国 际 电 信 联 盟

ITU-T X.1205

国际电信联盟
电信标准化部门

(04/2008)

X系列：数据网、开放系统通信和安全性

电信安全

网络安全综述

ITU-T X.1205建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	
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	
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	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
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	
组网	X.600-X.629
效率	X.630-X.639
业务质量	X.640-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	
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	
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.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	**X.1000-**

欲了解更详细信息，请查阅 *ITU-T*建议书目录。

ITU-T X.1205建议书

网络安全综述

摘要

ITU-T X.1205建议书提出了对网络安全的定义。本建议书从机构的角度对安全威胁进行了分类，介绍了包括黑客行业最常用工具在内的网络安全威胁和薄弱环节，并探讨了不同网络层存在的威胁。

建议书谈到的化解威胁的各类网络安全技术包括：路由器、防火墙、反病毒防护、入侵检测系统、入侵保护系统、安全计算、审核和监测。建议书研究了深层保护、适用于网络安全的评估管理等网络保护原则，还研讨了风险管理战略和技术，包括培训与教育对网络保护的重要性，同时介绍了利用上述技术保证各类网络安全的示例。

来源

ITU-T 第 17 研究组（2005-2008 年）按照世界电信标准化全会（WTSA）第 1 号决议规定的程序，于 2008 年 4 月 18 日批准了 ITU-T X.1205 建议书。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。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全会（WTSA）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。

WTSA 第 1 号决议规定了批准ITU-T建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

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。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1205建议书

网络安全综述

1 范围

本建议书在第7节提出了有关网络安全的定义。本建议书从机构角度列出了各种安全威胁。

注 – 本建议书中使用的“身份”一词并非指其绝对意义。

本建议第7节研究了企业网络安全环境的性质、网络安全风险和端到端的通信安全。第8节论述了可行的网络保护战略，包括严密的政策管理、统一访问管理以及安全通信技术、灵活多样的管理级别保障管理安全性、分层管理网络安全技术和遭受攻击后的网络生存能力。

附录I研讨了各类安全威胁分类、黑客从业工具以及安全威胁等问题。

附录II对各种网络安全技术做出回顾，包括加密技术、访问控制技术、周边保护技术、防病毒和系统完整性、审核和监测以及管理技术。

附录III列举了网络安全示例，其中包括对远程接入、IP电话、VoIP客户、远端办公室以及无线局域网（WLAN）提供的安全保障。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.800] ITU-T X.800建议书 (1991年), CCITT 应用开放系统互连的安全架构（*Security architecture for Open Systems Interconnection for CCITT applications*）

[ITU-T X.805] ITU-T X.805建议书(2003年), 提供端到端通信的系统的安全架构（*Security architecture for systems providing end-to-end communications*）

[ITU-T X.811] ITU-T X.811建议书(1995年) | ISO/IEC 10181-2:1996, 信息技术－开放系统互连－开放系统的安全框架：认证框架（*Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*）

[ITU-T X.812] ITU-T X.812建议书(1995年) | ISO/IEC 10181-3:1996, 信息技术－开放系统互连－开放系统的安全框架：访问控制框架（*Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*）

[IETF RFC 1918] IETF RFC 1918 (1996年), 专用互连网的地址分配（*Address Allocation for Private Internets*）<http://www.ietf.org/rfc/rfc1918.txt?number=1918>。

[IETF RFC 2396] IETF RFC 2396 (1998 年), 统一资源标识符(URI):通用语法（*Uniform Resource Identifiers (URI): Generic Syntax*）。<http://www.ietf.org/rfc/rfc2396.txt?number=2396>。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语。

3.1.1 本建议书采用[ITU-T X.800］定义的以下术语：

a) 授权；

b) 安全架构；

c) 安全政策;

d) 用户。

3.1.2 本建议书采用［ITU-T X.805]定义的以下术语：

a) 安全维度；

b) 安全服务。

3.1.3 本建议书采用[ITU-T X.811］定义的以下术语：

a) 认证；

b) 原则。

3.1.4 本建议书采用［ITU-T X.81］定义的以下术语：

a) 访问控制信息；

b) 接入；

c) 访问控制；

d) 用户。

3.1.5 本建议书采用[IETF RFC 2396]定义的以下术语：

a) 统一资源标识符（URI）；

b) URI引用。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 **接入点：**IEEE 802.11无线集线器，用作接入点的特种台站（STA）。

3.2.2 **基础服务集（BSS）：**一个接入点（AP）覆盖的服务区域。

3.2.3 **加密算法：**加密算法是改变数据并使之得到加密伪装的方式。

3.2.4 **网络环境：**包括用户、网络、装置、各种软件、程序、存储和传送过程中的信息、应用、服务以及与网络直接或间接连接的系统。

3.2.5 **网络安全：**网络安全涉及用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术。机构和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中全部传送和/或存储的信息。网络安全工作旨在确保防范网络环境中的各种安全风险，实现并维护机构和用户资产的安全特性。网络安全的总体目标包括下列各个方面：

- 可用性
- 完整性（其中可以包括真实性和不可否认性）
- 机密性。

3.2.6 分布式系统：使BSS在ESS中实现互连的非标准化媒质。

3.2.7 扩展认证协议：这一支持补充认证方式的PPP扩展，是[b-IEEE 802.1X]规范的组成部分。

3.2.8 扩展服务集：其BSS置于单一IP子集之中的单一无线LAN。

3.2.9 防火墙：强化两个或更多网络间界线的一个或一组系统。根据本地安全政策对网间接入施加限制的网关。

3.2.10 外地代理：在访问主机网络的同时向移动节点提供服务的被访/主机网络路由器。外地代理负责移动节点和其它节点以及移动归属网络和主机网络之间的隧道与传送。

3.2.11 honeyspot：一种摹仿网络的软件程序，能够吸引（也可能迷惑）入侵者并跟踪他们的行动。这些系统的输出可用于推断入侵者的意图和采集证据。

3.2.12 归属代理：为正在访问其它网络的移动节点提供服务的路由器，并能持续获得关于该移动节点的最新定位信息。

3.2.13 热点：使IEEE 802.11用户能够连接互联网的公共场所。

3.2.14 IP移动性：能为在行进中“访问”不同IP子网的移动节点增加透明连接性的机制。这是一种为有线和无线网络移动节点提供移动管理的机制。

4 缩写

本建议书使用下列缩写：

3DES	三重数据加密标准
AAA	认证、授权和计费
ACL	访问控制清单
AES	高级加密标准
AP	接入点
ASP	应用服务提供商
BSS	基本服务集
CA	证书机构
CMP	证书管理协议
COPS	公共开放政策服务
CRL	证书撤消列表
DISA	直接呼入
DNS	域名系统
EAP	扩展认证协议
EMS	网元管理系统

ESS	扩展服务集
ESSID	服务区标识符
FTP	文件传送协议
HMAC	基于散列函数的消息认证校验
HTTP	超文本传输协议
IDS	入侵检测系统
IKE	互联网密钥交换协议
IP	互联网协议
IPSec	互联网系安全
ISP	互联网服务提供商
L2TP	第二层隧道协议
LAN	局域网
MAC	消息认证码
MD5	信息摘要算法 5
MIC	消息完整性检测
MIME	多用途互联网邮件扩展
MPLS	多协议标记交换
MU	移动单元
NAT	网络地址转换
NGN	下一代网络
NIC	网络接口卡
NOC	网络操作中心
OAM&P	运营、管理、维护和配置
OCSP	在线证书状态协议
OS	操作系统
OSI	开放系统互连
PDP	决策点
PEAP	受保护的扩展认证协议
PEP	策略执行点
PGP	相当好的隐私（一种软件加密程序）
PKI	公共密钥基础设施
PKIX	公共密钥基础设施X.509
PoP	持有辨认法
PPP	点到点协议
PSTN	公共电话交换网
RADIUS	远程用户拨号认证系统
RSA	Rivest Shamir Adleman 公共密钥算法

SHA-1	安全散列算法1
SIP	会话发起协议
SMTP	简单邮件传输协议
SNMP	简单网络管理协议
SP	服务提供商
SSH	安全壳
SSID	服务区标识符
SSO	单点登录
TKIP	动态密钥完整性协议
TLS	传输层安全协议
UE	用户设备
URI	通用资源标识符
UTC	协调世界时
VAR	增值转销商
VLAN	虚拟局域网
VoIP	IP语音
VPLS	虚拟专用局域网业务
VPN	虚拟专用网
VPWS	虚拟专用线路业务
WAN	宽域网
WEP	有线等效加密
WLAN	无线局域网
WPA	Wi-fi保护接入
XML	可扩展标记语言

5 常用语

本建议书所述的用户设备（UE）为广义的、在用户所在地和往往无法由运营商或服务提供商控制的用户设备，包括各种装置、（基于硬件或软件的）实体、移动和/或静态装置、个人计算机（PC）、（多媒体推动的）终端、电话等等。

