

目前大家讨论网络安全比较多的是如何防止非法用户侵入内部网，目前世界上公认的有以下几个方案：

- Ⅰ 在两个网之间设置防火墙软件；
- Ⅰ 安全检查（身份认证）；
 - Ⅰ 加密
 - Ⅰ 数字签名
 - Ⅰ 内容检查
- Ⅰ 通过网络的逻辑分段（虚拟网）和物理分段并实现网络的交换化，将不同的网段相互隔离，除了可以防止网络风暴，还可以防止数据的流失。

由于以上几个方面已经讨论了很多了，在这里我们就不详细讨论了。下面我们着重讨论一下内部网数据的安全问题。

外部网与内部网之间的安全问题，由于近年来对黑客的宣传，大家都比较重视，而对内部网的安全问题却不太重视。实际上，网络的安全包括外部网和内部网的安全，一旦外部网被突破（这是经常发生的），内部网的安全措施就成为最后一道防线，如果仍被突破或通过电磁感应侵入，整个网络将完全暴露，所有重要数据都将被窃取，甚至入侵者还可以假扮身分发出命令，其后果将不堪设想。

内部网的安全一般主要靠网络的物理划分、网络操作系统的权限管理和一套行之有效的安全管理制度。由于现在网络一般采用非屏蔽双绞线作为传输介质，随着科技的进步，入侵者完全可以采用非接触方式在远方通过双绞线的电磁辐射来获取网络信息。这样，网络操作系统的权限管理和安全管理制度都将失效。因此，象政府上网等国家机关尤其是要害机关就应该采用一套对传输线路上传输信息进行加密的系统，而该系统又可以对上层协议软件和应用软件透明传输并实现以太网/快速的传输速率。为了适应我国急剧发展的政府及其它一些特殊部门和公司网络对网络安全产品的迫切需要，我们开发了基于以太网传输标准的加密网卡系统。下面，我们就对它及其组网方式进行介绍。

1. 加密网卡系统介绍

加密网卡是供军用及其它一些需要通讯加密的政府要害部门如检察、公安等使用的一种高性能加密网卡。也可以用于有保密要求的政府部门。该加密网卡性能完全满足这些部门的特殊要求，具有高速的通讯速率，快速的加密、解密算法，灵活的布线方式，简单的安装使用方法，而且数据加密、解密对用户是完全透明的，用

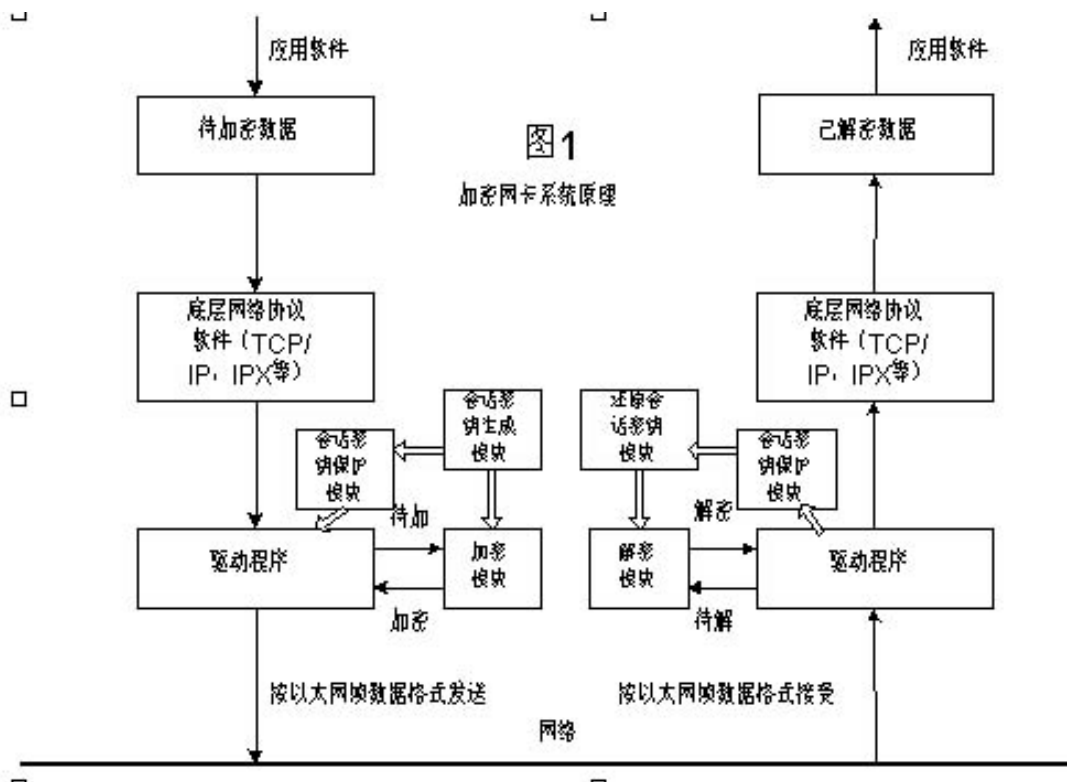
户根本不用考虑数据是如何加密、解密的。所以，加密网卡系统是一个比较理想的加密系统。

