国　际　电　信　联　盟

ITU-T

国际电信联盟
电信标准化部门

X.800

修订1
(10/96)

X系列：数据网路与开放系统通信
安全

CCITT应用的开放系统互连安全架构

修订1：局域网的二层安全服务和机制

ITU-T 800 建议书 - 修订1

（前 CCITT 建议书）

ITU-T

国际电信联盟

ITU-T X 系列建议书

数据网路与开放系统通信

公用数据网	X.1-X.199
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	X.200-X.299
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	X.300-X.399
概述	X.300-X.349
卫星数据传输系统	X.350-X.399
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI 组网和系统概貌	X.600-X.699
组网	X.600-X.629
效率	X.630-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI 管理	X.700-X.799
系统管理协议子集和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能	X.730-X.799
安全	**X.800-X.849**
OSI 应用	X.850-X.899
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.899
开放分布式处理	X.900-X.999
[...]	

欲了解更详细信息，请查阅 ITU-T建议书目录。

前言

ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化大会（WTSC）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSC第1号决议（赫尔辛基，1993年3月1-12日）规定了ITU-T成员批准建议书所遵循的程序。

ITU-T第7研究组（1993-1996年）编写的ITU-T X.800建议书修订1，于1996年10月5日根据WTSC第1号决议获得批准。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

© 国际电联 2013

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

摘要

X.800建议书概述了分配到七层OSI参考模型的安全服务。作为附件D发布的修订1，将数据链路层的安全服务加以扩展，以满足网络安全要求。

X.800 建议书修订1

CCITT应用的开放系统互连安全架构

附件 D

局域网的二层安全服务和机制

（1996年，日内瓦）

D.0 引言

本附件涉及局域网（LAN）的二层安全服务和机制。

第7段的表2对安全服务位置的说明提出，第2层只应提供保密性服务。然而众所周知，可能需要在某些环境中部署局域网附加2层安全服务和机制。例如，一个可能没有部署完整的OSI功能或接受2层中继的机构，可能需要除保密以外的安全服务。

D.1 LAN安全服务

可在数据链路层以单一或组合形式向LAN提供的安全服务包括：

a) 对等实体认证；
b) 数据来源认证；
c) 接入控制；
d) 连接的保密性；
e) 无连接的保密性；
f) 无恢复的连接完整性；以及
g) 无连接的完整性。

D.2 LAN的安全机制

可按以下方式提供上述安全服务：

a) 可通过加密派生或受保护的认证交换、受保护的密码交换和签名机制的适当组合，提供对等实体认证服务；
b) 可通过加密派生或签名机制提供数据来源认证服务；
c) 可通过适当利用具体的接入控制机制提供接入控制服务；
d) 可通过加密机制提供连接保密性服务；
e) 可通过加密机制提供无连接保密性服务；
f) 可利用数据完整性机制，有时还可结合加密机制提供无恢复的连接完整性服务；以及
g) 可利用数据完整性机制，有时还可结合加密机制提供无连接的完整性服务。

D.3 LAN安全表的修订

表2/X.800尚未得到修订，但能够体现用于以下安全服务的二层（LAN）的图例Y：

- 对等实体认证；
- 数据来源认证；
- 接入控制服务；
- 无恢复的连接完整性；以及
- 无连接的完整性。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况

瑞士印刷
2013年，日内瓦