6 引言

利用网络连接异构IT系统可以给机构带来生产力增益，并使它们掌握联网系统赋予的新的能力。如今人们能够比较轻松地远距离获取信息、相互交流并监控IT系统。因此，现今的网络在许多国家的电子商务、语音和数据通信、公用事业、金融、医疗、运输和防务等关键基础设施中发挥着重大作用。

网络的连接和普遍接入对于今天的IT系统至关重要。然而互连的IT系统接入普及但结合松散，这可能是造成隐患普遍存在的罪魁祸首。诸如拒绝服务攻击、盗窃金融和个人数据、网络失效和语音及数据通信业务中断等针对联网系统的威胁，正在与日俱增。

今天使用的网络协议是在互信的氛围中制定的，多数新的投资与研发工作致力于新功能的创建而不是强化其安全。

网络安全威胁正在迅速蔓延，病毒、蠕虫、特洛伊木马、电子欺骗攻击、“身份盗窃”[1]、垃圾邮件和网络攻击也愈演愈烈。必须了解网络安全问题，才能为促进未来网络的安全奠定知识基础。

鼓励公司和政府机构将安全视为一种寻求系统、网络、应用和资源保护方式的思维过程与方式。这种思维的依据是连接网络具有与生俱来的风险。然而，安全不应成为经营的障碍，其目标是如何以安全的方式提供所需的服务。

在当今的商业环境中，周边的概念正在淡出。网络内部与外部之间的界限也正在淡化。应用在网络上分层运行，而人们设想层与层之间存在安全保障。分层的安全解决办法能够使机构对威胁层层设防。

7 网络安全

鼓励机构制定满足其安全需求的全面规划，并应将安全视为一种寻求系统、网络、应用和资源保护方式的思维过程与方式。

7.1 什么是网络安全？

本建议书第3.2.4段对网络安全这一术语做了定义。

网络安全技术可用于确保系统的可用性、完整性、真实性、机密性和不可否认性。网络安全可用于确保用户的隐私得到尊重，而网络安全技术可用于确定用户的可信度。

无线网络和IP语音（VoIP）等技术可扩大互联网的覆盖与规模。与此相关的网络环境包括用户、互联网、与之相连的计算设备和所有应用、服务以及与互联网和下一代网络（NGN）环境（后者即具公众亦具专用特征）直接或间接连接的系统。因此，采用VoIP技术的台式电话机便成为网络环境的一部分。然而只要独立设备能够通过可移动媒介与联网的计算设备共享信息，它们也能成为网络环境的组成部分。

网络环境包括在计算设备上运行的软件、在这些设备上存储（以及传送）的信息或这些设备生成的信息。容纳这些设备的设施和建筑也是网络环境的一部分。网络安全必须将这些因素考虑在内。

---

1 “身份盗窃”一词仅系指未经授权即对特定识别码和其它信息（二者共同构成特定用户的身份特征）进行使用的情况。身份盗窃与通常的盗窃（目标物体真正从受害人处移走）不同，通常涉及收集或复制有关身份的细节（而合法拥有人可能对盗窃行为毫无察觉）。

网络安全的目的在于保证网络环境的安全，是一种众多公共和私营机构的利益攸关方均可参与的系统，并为了安全采用多种组件和不同方式。因此，可以从以下的角度理解网络安全：

– 可用于保护互联网络（包括计算机、设备、硬件、存储信息和经转信息）免受未经授权的访问、篡改、盗窃、中断或其它威胁的一系列策略和行动。
– 对上述策略和行动进行持续的评估和监测，以便在威胁性质不断演变情况下维持安全质量。

国际电联[b-ITU-T Y. 2201]提出了可用以加强NGN网络安全的要求。该工作要求通过对装置和用户的单独认证予以配合。下一代网络多因素双边认证配合逐项服务授权将降低针对用户的攻击的风险。

7.2 企业网络安全环境的性质

机构需要为满足其安全需求制定一项综合计划。安全不是通用万能的（见[b-ITU-T Y.805]），是不能通过一套互连模块实现的。鼓励机构将安全视为一种寻求系统、网络、应用和网络服务保护方式的思维过程与方式。

安全必须贯穿所有网络层面。采用的分层安全措施一旦与有力的策略管理和实施相结合，便形成可供安全专业人员选择的模块化、灵活和可伸缩的安全解决方案。

安全是难以测试、预测和实施的，不可能对所有情况采取“一刀切”的解决办法。每个机构的安全需求和得到的安全战略建议都具有独特性和差异性。例如，每个企业、电信服务提供商、网络运营商或服务提供商都有一套独特的商业需求，并为满足这些需求而逐步形成了自己的网络环境。

例如，“封闭企业”在站址之间采用逻辑（即帧中继）或物理专线，为需要访问互联网的雇员有选择地提供远程接入，并通过（负责建立一种安全环境的）服务提供商提供的互联网数据中心实现在线状态。该机构还为（在旅馆工作的）远端雇员提供常规拨号接入。公司在雇员当中采用无外部接入的专用电子邮件以及无线局域网。

“扩展企业”或电信服务提供商、网络运营商或服务提供商可通过互联网的IP VPN给予远端雇员和办公室接入支持，提供高速和低成本的连接。包括提供通用互联网接入（如提供可与外部世界互通的内部电子邮件系统）。

“开放企业”的业务模式通过允许合作伙伴、提供商和客户访问企业管理的互联网数据中心，甚至允许有选择的访问内部数据库和应用（如供应链管理系统的一部分），使互联网得到利用。内部和外部用户可利用有线或移动装置，从家中、远端办公室或其它网络接入企业网，但这类企业的安全要求不同于其它企业。

图7-1是企业类型的综合图示。

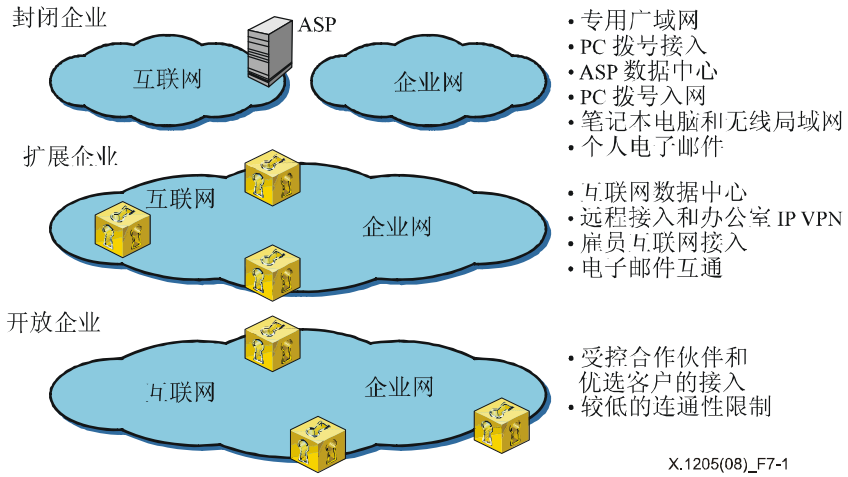


图7-1 – 通用的企业类型

网络安全需要风险管理。这一程序包括确定一系列需要保护的组件。为便于风险分析工作，有必要考虑将攻击分为以下类型：

1) 服务中断攻击：这类攻击可暂时或永久地使用户对目标服务的访问陷于瘫痪。其实例包括无法接入网址，或无法从事金融交易或发起语音呼叫。一些类型的攻击可导致业务中断。例如，拒绝服务（DoS）、分布式拒绝服务攻击（DDoS），或对关键基础设施所在建筑的破坏可使用户无法接入服务。

2) 资产破坏。这类攻击包括对基础设施的盗窃和滥用。大规模的此类攻击会影响网络安全。

3) 组件劫持。这类攻击包括控制某些设备，并利用它们对网络环境的其它成份发起新的攻击。

网络环境的任何部分都可被视为安全风险，而这种风险通常被认为是综合威胁评估的结果。威胁分析包括描述可能发起的攻击的类型、潜在的攻击者及其攻击方式以及攻击得逞造成的后果。另一方面，本建议书提到的薄弱环节是指攻击者可以利用的弱点。将风险评估与威胁分析相结合，可使机构对其网络可能面临的风险作出评估。

攻击可能自网络环境发动，例如通过蠕虫病毒或其它恶意软件直接攻击电信管线等重要基础设施，也可能通过获得信任的内部人员内应发起。还有可能出现组合式攻击。风险通常分为高、中、低三种类型。风险程度又因网络环境成份的不同而有所差异。

安全完全是以风险管理为目的。可采用多种技术进行风险管理。例如，可以采用制定防范战略方式，针对可能出现的攻击制定对策；检测包括发现实施中或已完成的攻击；针对攻击制定的对策，具体提出了阻止攻击或减轻其影响的一系列应对措施；制定恢复战略可使网络从已知状态恢复运行。

