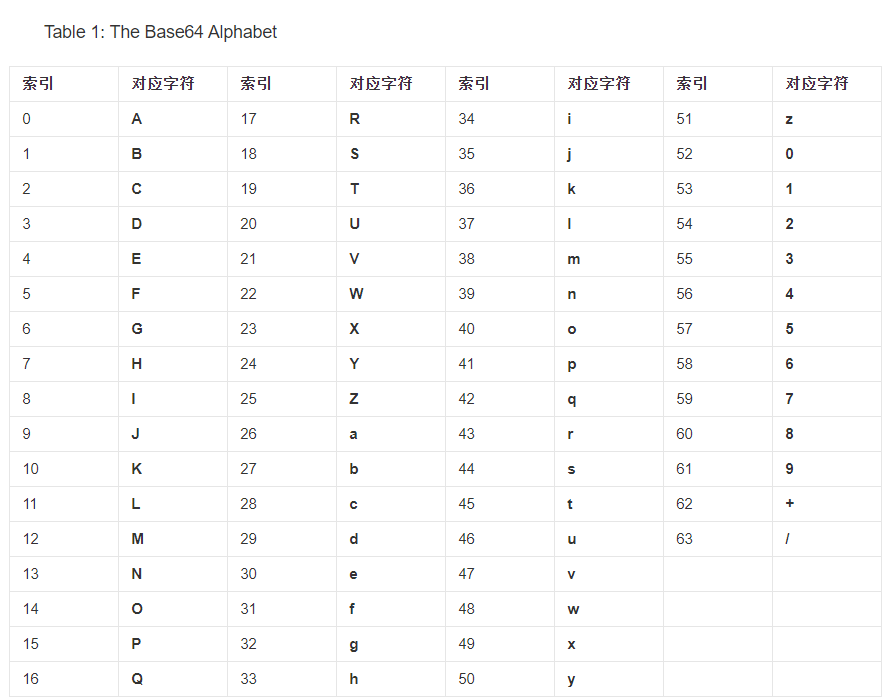
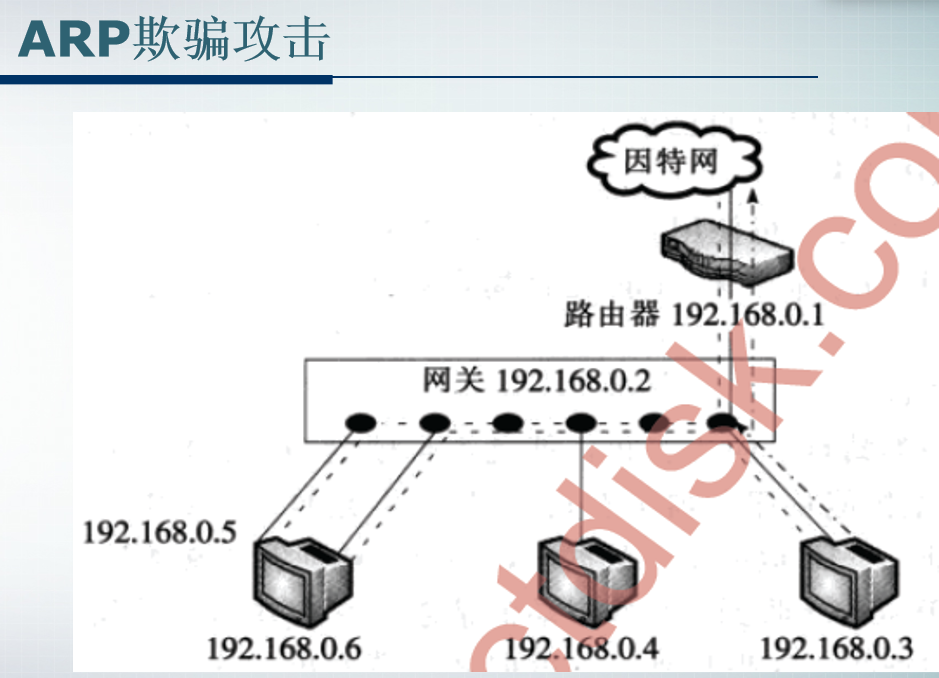
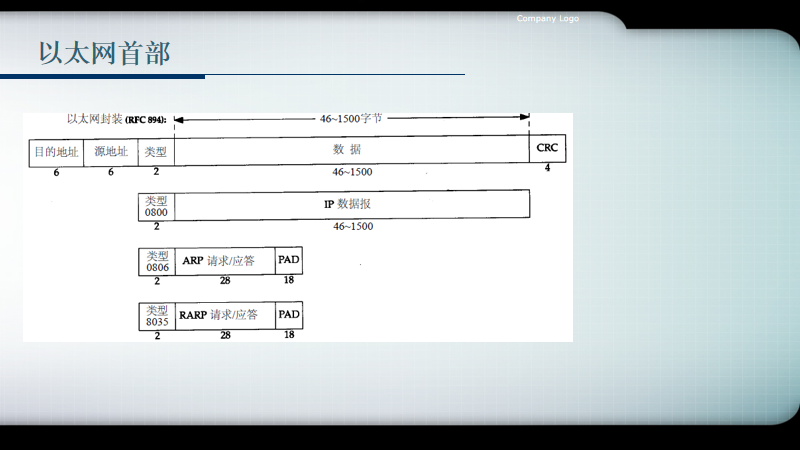
# 简答题

