- 加密。SNMP PDU 能够使用密码分组链接模式的数据加密标准（DES）进行加密。注意到因为 DES 是一个共享密钥的系统，故用户用于加密数据的密钥必须被要对该数据解密的接收实体所知道。
- 鉴别。SNMP 使用了报文鉴别码（MAC）技术，以提供鉴别并保护数据不受篡改［RFC 4301］，其中的 MAC 我们已在 8.3.1 节中学习过。前面讲过 MAC 要求发送方和接收方都知道一个共同的密钥。
- 对重放攻击的防护。在第 8 章中我们讨论了不重数能被用于防护重放攻击。SNMPv3 采用了相关方法。为了确保一个接收的报文不是某个先前报文的重放，该接收方要求发送方在每个报文中包括一个基于接收方中的计数器的值。该计数器的功能与不重数相同，反映了自接收方的网络管理软件最后一次启动以来的时间和自接收方的网络管理软件最后一次配置以来启动的总数。只要在接收报文中的计数器位于接收方的实际值的某种错误容限内，该报文被认为是非重放攻击的报文，此时它已被鉴别和/或加密。详见［RFC 3414］。
- 访问控制。SNMPv3 提供了一种基于视图的访问控制［RFC 3415］，该方法控制了哪些网络管理信息能被哪些用户查询和/或设置。一个 SNMP 实体在本地配置库（Local Configuration Datastore，LCD）保留了有关访问权限和策略的信息。LCD 的某些部分自身可作为被管对象访问，在基于视图访问控制模型配置 MIB 中定义［RFC 3415］，并因此能够经 SNMP 从远程进行管理和操作。

9.4 ASN.1

在本书中，我们已经涉及了一些计算机网络的有趣主题。然而，本节有关 ASN.1 的内容或许算不上前 10 个有趣的主题。像蔬菜有益于健康一样，有关 ASN.1 的知识和表示服务的更广泛问题是对你有益的东西。ASN.1 是一种源于 ISO 的标准，用于一些因特网相关的协议中，特别是用于网络管理领域中。例如，我们在 9.3 节中看到，SNMP 中的 MIB 变量与 ASN.1 有不解之缘。尽管 ASN.1 的有关资料可能相当枯燥，但我们希望读者能够认识到这些相关材料的重要性。

为了激发我们下面的讨论，这里考虑下列可能的实验。假定一个人能够可靠地将数据从一台计算机的内存直接复制到远程另一台计算机的内存中。如果他能够这样做，其中的通信问题将是如何解决的？该问题的答案取决于他对“通信问题”的定义。毫无疑问，一个完善的内存到内存复制将是从一台机器到另一台机器的比特和字节的精确通信。当在接收计算机上运行的软件存取这些数据时，这些比特和字节的实际复制意味着什么？我们能够看到与在发送计算机内存中所存储的一样的值吗？对该问题的答案是“不一定”！该问题的症结在于，不同的计算机体系结构、不同的编译程序具有不同的存储和表示数据的常规方法。如果数据要通信，或在多台计算机中存储（因为数据在各通信网络中），显然必须要解决数据表示的问题。

作为该问题的一个例子，考虑下面简单的 C 代码段。这个结构怎样在内存中安排呢？

```
struct {
  char code;
  int x;
  } test;
test.x = 259;
test.code = 'a';
```