供了即插即用连网机制。所以DHCP协议用在一台计算机加入一个新的网络时，需要运行DHCP协议来获取这台计算机的IP地址。当一台计算机第一次运行引导程序时，ROM中有没有该计算机的IP地址、子网掩码、或某台域名服务器的IP地址的任何一个。

6-37

解：SNMP使用两种操作："读"操作，用Get报文来检测各被管对象的状况；"写"操作，用Set报文来改变各被管对象的状况。SNMP在Get报文中设置了请求标识符字段，而代理进程在发送响应报文时也要返回此请求标识符。由于管理进程可同时向许多代理发出请求读取多台代理的报文，因此设置了请求标识符，可使管理进程收到返回的响应是对应于哪一个请求报文。

厦門大學
XIAMEN UNIVERSITY
ADD:FUJIAN XIAMEN CABLE:0633 P.C:361005

7-07

解：对称密钥体制的特点：加密密钥与解密密钥是相同的。优点：ee的简单。缺点：在高度自治化的大型计算机网络中，用传统来传送密钥是不合适的，传送密钥的安全性通信不容易找到。且如果丢失的是密钥，就会给密钥的管理和更换带来极大不便。公钥密码体制的特点是：加密密钥PK是向公众公开的，而解密密钥SK是需要保密的。加密算法E和解密算法D也都是公开的。优点：可以进行数字签名，可以避免对称密钥密码体制的密钥分配问题。缺点：使用数字公式进行加密和解密，比使用对称密钥加密求慢得多，开销较大。

7-13

解：不行。因为A也有和B同样的密钥。如果A出示此报文给第三方，第三方可能会认为此报文为A编造的。A无法证明世界上只有B才是该报文的唯一发送方，因为A也可以用该密钥产生报文。

7-25

解：描述TLS在多数情况下用的是单向登别，即客户端(浏览器)登别服务器。描述TLS的工作过程分为握手阶段和会话阶段。双方建立TCP连接后，协商加密算法，客户A向服务器B发送自己选定的加密算法，服务器B从中确认自己所支持的算法，同时把自己的CA的主证书发送给A。客户A用数字证书中CA的公钥对数字证书进行验证登别。接下来是生成主密钥。客户A按照双方确定的密钥交换算法生成主密钥MS，客户A用B的公钥PK_B对主密钥MS加密，得出加密的主密钥$PK_B(MS)$，发送给服务器B。服务器B用自己的私钥把主密钥解密出来。这样，客户A和服务器B都拥有了为后面的数据传输使用的共同的主密钥MS。为使双方的通信更加安全，客户A和服务器B最好使用不同的密钥，于是主密钥被分割成6个不同的密钥。

7-26

解：缺点在第③个步骤，用CA发布的公钥登别B的证书时可以发现对方是不是真正的经销商。

厦門大學
XIAMEN UNIVERSITY
ADD:FUJIAN XIAMEN CABLE:0633 P.C:361005

7-27

解：PGP是一个完整的电子邮件安全软件包，包括加密、签到、电子签名和压缩等技术。把现有的一些加密算法（如RSA公钥加密算法或MD5报文摘要算法）集合在一起。它提供电子邮件的安全性、发送方签到和报文完整性。

假定A向B发送电子邮件明文X，现在用PGP进行加密。A需要做以下几件事：①用A的私钥SK_A对明文邮件X进行签名，把签名插接在明文X后面。②利用随机数A生成一次性密钥K。③用A生成的一次性密钥K对已签名的邮件加密。④用B的公钥PK_B对A生成的一次性密钥K进行加密。⑤把已加密的一次性密钥和已加密的签名邮件，插接在一起发送给B。

B收到A发过来的报文后需做以下几件事：①B根据邮件的头标，很简地把已加密的一次性密钥和已加密的签名报文分离开。②用B的私钥SK_B解出一次性密钥K。③用导出的一次性密钥K对加密的签名邮件进行解密，分离出明文邮件X和A的数字签名。④用B手中A的公钥PK_A对A的数字签名解密，验证邮件的完整性。

9-09

解：假设A和C都和B通信，但A和C相距较远，彼此都检测不到对方发送的信号，但都会产生不重接，为了解决A、C互为隐蔽站的问题，使用RTS和CTS帧。在准备A发送数据帧之前先发送一个短的控制帧，叫作请求发送RTS，它包括源地址、目的地址和这次通信所需的持续时间。若信道空闲，则目的站B就响应一个控制帧，叫作允许发送CTS，它包括这次通信的持续时间。A收到CTS帧后就可以发送其数据帧。C收到B发送的响应CTS帧后，知道有站点要与B通信了，因此在一段时间内不会发送数据干扰A和B的通信。

RTS/CTS是选择使用的，因为使用RTS/CTS帧会增加开销，不一定能得到更好的效果。如果无线局域网的工作环境较好，碰撞产生不多，就可以不采用RTS/CTS帧。

9-26

解：该站点发送的信息为DIFS + RTS + SIFS + CTS + SIFS + 数据帧 + SIFS + Ack

$$= DIFS + 3\times SIFS + 1000字节 + 20字节 + 14字节 + 14字节$$

$$= DIFS + 3\times SIFS + 1048字节$$

∴ 经历的时间 $= 128\mu s + 3\times 28\mu s + \frac{1048\times 8}{11}\mu s \approx 974.2\mu s$