1.1 主要性能指标

- I 工作方式：提供全双工/半双工工作方式
- I 接口标准：与计算机采用 PCI 总线接口，与网络采用双绞线 RJ-45 接口，可采用屏蔽或非屏蔽双绞线
- I 数据传输速率 (bit/s)：10M/100M
 - I 密码方式：序列加密
 - I 基本密钥量： 1×10^{19}
 - I 信息密钥量： 1×10^{12}
- I 加、解密时延：数据延时最大不超过 20%

1.2 基本原理

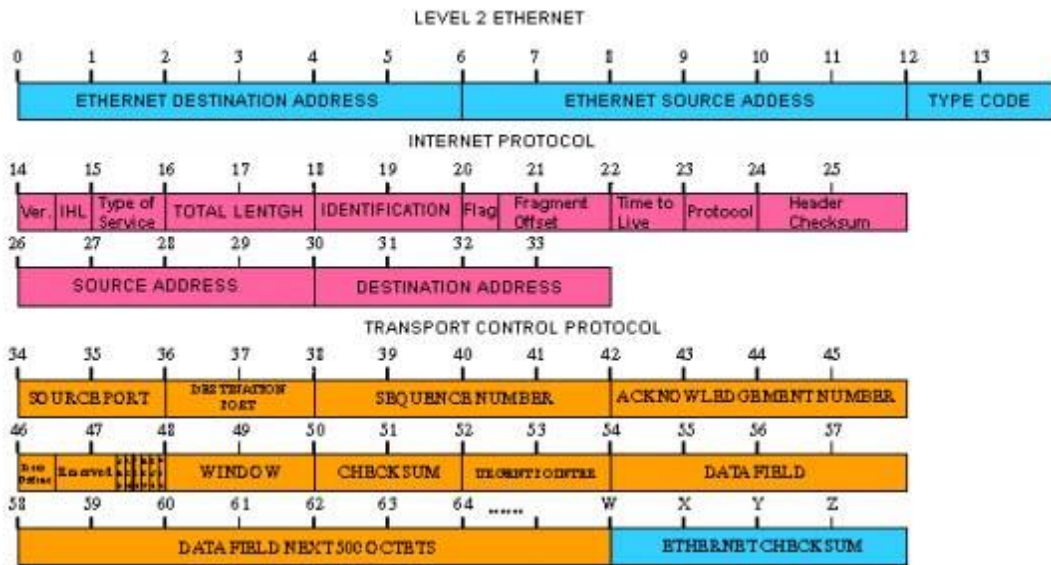
加密网卡系统由一块加密网卡及一套驱动软件组成，提供加密和驱动程序功能。加密网卡采用目前流行的 PCI 总线，提供即插即用功能。提供 10M/100Mbps 的通讯速率，可根据接入设备自动调整通讯速率和全双工、半双工工作方式。当不使用加密功能时，与现有的商用 10M/100M 以太网卡完全兼容。当使用加密系统提供加密时，则该计算机就成为一台加密的计算机，只有与其它插有同样加密网卡的计算机才能正常通讯，其它计算机即使接受到通讯内容也不能破译其内容。其安装方法也非常简单，与普通的商用网卡安装方法完全一样，易学易用。采用软硬件结合的加密方案，实现加密、解密、会话密钥生成和会话密钥保护等功能，采用特殊的加密算法，即保证了加、解密的快速，又保证了加密的安全性，也能灵活的对密钥进行管理。本加密网卡适用于目前流行的硬软件平台（如 WINDOWS NT，WINDOWS 95/98 等），具有良好的适用性和兼容性。