7.3 网络威胁和应对方法

ITU-T X.800 建议书认为，对数据通信系统的威胁包括以下内容：

a) 破坏信息和/或其它资源；

b) 毁损或修改信息；

c) 信息和/或其它资源的盗窃、删除或丢失；

d) 信息披露；以及

e) 服务中断。

根据[ITU-T X.800]，威胁既可分为意外或有意类型，也可分为主动或被动类型。意外威胁属无预谋的威胁。发生意外威胁的实例包括系统故障、操作失误和软件缺陷。有意威胁可能包括采用易于得到的监测工具进行漫不经心的检查，以及利用专业系统知识进行的复杂攻击。有意威胁一旦得手，便可被视为一次"攻击"。成功实施的被动威胁不会导致对系统内存信息的任何修改，也不会改变系统的运行和状态。利用被动线路窃听监测通信线路传输的信息，便是实现被动威胁的行动。对系统的主动威胁涉及篡改系统内存信息，或改变系统的状态和运行。未经授权的用户恶意修改系统的路由表，便是主动威胁的实例。附录I简要介绍了这样一些具体类型的攻击。

X.800述及的安全风险同样存在于网络环境，根据[ITU-T X.800]，安全特性通常会提高系统成本，并增加其使用难度。因此在设计安全系统之前，最好明确需要防范的具体威胁。这就是众所周知的威胁评估。一个系统存在许多薄弱环节，但会被利用的只是其中的一部分，其原因或许是攻击者无从下手，或许这样做的结果不值得花费精力和冒被发现的风险。虽然详细的威胁评估问题超出了本建议书的范围，但它们大体包括：

威胁是针对资产的威胁，因此首要步骤是列出需要得到保护的资产。评估工作的下一步是对威胁做出分析，然后分析脆弱环节（包括影响评估）并采取对策和安全机制。

a) 确定系统的薄弱环节；

b) 分析利用这些隐患造成威胁的可能性；

c) 逐一评估可能得手的威胁的影响；

d) 估算每次攻击的成本；

e) 计算出潜在对策的成本；以及

f) （或许采用成本效益分析法）选用合理的安全机制。

在某些情况下，保险理赔等非技术措施可能是较技术安全措施更具成本效益的选择。一般来说，万无一失的技术安全是不存在。因此，我们的目标应该是大幅度提高攻击成本，使风险降至可接受的程度。

7.4 端到端的通信安全

[ITU-T X.805]为解决端到端的网络安全问题确定了一种网络安全框架。[ITU-T X.805]适用于其端到端安全受到关注的各类网络。该框架独立于网络支撑技术。

安全架构可全面应对服务提供商、企业和用户的安全挑战，并适用于无线、光纤和有线语音、数据及融合网络。它可消除管理、控制和使用网络基础设施、服务及应用方面的安全担忧。［ITU-T X.805]有助于主动发现和克服安全隐患。该安全架构可将一套复杂的端到端网络安全特性逻辑地划分为独立的架构组件。这一划分为形成系统的端到端的安全方法留出了余地，可用于制定新的安全解决方案和评估现有网络的安全性。

[ITU-T X.805]所说的安全维度，系一组旨在解决某一具体网络安全问题的安全措施。[ITU-T X.805]提出的防范所有重大安全威胁的八个维度，突破了网络的局限，扩展到应用和最终用户信息领域，并适用于服务提供商或向其客户提供安全服务的企业。这些方面包括：

1) 访问控制；

2) 认证；

3) 不可否认性；

4) 数据机密性；

5) 通信安全；

6) 数据完整性；

7) 可用性；以及

8) 隐私保护。

为提供端到端的安全解决方案，必须将安全维度用于分层的网络设备和设施群组，即所谓安全分层结构。建议书涉及了以下三个安全层面：

1) 基础设施安全层；

2) 服务安全层；和

3) 应用安全层。

安全各层通过提供顺序网络安全法，确定了那些安全问题必须在产品和解决方案中得到解决。例如要首先解决基础设施层的安全隐患，然后是业务层的隐患，最后解决应用层隐患。图7.4-1描述了安全维度用于安全分层以减少各层安全隐患的方式。

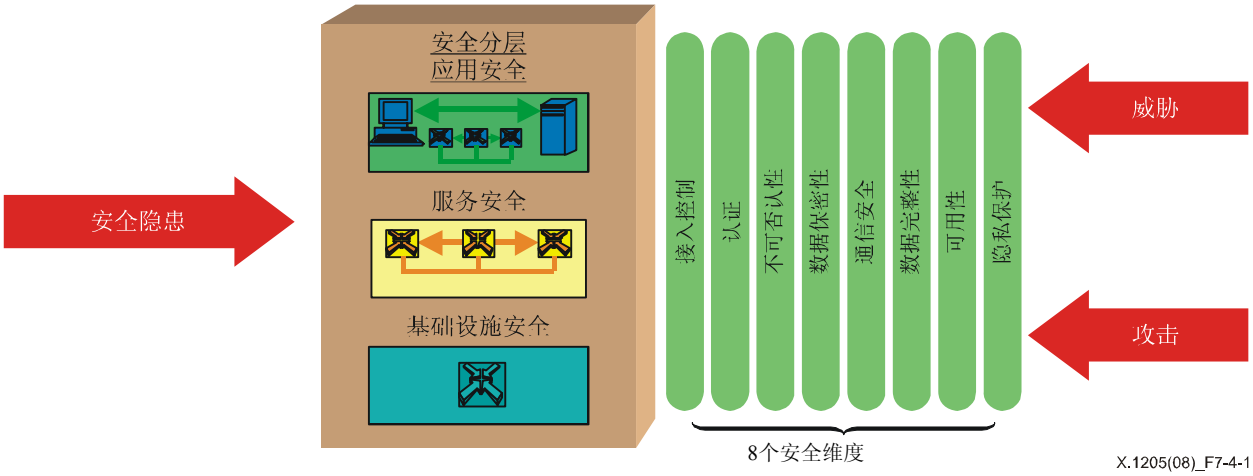


图7-4.1 – 将安全维度用于各安全层面

[ITU-T X.805]介绍的安全平面，是受网络维度保护的某一类网络活动。[ITU-T X.805]定义了代表网上出现的三类受保护活动的以下三个平面：

1) 管理平面；

2) 控制平面；以及

3) 最终用户平面。

上述安全平面满足的具体安全需求分别涉及网络管理活动、网络控制或信令活动以及最终用户活动。[ITU-T X.805]提议，网络的设计应能使各网络平面的事件相互隔离。例如，应最终用户请求发起的充斥最终用户平面的查询信息，不应将管理平面的OAM&P接口拒之门外，使管理者无法对问题采取纠正措施。

图7.4-2显示了包括安全平面的安全架构。安全平面概念能够对与这些活动相关的具体安全问题进行区分，并能够独立的解决这些问题。以业务安全层负责解决的VoIP为例，保证业务管理安全的任务应独立于保证业务控制安全的任务。这项任务独立于向业务（如用户语音）传送的最终用户数据提供安全保障的任务。

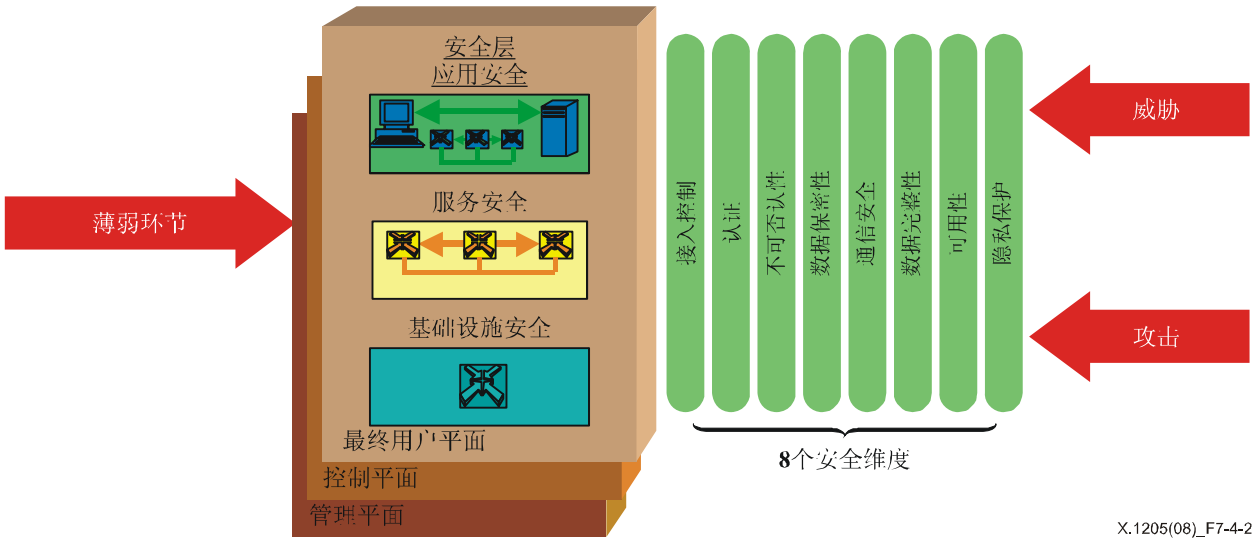


图7-4.2 – 安全平面反映了不同类型的网络活动

8 可行的网络保护战略

安全涉及网络体系结构的各个层面。本方法构成设计安全网络的良好开端。对网络进行分解，可以使更高层网络根据自身需要确定自己的安全要求，并方便使用较低层的安全服务。采用分层的网络安全方式，人们可以为各机构灵活制定网络层、应用层和管理层的、规模变化自如的安全解决方案。

