# 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

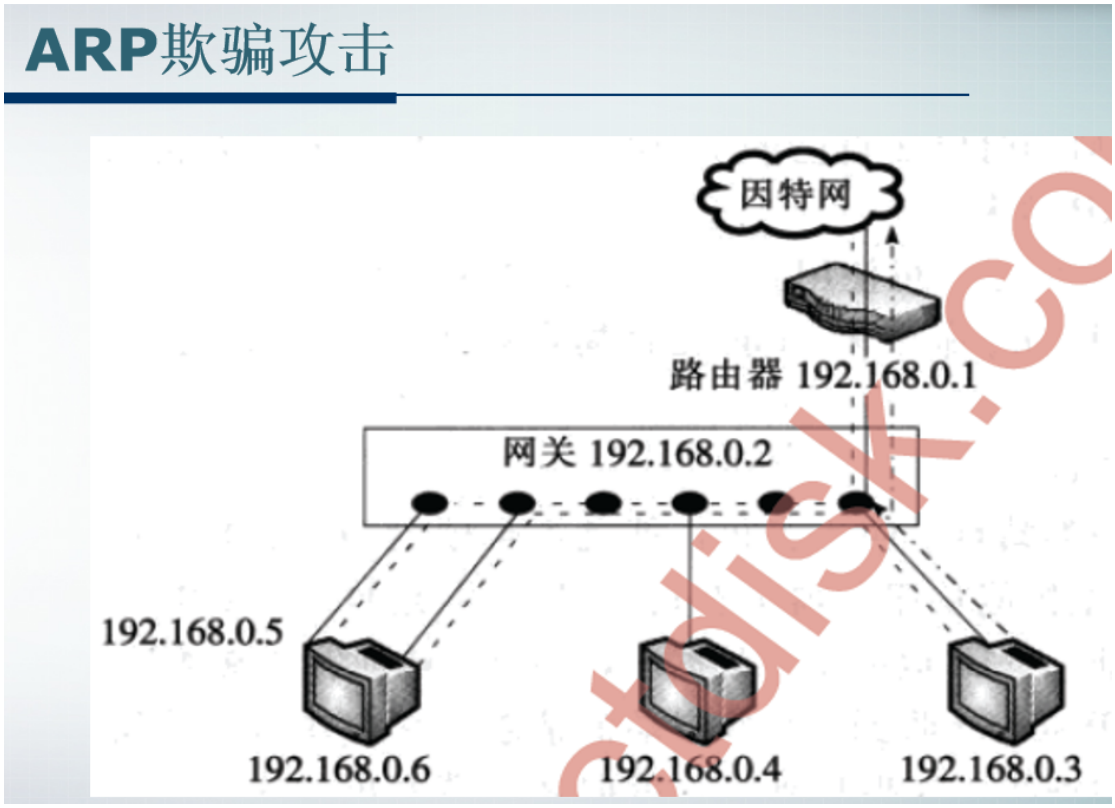
二进制转十进制：24 20 9 35

对应下表转换：YWJj

Table 1: The Base64 Alphabet

| 索引 | 对应字符 | 索引 | 对应字符 | 索引 | 对应字符 | 索引 | 对应字符 |
|---|---|---|---|---|---|---|---|
| 0 | A | 17 | R | 34 | i | 51 | z |
| 1 | B | 18 | S | 35 | j | 52 | 0 |
| 2 | C | 19 | T | 36 | k | 53 | 1 |
| 3 | D | 20 | U | 37 | l | 54 | 2 |
| 4 | E | 21 | V | 38 | m | 55 | 3 |
| 5 | F | 22 | W | 39 | n | 56 | 4 |
| 6 | G | 23 | X | 40 | o | 57 | 5 |
| 7 | H | 24 | Y | 41 | p | 58 | 6 |
| 8 | I | 25 | Z | 42 | q | 59 | 7 |
| 9 | J | 26 | a | 43 | r | 60 | 8 |
| 10 | K | 27 | b | 44 | s | 61 | 9 |
| 11 | L | 28 | c | 45 | t | 62 | + |
| 12 | M | 29 | d | 46 | u | 63 | / |
| 13 | N | 30 | e | 47 | v | | |
| 14 | O | 31 | f | 48 | w | | |
| 15 | P | 32 | g | 49 | x | | |
| 16 | Q | 33 | h | 50 | y | | |