其加解密原理图 1 所示：

以 TCP/IP 协议为例，TCP/IP 的帧格式如图所示前 54 字节是 TCP/IP 帧包头信息。信息应用程序发送数据后，由 TCP/IP 协议组软件将它打包成 TCP/IP 帧，再通过 NDIS 接口协议将它传递给驱动程序，通过软硬结合的加密算法，选择适当的密钥，将 TCP/IP 数据包按 64 位或 128 位加密（加密位数越高，数据越难解密，就越安全，当然，数据加解密所用时间就越长），再发送出去。这里的数据包的有关地址解析，IP 帧控制信息，TCP 帧控制信息等以太网帧控制信息都不加密，以免通过具有第三层交换功能的交换机时无法进行数据路由。接受方收到数据包之后，按相反的方向进行解密。通过以上过程可以看出，数据加解密对上层软件完全透明，由于采用软硬结合的加解密方法，加解密速度快，这些都是纯软件加密方案无法作到或做起来很难的。

OCTET LOCATIONS ON A TCP/IP FRAME



还有就是密钥的更新和维护。根据我国公安部和国家安全局的规定，普密和特密级的密钥必须专人管理和专人定期更新。而政府上网的内部网络属于政府机关的网络，应该采用普密级的加密方案。因此加密网卡系统的密钥更新不适合通过网络自动更新，我们专门设计了更新密钥的接口，不用开机就可更新密钥，减少了工作人员的工作量，保证了密钥的安全。

2. 加密网络方案

一个构建中的政府机关内部网拓扑结构如图 2 所示。

该网是一个全交换式网，可以实现交换到桌面。每个房间都有不等的信息口，客户端计算机通过非屏蔽双绞线连到本楼层的 10M 交换机，10M 交换机再通过光纤以 100M 速率连到主交换机上。其中，1 层到 7 层连到一台主交换机，8 层到 14 层连到另外一台主交换机上。两台主交换机之间通过特殊接口相连。这里的主交换机采用的是 3com 的 CB3500 交换机，它可以以线速实现第三层交换，按端口、MAC 地址、IP 地址等划分虚拟网，而且在断电的时候可以通过特殊接口将本交换机以太网接口的信息传到另外一台交换机中。通过这样的网络拓扑，就可以实现服务器的冗余功能，增强网络的容错性，保证政府上网网络的稳定性。