8.1 严密的政策管理

设计合理和实施得当的安全政策对各类企业和机构均必不可少。安全政策应机动灵活，不断得到加强、落实和完善，反映企业或机构在基础设施和服务需求方面的最新变化。

安全政策必须明确无误地确定机构（及企业）资源面临何种风险，应如何化解这些风险。安全政策必须对有关脆弱性和风险评估的工作做出规定，并明确应采取哪些恰如其分的访问控制规则。必须对网络的各个层面进行风险和脆弱性评估。同时，安全政策还必须有助于确定和发现违反安全规定的行为，阐明相应对策。

我们建议IT管理员使用黑客所用的工具对网络脆弱性做出评估。同时必须采用最小特权访问原则，确保对审核跟踪工作进行审议，做到政策管理无懈可击。IT管理员如在审核中发现问题，则应确保对政策进行更新，以反映最新情况。

止步于纸上谈兵的安全政策毫无价值，但安全政策的落实却与人休戚相关。应当在各方之间很好地分清执行政策的职责和责任。

8.2 统一访问管理

访问管理一词用以定义为控制资源使用而既可以使用认证服务、也可以使用授权服务的系统。认证是一种程序，用户通过该程序申请建立针对某一网络的身份。授权则根据访问控制机制确定该身份用户所拥有的特权级别。确定和执行访问控制政策是访问级别控制的基础。图8-2具体显示安全认证和授权参考模型应采用的参考模型。

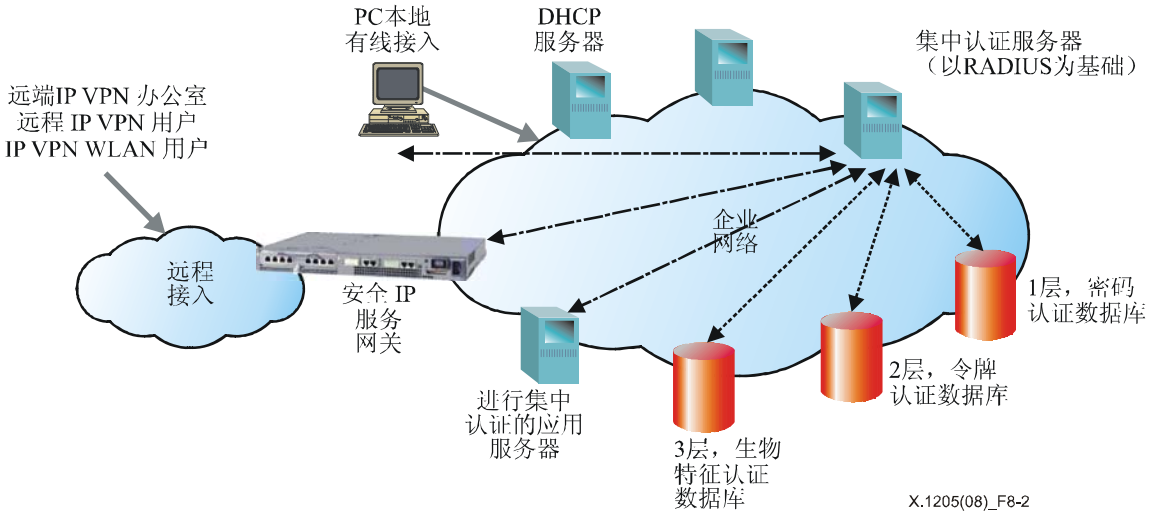


图8-2 – 安全认证和授权参考模型

从图8-2中可以看出，应采用下列建议：

1) 使用集中式认证机制，以方便管理，取消局部存储的密码的使用（局部存储的密码往往静止不变，功能很弱）。

2) 使用集中式授权系统，并与认证系统密切配合，同时根据特定企业的需要，实现适当的层次变化。

3) 对各种密码均采用严格（复杂）的密码规则。

4) 以单向加密（散列）形式安全地存储各种密码。

5) 简单即意味着方便使用和易于管理。系统简单就会安全，因为（复杂系统的）保障措施很可能引人注目。

6) 有关安全事件的认证和授权记录万无一失。

访问管理方式多种多样，其中包括：IP源过滤，代理和基于证书的技术。每一种方法均利弊兼具。根据企业类型，可能需要在安全方面采用多种不同方式或多种方式合并一体的举措。例如，一家企业可能通过IP源过滤，管理对工作站的访问，同时采用基于证书的手段管理其它用户。

可采用若干方法进行用户认证，具体技术包括：密码、一次性密码认证、生物特征技术、智能卡和证书。依靠密码进行的认证必须使用强密码（strong password），密码长度至少为八个字符，其中至少包括一个字母、一个数字和一个特殊字符。仅仅采用密码认证可能无法满足安全需求，因此，根据对网络脆弱性的评估，可能需要采用密码认证与其它认证和授权手段并举的方式，后者包括证书、轻量级目录访问协议（LDAP）、远程用户拨号认证系统（RADIUS）、网络认证协议（Kerberos）和公共密钥基础设施（PKI）。

所有认证机制均优缺点兼具。虽然用户身份（ID）/密码组合方式简单、成本低廉和易于管理，但牢记大量复杂的密码却是用户的一大难题。双因素和三因素身份认证系统虽然增加了认证力度;但却成本昂贵、更为复杂，并难以保持。

企业认证和授权的较好解决方案是采用由强密码组成的“单一密码”系统。此类系统保障认证安全性高、实现逐级授权且易于管理。在这一系统中，用户的单一强密码与企业内诸多认证和授权应用及系统得到同步使用。企业所有系统和应用均自动将认证和授权功能转向单一密码系统。此时用户仅需要牢记一个强密码，因此系统使用简单，用户难以置系统于不顾。单一密码系统的优点包括：

- 以统一一致的方法建立密码。
- 以统一一致的方法做出认证和授权。
- 以统一的方法注册和结束用户账户。
- 执行企业的密码优势导则。
- 连贯一致 – 客户了解如何行事。
- 标准化 – 易于支持和采用。
- 快捷方便 – 标准的界面和应用程序接口（API）。
- 成本低廉，寻求帮助的呼叫数量下降。

开放式和大型企业在构思访问管理政策时面临的挑战最为艰巨。访问管理必须构成安全政策的组成部分。企业和机构必须设计统一的访问管理系统，并细化与下列方面顺利接轨的相关规则：

- 身份属性目录和数据库
- 多重认证系统，如密码、Kerberos、TACACS 和 RADIUS
- 主机、应用和应用服务器

统一访问管理系统应在对每一个用户进行认证后实行会话管理。我们建议不仅实现灵活配置，而且应以针对具体对象的、得到细化的规则配合政策的执行。应当进行适当的监督、记账并确保审核跟踪。建议为每一个管理员设立独特的账户，明确其责任，并将每项行动均与个人挂钩。

8.3 安全通信

综合统一的网络能够传输语音、数据和视频。保障网络流量的安全就必须保障网络通信的机密性、完整性和准确性。应当为电话网的呼叫和信令话务提供安全性。必须在数据、语音和移动网上使用加密技术。

加密方式多种多样：

- 使用IPSec的虚拟专用网（VPN）技术，包括认证报头（AH）、封装安全有效荷载（ESP）或使用第2层隧道协议（L2TP）的隧道技术。
- 基于互联网密钥交换（IKE）的密钥管理。
- 基于公钥基础设施X.509（PKIX）的证书管理。

- 证书管理协议（CMP）（见[b-IETF RFC 2510]）和在线证书状态协议（OCSP）（见[b-IETF RFC 4557]）。
- 在应用层使用传输层，通过安全协议（TLS）（见[b-IETF RFC 4366]）与强密钥并举的方式。

使用基于标准的加密算法和散列技术（包括DES、3DES、AES、RSA和DSA（见[b-IETF RFC 2828]）十分重要。MD5（见[b-IETF RFC 1321]）和SHA-1（见[b-IETF RFC 3174]）可用于保证信息完整性，并采用Diffie-Hellman（见[b-IETF RFC 2631]）和RSA（见[b-IETF RFC 2828]）进行密钥交换。

注 – NIST（国家标准和技术学会）目前鼓励采用SHA-256（带有256比特加密密钥的安全散列算法）而非SHA-1。

[b-IEEE 802.11]标准定义的有线等效加密（WEP）协议确定了保护无线局域网（WLAN）接入点和网络接口卡（NIC）之间空中传输的技术。事实表明，该协议并不安全。人们必须采用IPSec等更多保护措施才能够保障WEP之上WLAN的安全。另一种方法是采用Wi-Fi保护接入（WPA）来加强保护。

8.4 灵活多样的安全级别

VLAN是一套包括服务器和其它网络资源的网络装置，其配置方法使其如同连接于一个网部分一样工作。VLAN中其它用户的资源和服务器不会被VLAN的其它成员看到。VLAN更有效地分割网络，从而提高绩效。VLAN限制广播和节点到节点的流量，从而减轻网络的整体流量负担。VLAN间的数据包可通过路由器传送，因此有助于实施基于路由器的安全措施，限制对该网络部分的接入。