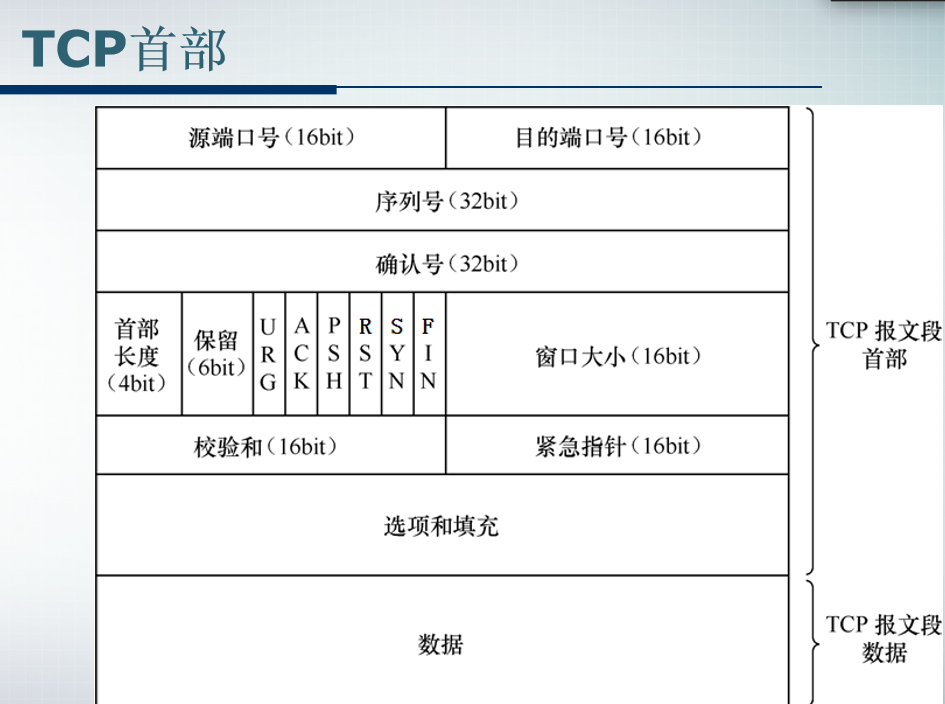
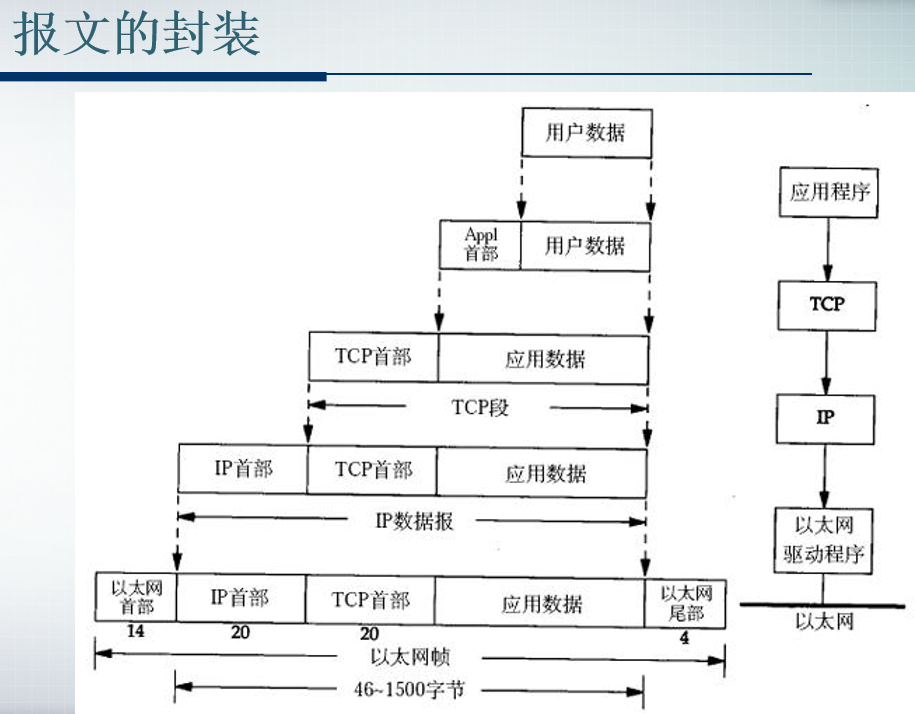
1. Base64编码：  
   （3\*8 -> 4\*6）  
   e.g: 输入： abc  
    转换ascll码：97 98 99  
    转换二进制：01100001|01100010|01100011  
    重新组合成4组6位：011000|010110|001001|100011  
    每组前面用0补全8位：00011000|00010100|00001001|00100011  
    二进制转十进制：24 20 9 35  
    对应下表转换：YWJj  
    