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，

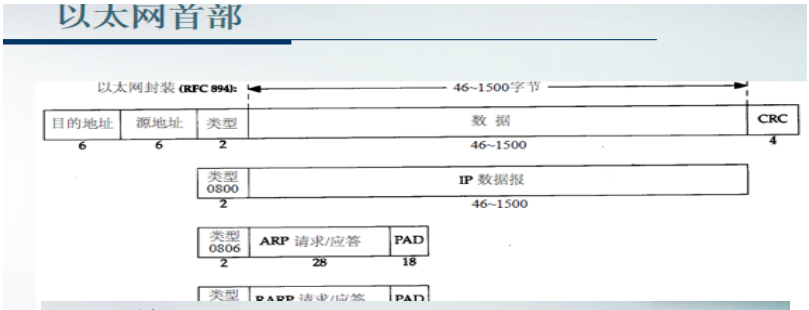
另一边用网卡 2 伪造主机地址向网关发送 ARP 请求包，把自己伪装成被攻击主机，

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，

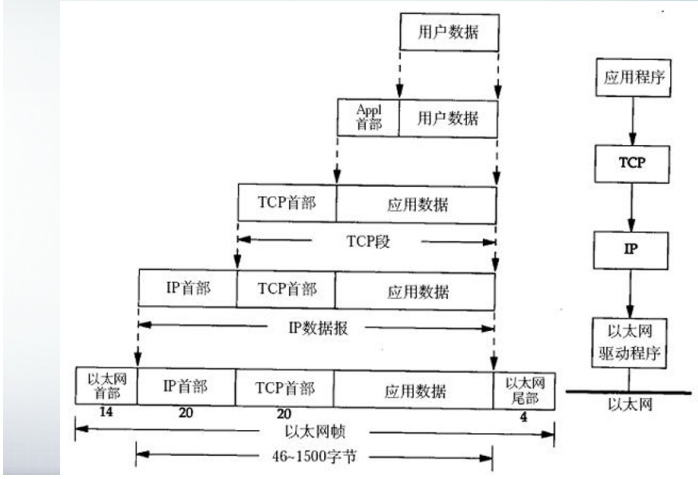
起到同时欺骗目标主机和网关的目的。

3. 数据帧的解读：




## TCP首部


## 报文的封装




## UDP首部


4. IP 源路由攻击：

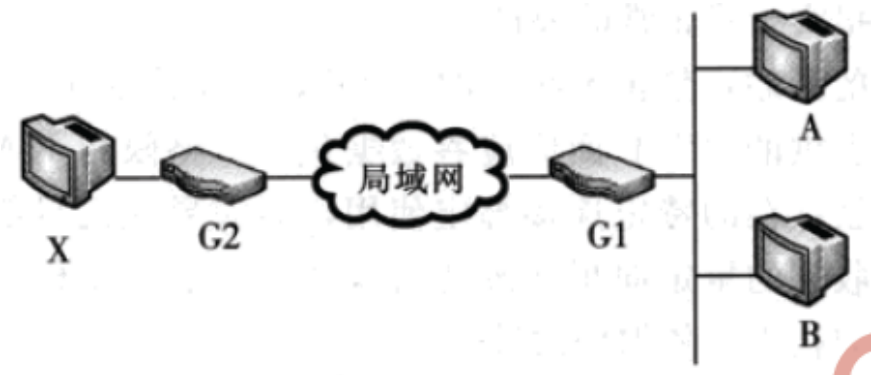



**图 2－12　IP 源路由攻击实例**

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 G 2 发送

4：G 2 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。