分层开展安全工作有助于人们提供灵活多样的安全级别。每增加一级，均是对较低层次能力的扩充；每增加一级，均会使安全工作细化又细化。

例如，可以采用虚拟局域网（VLAN）对基本网络进行条块分割，将不同业务功能局限在自有的专用局域网范围之内，严格控制或禁止来自其它VLAN的流量。中小型企业在其各分支所在地部署VLAN益处颇多。使用VLAN“标签”（tag）可将流量按财务、人力资源和工程进行归类集中。在安全方面，必须实现VLAN之间无“泄露”的数据分离。

通过在网络战略点上采用边界和分布式防火墙过滤手段可以实现第二层次的安全性。加入防火墙可以将网络进一步分割为更小的区域，从而确保与公众网之间连接的安全性。防火墙将对来向和去向流量的访问局限于在防火墙内明确得到配置的协议。此外，防火墙还可以对出网和入网用户进行认证。支持网络地址转换（NAT）的防火墙能够最佳实现[IETF RFC 1918]规定的网络内IP寻址（专用互联网地址分配）。

防火墙为访问控制提供了十分有益的额外层次的保护。实施基于政策的访问可以根据业务需要为客户量身定制访问计划。而采用分布式防火墙方式则有助于企业按照需要逐步对安全解决方案加以扩充。可以在端点系统上部署个人防火墙，确保应用的完整性。

通过增加3层VPN可以实现第三层次的安全性。VPN提供更加细化的用户访问控制机制，并使该项工作更加人性化。VPN将安全工作细化到每个用户个人，因此确保远端地点和业务合作伙伴进行安全的远程访问。采用VPN后，不再需要专用线路。利用安全隧道在互联网上进行动态路由可以保障极高的安全性、可靠性和可扩展性。VPN与VLAN和防火墙并举

的方式可以方便网络管理员将用户或用户组的访问限于政策标准和业务需求决定的范围。VPN能够更有力地保证数据的完整性和机密性。为确保机密性和数据完整性，可以在该层完成强大的数据加密功能。

分层的安全解决方案不仅灵活，而且规模上变化自如。该解决方案易于调整使用，满足企业的网络安全需求。

8.5 保障管理安全性

安全的管理渠道或平台必须构成网络管理、性能和生存能力方面所有其它工作的基础，无论它是否构成机构或企业的“最佳做法”，或安全体系结构不可或缺的部分与否。显而易见，该基础对各类企业均至关重要，因为即使封闭企业目前也正在随着时间的推移，而逐步变为大型或开放企业。图8-5提出了保障网络操作中心（NOC）网络管理安全的可能的参考模型。

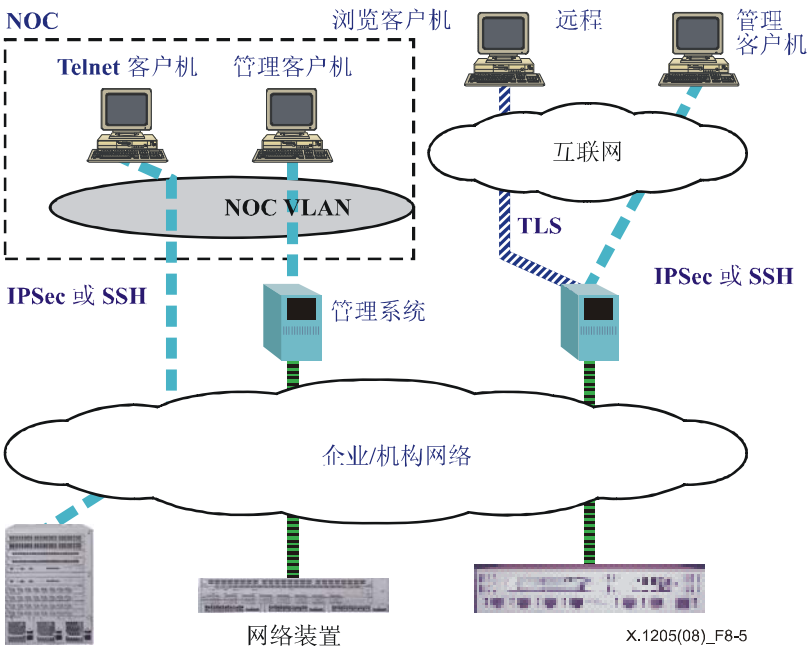


图 8-5 – 保障管理安全性的参考模型

安全管理是一项整体性的综合措施，而非某一特定网元的具体安全功能特性。为此，本建议书推荐的方式涵盖网络基础设施的各关键部分，并具体说明应采取何种行动来减少网络的潜在威胁。下述每一个领域均至关重要，需要人们在安全性方面给予高度关注，以确保对网络进行和谐一致的保护。

在确定网络管理平台安全之前应检验九个重要网络管理的领域，即：

- 活动记录万无一失
- 网络操作员认证
- 网络操作员访问控制
- 网络管理流量加密
- 保障操作员远程访问的安全性
- 防火墙

- 入侵发现
- 增强操作系统
- 无病毒软件

8.5.1 政策管理

安全记录旨在跟踪用户或管理员从事的活动和装置产生的事件，是严密的政策管理的关键一环。所收集的原始数据被称作“审核日志（audit log）”，而通过该日志对事件进行核证的途径被称作“审核跟踪（audit trail）”。有效的审核日志必须充分包含有关安全事件事后调查或分析的详细信息。审核日志是实现若干安全目标的手段，包括个人责任、重建已过事件、发现入侵和对问题进行分析。还可利用日志对长期趋势做出分析。日志中的信息有助于人们对安全问题追根溯源，并在未来做到防患于未然。应安全存储这些信息。此外，审核日志还可用于重建导致一系列问题发生的事件，包括入侵者对系统资源进行的非授权访问，或错误配置或实施不当导致的系统失常。

8.5.2 安全的访问管理

必须在强有力的、网络操作员和管理员集中认证基础上对网络操作员进行认证。集中管理密码有助于充分发挥密码的优势，避免在网元和EMS系统上对密码进行局部存储。RADIUS是实现集中式自动认证的基本机制。

应当对网络操作员实行良好的访问控制。例如，为确定授权等级，可以采用基于RADIUS服务器的技术提供基本的访问控制；而通过增加LDAP服务器，则可以在必要时提供更加细化的访问控制。

8.5.3 网络管理流量的加密

我们建议对所有网络管理数据流量进行加密，确保数据的机密性和完整性。企业使用带内（in-band）网络管理的情况日益增多，因此非常需要通过加密手段将管理流量予以分离。对管理流量进行加密可以在很大程度上防止内部作案，只有少数合法掌握加密密钥的内部人员除外。应当在网络操作中心（NOC）客户机和网元管理系统（EMS）服务器和/或网元之间提供加密，包括SNMP流量，因为SNMP v1和v2存在的脆弱性人所共知（这些问题在SNMP v3中已得到解决）。根据不同类型的流量，我们可以在链路上使用TLS、IPSec和安全壳（SSH）等安全协议（见[b-IETF RFC 4252]）。SSH是应用层安全协议，直接取代Telnet（见[b-IETF RFC 854]）和FTP（见[b-IETF RFC 959]），但通常无法用以保护其它类型的流量。另一方面而言，IPSec协议仅仅在网络层（3层）和传送层（4层）之间运行，因此无论使用何种应用和协议，均可以对各类数据流量进行保护。IPSec是优选方法，但是如果流量仅包括Telenet和FTP，则可以使用SSH。如果在NOC客户机和EMS和/或网元之间的网络管理中存在HTTP流量，则必须通过TLS技术对其加以保护。为确保管理流量的安全性，可以在网络的各个部分使用外部IPSec VPN装置。

8.5.4 操作员进行安全的远程访问

如果操作员或管理员通过公众网络从远端地点对网络进行管理，则必须保障其工作的安全性。可取的解决方案是利用IPSec提供安全的虚拟专用网，因为该手段可以对所有远端操作员进行强有力的加密和认证。应将VPN产品置于管理系统的接口处，而且所有操作员均应在其笔记本计算机或工作站上配备外联网访问客户机。

8.5.5 防火墙

使用虚拟局域网（VLAN）和防火墙等不同安全级别原则对网络管理环境进行分割，是一项良好的做法。防火墙控制着流经不同安全领域边界的流量的类型（协议、端口号码、来源和目的地地址）。根据不同类型的防火墙（应用与数据包过滤），我们也可以将此扩大，使其对数据流应用内容亦进行过滤。应根据具体的网络实施情况来确定防火墙的位置、类型和过滤规则。

8.5.6 入侵发现

可以将基于主机的入侵发现系统纳入管理服务器，从而保护网络免受入侵干扰。可以通过入侵发现系统向网络管理员发出警报，提醒他们可能出现安全事件，如服务器损坏或拒绝服务攻击。