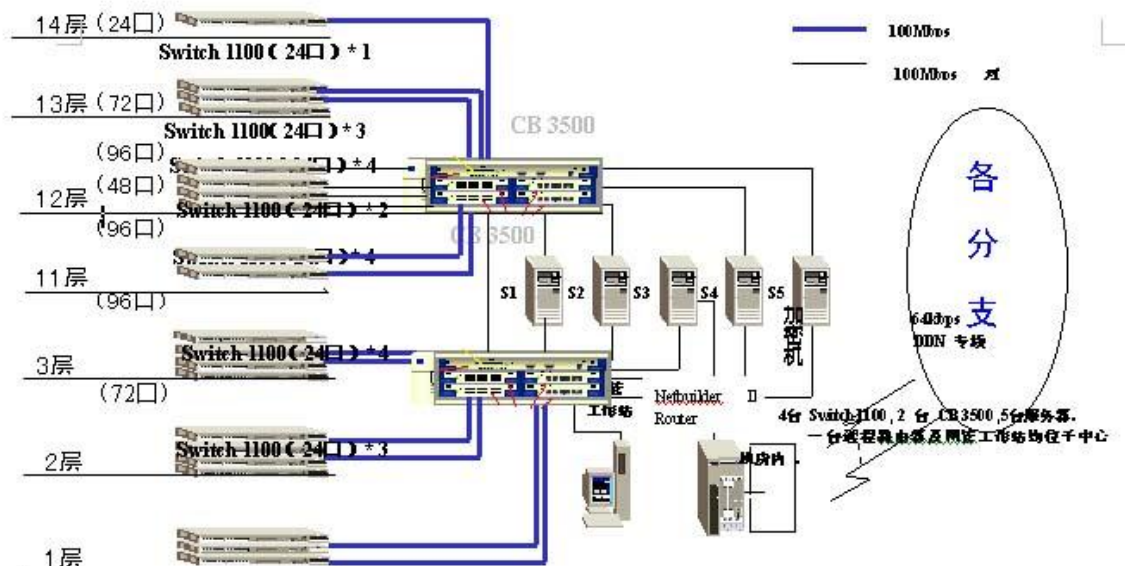
在每台客户端计算机中和服务器中均安装加密网卡系统，网卡中传输的纯数据均是经过加密的数据（所谓纯数据，就是指以太网帧中除了控制信息，地址信息等以外的传给上层软件的数据）。这样，入侵者虽然可以通过电磁方式获取信息，但是得到的是加密过的信息，无法窃取信息。而接受方因为采用了相同的加密网卡

系统，具有相同的密钥，就可以正确的接受信息，将信息传递到上层协议和软件。另外，可以根据阅读文件，查询数据的权限将密钥分为相应的级别，不同的密钥级别访问不同级别的文件。同时，高级的密钥可以访问低级密钥的计算机的内容，而低级计算机无法访问高级密钥的计算机。利用这种方法，与网络操作系统的权限管理相结合，可以更好的管理网络，确保网络的安全，也可以使领导更好的考察工作人员的工作。

在这个网络中，要特别注意网管工作站。由于网管工作站的特殊用途，它要接受来自交换机的信息并发送相应的网管信息到交换机，这就决定这些信息不能是加密的，否则就无法管理这些交换机。有两种方法可以解决这个问题。一种是这个网管工作站就安装普通商用网卡，就不存在这个问题。但是对于用户来说，在加密网络上传输的数据应该都是加密的，这里如果用的是商用网卡，就有可能是一个漏洞，如果被高超的入侵者利用就有可能造成可怕的后果。另外的方法就是为该网管工作站特制一套加密网卡系统，对网管信息不加密，对其它的信息加密。这样虽然费用要高，但是非常安全，有利于保持整个网络的抗侵入性。但网管信息千差万别，要全部准确的区分它非常困难，因此要根据具体的网络应用环境具体来设计这套加密网卡系统。

3. 应用前景

随着社会的进步，网络的飞速发展，政府上网、电子商务等基于网络的应用会越来越多，网络安全必将会越来越受到重视。采用加密网卡系统和防火墙等软件的软硬结合的加密解决方案的优越性会越来越明显，必将得到广泛的应用。



[参考文献]:

- 1、《INTERNET 网络安全专业参考手册》，（美）Derek Atkins 等著，严伟、刘晓丹、王千祥等译。机械工业出版社，1998 年 8 月
- 2、《TCP/IP 故障检测与维护》，（美）Mark A. Miller, P.E. 著，夏春和，张辉等译。科学出版社，1996 年 4 月