2. ARP欺骗的过程简介：  
     
    攻击者主机需要用两张网卡（0.5/0.6）接入交换机的两个端口，并具有转发IP数据包的能力。  
    主机A想要与网关通信，广播发送ARP请求，攻击者迅速拦截  
    用网卡1伪造网关地址向被攻击者发送ARP请求包，把自己伪装成主机A的网关，  
    另一边用网卡2伪造主机地址向网关发送ARP请求包，把自己伪装成被攻击主机，

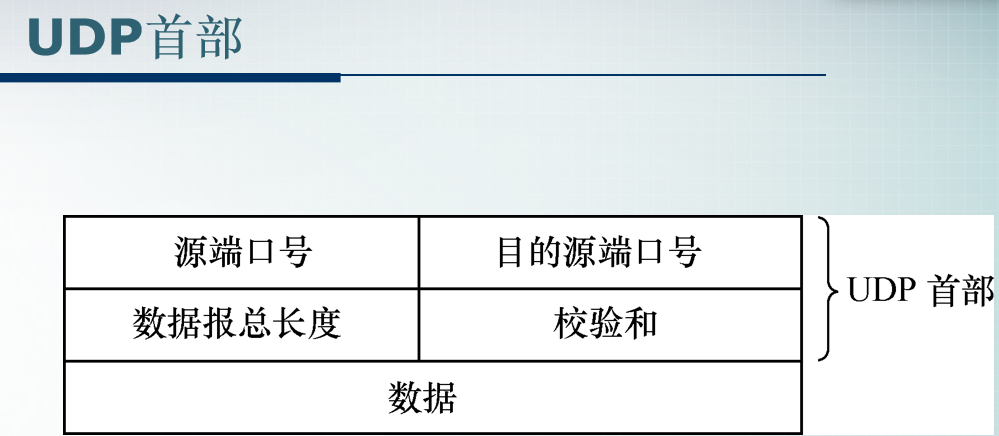
将错误的MAC地址和IP映射更新到网卡和目标主机上，  
 使自己成为两者通讯之间的中间人，转发和处理两者之间的数据，  
 起到同时欺骗目标主机和网关的目的。

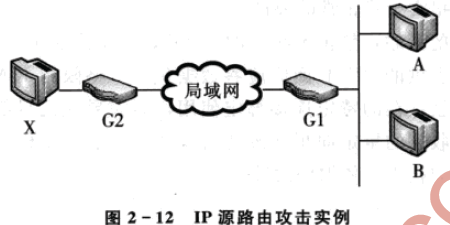
1. 数据帧的解读：









1. IP源路由攻击：  
   

现有主机A是主机B的被信任机，X想要冒充A从B获得某些服务。

1: 修改距离X最近的路由器G2将包含B目的地址的数据包将X所在网络作为目的地  
 2: 利用IP欺骗，将数据包的源地址改为主机A的地址并向主机B发送带有源路由选项的数据包。

３：B回送数据包时根据数据包的源路由选项反转使用源路由，向G２发送  
 ４：G２收到数据包后根据X事先修改的路由表向X所在网络转发数据包

5：自此，X即可在其局域网上侦听并收取B的数据包。  
源径路由就是数据发送的主句能要求目标主机回复报文所经过的路径。发送主机在发送数据的同时指定了目标主机回复信息经过的路径。入侵者可以将自己的主机添加到路由表中，然后向目标主机发送伪造的路由信息，让目标主机发源路径回复。这样目标主机的回复信息就按照这个路径经过入侵者的路由器，入侵者就可以从目标路由器中窃听信息了。  
5. NAT的工作过程：  
 NAT即网络地址转换，内网使用内部地址通过NAT转换成合法的IP地址并在Internet上使用。

NAT有三种类型：  
 静态NAT：内网主机与外网某个合法地址一对一对应映射  
 NAT池：在外网中定义一系列合法地址动态分配映射到内部网络  
 端口NAT（PNAT）：内部网络地址映射到外部网络的一个IP地址的不通关端口。  
过程：内网主机A与外部网络主机B通讯，源ip为A的内网地址，目的IP为主机B的外网地址，到网络边界通过NAT技术将源IP转换为主机A映射的某外网合法地址，目的IP不变，主机B收到并回复消息时，将主机A映射的某外网合法地址作为目的IP地址，主机B的外网地址为源IP地址，主机A所在的局域网的网络边界收到B的消息后又通过NAT技术把A映射的某公网地址替换为A的内网地址并将数据转发给主机A。