8.5.7 应用安全层

建议增强网络管理工作采用的所有操作系统的功能，不论其为通用系统还是内置的实时系统，用于网络管理能力的所有操作系统均应得到增强。如果没有操作系统具体的增强指南，应与操作系统制造商取得联系，以获得最新的增强补丁和程序。

8.5.8 无病毒软件

必须对所有由内部开发或从第三方购买的软件进行检查，尽可能保证使用无病毒软件。必须制定有关检查病毒是否存在的程序，在将软件纳入产品之前，利用具体的病毒检查工具对所有软件进行扫描。

8.6 跨应用、网络和网络管理的分层安全性

每一个机构或企业均有自己的、与众不同的最低安全标准和技术基础设施。通过互联网的应用给企业带来了更多的风险和威胁，因此互联网应用必须在应用层具有内置安全保障。然而，采用可由低层网络提供的安全功能则能够加强应用的安全性。

使用互联网的企业在设计网站时必须极为谨慎小心。[b-IETF RFC 2196]（网站安全手册）阐述网站安全问题，是此项工作很好的参考手册。建议在应用层实施细化的安全政策，各对象的地址应在统一资源标志符（URI）层获得。应关闭所有不必要的功能。必须使用TLS。同时建议使用应用层网关，并重点加强认证和授权工作。应通过S/MIME（见[b-IETF RFC 2311]）和PGP（见[b- IETF RFC 1991］）等技术保障电子邮件服务的安全性。

在网络层，必须使用第8.7节讨论的技术来确保企业实现令人接受的安全性。对于各类型的企业而言，均存在针对每一项安全要求而量身订做的分层体系结构，可以通过采用这一体系结构实现企业的安全性。

在保障网络安全性方面，确保网络管理流量的安全性至关重要。为实现这一目标，我们首先需要确保增强操作系统的功能，使其在人所共知的威胁面前坚而不摧。应与操作系统制造商取得联系，以获得最新的增强操作系统的补丁和程序。与此同时，必须采取有效步骤，确保所安装的各种软件均不受任何病毒的侵扰。无论何时，均采用IPSec对所有管理流量进行加密，或采用TLS来保护HTTP流量。如果流量流向本地局域网之外，则必须对流量予以加密。建议通过SNMPv3和RADIUS实现网络操作员的远程访问控制，同时合并采用多层次控制机制，包括强密码，并最好配备集中式管理员访问控制系统。安全日志对于记录网络管理流量必不可少。

8.7 网络遭遇攻击时的生存能力

在当今环境中，企业的网络支持着企业开展各项关键业务，是企业开展业务不可或缺的手段。因此，必须随时保障业务伙伴网络的安全性、可靠性和可用性。

保障网络可靠性的方式多种多样，同时网络可靠性确保在软件和/或硬件发生故障时，网络继续正常工作。然而，在出现安全威胁时，必须采用网络生存能力概念。具有生存能力的网络系指在出现攻击时，网络能够继续及时发挥最低限度和不可或缺的功能性。这些功能性包括，即使由于攻击，网络某些部分已无法通达或出现故障，但依然有能力及时提供最基本的服务。

设计具有生存能力网络的第一步，是须将网络服务按基本服务和非基本服务两个类别加以机构。生存能力要求网络具有抵抗攻击的能力，因此必须就如何处理攻击和在攻击出现后进行的恢复工作制定明确的战略。根据攻击的类型，网络管理员应当考虑制定若干有关抵抗攻击、确定攻击和在攻击之后进行恢复的战略。具有生存能力的网络的特点之一是易于调整。例如，如果在网络的第一个服务器上发现入侵攻击，网络可以将流量从该服务器倒换至另一个服务器。

必须在设计网络安全政策阶段确定网络在遇到攻击时应能够提供的基本服务。该阶段，确定网络如何抵抗攻击，如何克服这一问题，以及如何以最佳方式实现攻击后的恢复。分析过程中，应当对管理系统、主机、应用、路由器和交换机加以考虑。

采用访问控制机制和功能强大的认证和加密手段，可以提高具有生存能力的网络对抗攻击的能力。对信息和数据包进行过滤并对网络和服务器实行条块分割同样可以提高网络对抗攻击的能力。此外，适当采用入侵发现技术可以帮助人们确定攻击。在进行系统和网络恢复工作中，我们可以适当采用备份技术。

附录I

攻击者采用的技术

（本附录不构成本建议书不可分割的一部分）

本附录简要阐述在数据处理和数据通信环境中尤应关注的某些攻击行为。

I.1 安全威胁分类

建议专业人员将其网络看作一种通常由无法得到信任的用户进行访问的资源。攻击者可以利用诸多工具、技术和方法损坏网络。黑客为访问网络会利用这些工具发起多重攻击。有些情况下，攻击者会充分利用安全工作的漏洞，通过再次攻击损坏网络的其它部分。

本节旨在阐述攻击者、黑客和入侵者用以破坏网络的技术、工具和方法。

I.1.1 授权威胁

未经授权即获得网络资源访问权往往由于系统配置不当或使用错误而产生。攻击者可以充分利用不尽如人意的企业系统用户和任务的认证或授权，或雇员的不良做法（如，当用户被迫牢记多个密码时，对密码进行公布），非法访问网络。

不恰当地分配隐蔽空间和在应用之间共享特权等会带来严重的安全隐患。攻击者可以利用陷门攻击非法进入网络。例如，攻击者可以使用常见字符串字典对用户名和密码进行猜测，实现对网络的非法访问。攻击者也可以通过算法生成密码。如果以明码形式传送密码，则密码可能被人截获。

攻击者在猜到用户名和相关密码之后，则能够获得机构的资源，其程度取决于被破坏账户所拥有的特权。攻击者对机构造成的破坏程度亦由其意图决定。多数情况下，黑客会利用遭损坏的账户安装进入企业网的后门。

用于远程访问电子邮件的协议（如互联网邮件访问协议（IMAP）、POP3和POP2）使用简单的用户名和密码认证技术，为暴力攻击带来可乘之机。目前已公布的一些手段都有助于攻击者以远程方式利用这些协议提供的服务。

在获得未经授权的网络访问方面，还存在更加先进复杂的方法。攻击者可以利用蠕虫进行系统欺骗，即，系统某一部分假扮为另一部分。例如，蠕虫可以利用发送邮件（sendmail）和in. rhosts（UNIX系统使用）中很弱的认证功能，享用调试数据流。可以关闭发送邮件的可选调试程序，保持该程序开的状态是一种使用缺陷。

I.1.2 IP 欺骗

IP欺骗是利用信任关系的一种非常复杂的攻击行为。攻击者对值得信赖的主机身份做出假设，以破坏该目标主机的安全。就目标主机而言，它认为自己在与一个值得信赖的主机进行对话。

在这种攻击中，攻击者首先确定一台身份将得到假设的值得信赖的主机。首先，攻击者确定主机的信赖规律（该工作通常要求确定该主机信任的一系列IP地址）。其次，使主机停止运转，方便攻击者对其身份进行假设。可以通过使用TCP SYC泛洪攻击技术实现这一目标。

IP欺骗攻击之所以能够得逞，是因为IP地址易于仿冒，且基于网络的地址认证技术局限重重。IP欺骗攻击漫无目的，攻击者可能并不能得到目标主机的回应。但是，如果对路由表进行操纵，使用由欺骗得来的IP地址源，则攻击者可以获得双向通信的权利。IP欺骗攻击往往是攻击者实施诸如拒绝服务（DoS）和泛洪攻击等的第一个步骤。

应当指出，多数（当然并非所有）互联网服务提供商和诸多反应迅捷的企业网络目前都在进行去向流量地址过滤，从而限制了肆无忌惮的IP欺骗攻击。针对这种情况，攻击者一直在忙于建造“机器人网络”，以便继续匿名存在。

I.1.3 网络嗅探

最初网络嗅探的目标是帮助网络管理员对问题做出诊断，对网络进行分析并改进网络性能。进行网络嗅探的人员在未被交换的网络部分从事工作，包括通过枢纽连接的网络部分，因此嗅探人员可以看到网络该部分的所有流量。

早期的嗅探人员对网络流量数据包报头进行识读，并重点确定低水平数据包特性（如来源和目的地地址等）。但是，现今的嗅探却能够通过数据包破解开放系统互连（OSI）模型各层的数据。

攻击者利用嗅探方式从通过公众或专用网的数据包中看到用户的信息和密码。他们还利用该方式获得有关用户名和密码的价值连城的信息，特别是以明码形式发送密码的FTP、Telnet和其它应用。用于远程访问电子邮件的协议（如IMAP、POP3和POP2）使用简单的用户名和密码认证技术，因此极易受到嗅探攻击。

用户往往在多个应用和平台之间重复使用密码，因此攻击者可以利用所获得的信息访问机密性受到破坏的网络的各种资源。此外，这些资源还可被用作实施其它攻击的桥头堡。

总体而言，攻击者通过遭受损坏的公司物理设施的安全性来对网络进行嗅探。这就如同某人走入一家公司，并将其笔记本计算机与企业网络相连接。无线网络存在同样的风险，即，停车场的某人可以访问公司本地网。一旦进入核心分组网络，攻击者就可以摸清网络配置及操作模式，从而进行进一步的攻击作案。

I.1.4 拒绝服务

拒绝服务（DoS）攻击的重点是阻止合法用户使用某项服务。拒绝服务攻击易于实施，破坏极大。拒绝服务攻击能够中断企业的工作，有效切断企业与外界的联系。分布式拒绝服务攻击使用一个以上机器的资源来对某一资源同时发起拒绝服务攻击。

拒绝服务攻击形式多样，目标广泛，其重点是将网络、服务器、主机和应用资源消耗殆尽。某些此类攻击则侧重中断网络连接。例如，SYN泛洪攻击利用伪造半公开TCP连接请求，将目标资源的内存容量消耗殆尽。此类攻击妨碍合法用户访问主机、网络应用和其它网络资源。拒绝服务攻击能够做到：

- 拒绝网络与互联网连接
- 拒绝向合法用户提供网元
- 拒绝向合法用户提供应用

拒绝服务攻击充分利用受到攻击的系统体系结构存在的弱点。有些情况下，该攻击利用诸多互联网协议（包括互联网控制信息协议（ICMP））共同存在的缺陷。例如，某些拒绝服务攻击向IP广播地址发送大量ICMP echo（ping）数据包，而这些数据包使用潜在被攻击目标的由欺骗获得的IP地址。目标资源收到的答复数量之多足以导致该资源瘫痪。此类攻击被称作借刀杀人式（smurf）攻击。另一种攻击虽然使用用户数据报协议（UDP），但理念并未改变。

I.1.5 桶队攻击

桶队攻击（Bucket brigade attack）亦被称作中间人攻击。实施此类攻击的人在服务器和客户机之间交换的公共密钥中侦听信息。之后攻击者重新发送信息，以其公共密钥取代对方要求的公共密钥。最初发起通信的双方认为他们在相互间进行通信。攻击者可以获得信息或修改信息。可以采用网络嗅探方式发起此类攻击。

I.1.6 后门陷阱

后门是一种快速获得网络资源的方法，其出现方法可能是：

- 系统开发员人为将其置入系统，以便在开发过程中快速访问资源，但在交付产品时未将该功能关闭
- 雇员为方便自己工作将其置于系统
- 标准操作系统安装的组成部分，在进行增强（如默认用户登录身份和密码组合）时未将其取消
- 由心怀不满的雇员留在系统之内，以便其被解雇之后访问企业系统
- 由执行恶意代码（如病毒）创建

I.1.7 伪装

此种行为系指为访问网络而伪装成合法的维护或工程人员，而且仅仅暴露了利用物理设施安全漏洞和人为缺陷，实施诸多威胁的冰山的一角。例如，入侵者可以修改与网络配置管理和信令层相关的数据，以及与计费和使用数据有关的数据。

I.1.8 答复攻击

此类攻击是对信息或信息的一部分进行重复，以便产生未经授权的效果。例如，某一实体为了认证自身而对含有有效认证信息的信息做出答复。

I.1.9 修改信息

修改信息系指在数据传输过程中内容被修改，但却未被发现，并达到未经授权的效果。

I.1.10 内部攻击

内部攻击系指系统合法用户在不经意或无授权情况下做出的某种行为。许多人所共知的计算机犯罪涉及内部人员对系统安全的损坏。严格筛选工作人员，持续不断检查软硬件和安全政策，有助于降低内部人员作案的风险。对审核进行完善跟踪可以大大提高发现此类攻击的可能性，因此应当加以提倡。

I.2 安全威胁

诸如企业之类的各类机构均面临多种威胁。各机构的安全需求以及应采用的安全战略均与众不同，独一无二。从安全角度而言，最难以应对的环境是开放企业环境。在此，企业上下均需要控制雇员、伙伴甚至客户对企业数据库和应用的访问。

I.2.1 应用层攻击

应用层攻击花样翻新，方法多样。由于普通公众可以通过由HTTP协议（端口80）规范的、众所周知的端口地址访问网络主机，因此黑客可以充分利用它发起避开防火墙的攻击。

应用层攻击利用操作系统和应用的脆弱性获得对资源的访问权。配置不当和授权失误均可导致出现安全漏洞。例如，一台主机可能是网络服务器，应对所有人提供所需的网页。主机应按照安全政策规定，严格将shell命令访问限于得到授权的管理员。

账户收集针对的目标是应用要求用户提供登录身份和密码时所进行的认证程序。为用户登录错误身份和错误密码产生不同误码信息的应用极易受到此类攻击的影响。根据误码信息的性质，入侵者可以针对具体客户发起攻击，即，首先确定有效的用户登录身份，之后通过其它形式的密码解读技术获得密码。

可以以病毒、蠕虫、缓冲器溢出和密码收集等方法实施应用层攻击。网络服务和单点登录技术的出现使该情况雪上加霜，因为这些技术实现了基于传统设施的应用在网络上的使用，而设计传统应用时并未将网络连接和安全性考虑在内。

某些应用层攻击的目标仅仅是肢解网站。其它攻击则意在毒害网站小甜饼，以非法获得某一特定服务器的信息。应用通常不检查小甜饼的有效性，因此可能成为执行藏匿于小甜饼的恶意代码的受害者。现有的浏览器存在一些人所共知的脆弱性，方便实施以小甜饼为基础的攻击。

攻击者也可以使用跨网站脚本技术在加入URL的脚本标签中插入恶意代码。当毫无意识的用户点击该URL时，恶意代码得到执行。使用TLS可以解决应用层的某些安全问题，但是SSL不能充分保护网络应用。即使使用SSL也不能阻止诸如账户收集和密码解读等攻击。

为减少网络层攻击的威胁，我们建议增强网络管理工作所采用的所有操作系统，无论这些操作系统是通用操作系统还是嵌入式实时操作系统。应当严格按照产品制造商提供的具体和最新的增强指南开展工作。对于使用旧的操作系统的传统系统而言，产品制造商可能无法提供安全补丁。同时我们建议使用安全电子邮件、应用层防火墙、主机入侵预防和发现系统、功能强大的认证技术、强密码和网站适当退出控制机制，阻止显示未经授权的网络内容。

I.2.2 网络层威胁

攻击者可以使用专业工具发起各种程度的网络层攻击。大型和开放式企业特别容易受到网络层攻击的影响。很多严重的安全威胁通常均与网络基础设施密切相关，包括蓄意破坏、破坏、网络配置不佳、拒绝服务、数据探测、工业间谍和服务窃取。攻击可以由内部人员从网络内部发起，也可能由黑客从外部进行。

最新的黑客技术发展（如基于移动终端的端口扫描）表明，对网络基础设施的攻击甚至可以发端于移动终端。我们建议制定良好的安全政策和通俗易懂的安全程序，以保护网络基础设施。交换机、路由器、接入点、远程访问服务器、无线接入点、主机和其它资源必须得到保护。

IP分组网络可能遭到的常见网络基础设施威胁和脆弱性包括：

1) 不安全的协议泛滥：某些网络依然在使用实践也已证明存在安全漏洞的协议，其中包括：ICMP、TELNET、SNMPv1&2、动态主机控制协议（DHCP）、普通文件传输协议（TFTP）、路由信息协议1.0版本（RIPv1）、网络时间协议（NTP）、域名服务器（DNS）和HTTP。

2) 使用功能弱小、静止不变和由局部管理的密码：某些网络依然在使用由简短和通俗的字典词话组成的密码，极易猜测。某些管理员在所有网元上使用的口令可能一成不变，而所有管理员可能共用并了解这一密码。

3) 未得到保护的安全信息：在某些网络中，诸如密码文件等重要信息并未得到加密。而诸如密码等其它信息则以明码形式在网络上传送。防火墙规则规定不当，加密密钥形同虚设。

4) 未经认证的软件装载和配置文件：装载不正确或恶意软件可能对网络造成威胁，而配置文件则可能造成服务丢失，甚至导致性能陡降。这些做法均为内部和外部人员安装特洛伊木马和其它恶意代码等造成可乘之机，同时它可能导致装置配置不当。

5) 未得到增强的网元和操作系统：厂商默认操作系统装载未根据常见攻击得到增强，因此对网络造成威胁。这种情况包括运行不必要的服务，而同时保持默认账户和密码的开启状态。

6) 管理端口和接口并非必要地暴露于公共网络：使带内管理接口保持与公共互联网连接，也是对网络造成威胁的原因所在。更多的威胁可能源自支持机制的滥用，如通过拨号、综合业务数字网或其它连接以支持模式访问核心网络。

I.2.3 未经授权的访问

未经授权的访问系指一系列不同类型的攻击。实施此类攻击的人员的最终目标是非法获得某些资源，且各类企业均存在这一安全问题。任何允许进行互联网访问或提供远程局域网访问能力的企业均可能受到未经授权的访问的攻击。

方便出差在外的员工通过拨号方式访问电子邮件，并使得远端办公室通过拨号线路、内联网和将外部伙伴与企业网连接的外联网进行访问的远程服务，也使网络更易受到黑客、病毒和其它攻击的危害。黑客可以利用专业工具访问企业网络，从而危及敏感信息，或网络被用作攻击其它网络的工具。

在各个层面对网络实施保护有助于防止未经授权的访问攻击。在网络层使用防火墙、代理服务器和用户至会话的过滤手段能够进一步加强网络保护，但黑客也无时无刻不在变得更加精明。在网络和应用层使用用户访问控制手段以及恰当的认证和授权方式，可以最大程度地降低未经授权的访问攻击风险。

I.2.4 窃听

窃听是一种难以发现的威胁。实施此类攻击的人员的目的在于听取企业局域网的信息，并最准确地记录其原始数据。攻击者采用市场上销售的、现成“混杂模式”以太网适配器展开攻击。通过该模式，攻击者可以在网络上获取每一个数据包。如今攻击者可以通过诸多免费的网络嗅探程序来实施窃听。

任何允许进行远程访问的企业均可能受到此类攻击的危害，开放式和大型企业在此最为不堪一击。以太网交换技术在预防窃听威胁方面束手无策，因为地址解析协议（ARP）欺骗可以使交换机制完全唯命是从。以太网交换手段只能遏制“懒惰窃听者”。采用功能强大的访问管理技术和加密技术可以最大程度地降低此类攻击的威胁。

附录II

各种网络安全技术

（本附录不构成本建议书不可分割的一部分）

攻击技术的成熟度和有效性都在不断提高。如今，入侵者可以迅速展开攻击，以利用产品中存在的薄弱环节。进攻者可使这些攻击自动化，并提供给公众使用。表II.1提供对抗网络威胁的现有技术。

表II.1 – 网络安全技术

技术手段	类别	技术	目的
密码技术	证书和公钥架构	数字签名	用于发行和保持可在数字通信中使用的证书
		加密	用于传输和存储过程中的数据加密
		密钥交换	建立一种用于保证连接安全的会话密钥或交易密钥
	保证	加密	保证数据的真实性
访问控制	周边保护	防火墙	进出网络的访问控制
		内容管理	检测不合规信息的流量
	认证	单一因素	利用用户身份/密码组合验证识别码的系统
		双因素	需要物理标记并知晓一秘密的两个部分才准予用户系统接入的系统
		三因素	附加一项生物识别技术或人体特征测量等识别因素
		智能令牌（Smart tokens）	通过细查智能卡一类装置确定用户的可信识别码
	授权	基于职能	根据赋予用户的职能控制用户使用相应系统资源的授权机制
		基于规则	根据与每位用户相关的规则而不是其在机构中的任职控制用户使用相应系统资源的授权机制

表II.1 – 网络安全技术

技术手段	类别	技术	目的
系统完整性	反病毒	签名方式	利用其密码签名防范病毒、蠕虫和特洛伊木马等恶意计算机密码
		行为方法	检查运行程序中的非授权行为
	完整性	入侵检测	可用于向网络管理员报告可能发生的诸如服务器文档受损等安全事件
审核和监测	检测	入侵检测	将网络业务和主机记录项目与具有黑客特点的数据签名进行比对
	防范	入侵防范	发现对网络的攻击并采取机构提出的缓解攻击影响的行动。可疑活动会触发管理员报警和其它可配置的响应
	日志纪录	记录工具	将网络业务和主机记录项目与具有黑客特点的数据签名及地址描述文件进行监测和比对
管理	网络管理	配置管理	允许进行网络控制与配置以及故障管理
		补丁管理	安装网络设备的最新更新和修复软件
	政策	执行	使管理员能够监测和执行安全政策

II.1 密码技术

密码技术是将无格式数据通过加密转换为密码的操作。通过解密技术可将密码数据还原成原始的无格式文本。现有的密码技术可用于数据的加密/解密，也可用于信息发起方的认证和不可否认性。

加密技术对存储于设备或存储媒质以及正在通信链路上传输的信息，起着重要的保护作用。

在密码技术中，利用数学算法对数据进行加密的工作通常称为数据加密。另一方面，对加密数据进行数据加密反向操作即可还原原始数据。加密技术利用密钥进行加密和解密工作。

密码技术可以分为两个基本类型：对称密钥和非对称密钥。

1) 对称密钥加密技术采用的是加密密钥与解密密钥相同的算法。这一模型安全依赖于猜测密钥的难度。通信的各方就密钥达成一致，并对他人实行密钥保密。对称密钥算法的实例包括三重数据加密标准（3DES）和高级加密标准（AES）。

2) 非对称密钥密码技术采用的算法使用一个密钥进行数据加密，而用另一密钥进行加密文本的解密。这类加密技术的用户拥有只有用户掌握的专用密钥，其公共密钥是对外公开的。其他人可利用公共密钥进行无格式文本的加密。只有相应专用密钥的持有者才能进行无格式文本的解密。

对称密钥加密技术的计算速度通常高于非对称加密技术。然而，对称密钥加密技术的主要问题在于密钥的分发。因此，它们通常无法适应大规模部署。另外，非对称密钥密码技术（亦称公共密钥密码技术）可以部分解决对称密钥密码技术的密钥管理局限性问题。公共密钥密码技术依靠数字证书解决公共密钥的管理和废止问题。为提高计算速度，公共密钥密码技术可以用作一种以对称密钥换取在会话或交易中的使用权的安全方式。

数字签名是部署公共密钥加密技术的实例。数字证书为公共密钥和证书持有者的结合提供了保障。数字签名可以提供认证、数据完整性和交易的不可否认性，确认信息发送人声称的识别码的佐证并通常与数字证书共同使用。数字证书是承载公共密钥密码技术和数字签名所需信息的媒体，可由经批准或具有可信度的机构颁发给用户。

消息认证码（MAC）是一种消息认证校验和，是通过对一消息运用认证方案和密钥得出的。与数字签名技术相比，MAC采用同一密钥进行计算和验证。因此，MAC只能由既定的接收方加以验证。在基于散列函数的MAC（HMAC）（见[b-IETF RFC 2104]）之中，一个（或多个）密钥与一个散列函数共同生成一个附于消息之后的校验和。

II.2 访问控制技术

访问控制重点保证只有经授权的用户可访问网络设备或连接系统。实际上，访问控制可使IT专业人员更好地分析和了解其网络所受攻击的类型和性质。可用于访问控制的技术多种多样。以下分段对这些方法做了论述。

II.2.1 周边保护

周边保护技术可防止不受信任或未经授权的用户利用网络或计算机。这种技术在受保护区域和对外或对不受信任的外人（其中不包括不受信任的内部人员）开放的区域之间设置逻辑或物理边界。周边保护技术可用于保护网络或单一设备。这种技术示例包括：

1) 内容过滤或内容管理软件对可网上访问或发布的数据类型加以限制（见[b-ISO/IEC 10828-3]），还限制了用户访问其范围以外内容的能力,从而最大限度地减少了自不受信任的地点下载病毒和其它恶意密码的机会。内容过滤可以URI（见[IETF RFC 2396] ）过滤器的形式出现，使用户无法访问具有可疑内容的网页。内容过滤可用于扫描电子邮件等应用消息，以发现垃圾邮件病毒或未经批准的内容。

2) 防火墙：此项技术（见[b-ISO/IEC 10828-3］）可分为四大类型：包过滤器、电路层网关、应用层网关和多阶层状态检查防火墙。

- 包过滤防火墙在IP层运行，通常是路由器防火墙的一部分。它们将每个IP包与既定规则进行对比后，前转到下一路由或其最终目的地。防火墙根据比较结果或丢掉该包，将它前转，或向发起方发送一条信息。规则可包括IP地址的来源和目的地，使用的来源和目的地端口号码及协议。网络地址转换（NAT）路由器具有提供包过滤防火墙的优势，还能够隐匿防火墙内设备的IP地址。包过滤防火墙对网络性能的影响很小，并能在一定程度上提供网络层的安全。
- 电路层网关监测处于TCP/IP的TCP层的TCP之间的握手，对请求的会话的合法性作出判断。此外，经电路层网关向远端电脑发出的请求，在接收方看来似乎的确来自网关。这项技术有助于隐藏受保护网络的信息。电路层网关不进行逐包过滤。
- 代理或应用层网关可对OSI模型的应用层封包进行过滤。来向与去向请求无法访问无代理的服务。代理对应用层的封包进行检查，过滤HTTP POST（见[b-IETF RFC 2616]）等针对应用的指令，拒绝未经配置的业务接近应用，还能起到记录用户活动和登录的作用。代理可提供高度的安全性，对网络性能具有极为积极的影响。
- 多阶层状态检查防火墙综合了上述各类防火墙的特点。这种防火墙在网络层进行封包过滤，确定会话包是否有效并对应用层的包内容进行过滤。对于收发信双方间的连接而言，多阶层状态检查防火墙是透明的。

3) 网络地址转换（NAT）：此项技术能使网络编址计划受到防火墙的掩护。NAT中的内部网络系统IP地址被映射到一个不同的对应外部可路由地址。NAT能使多个防火墙内的系统共享同一个外部IP地址。外部用户依然可以通过前转某些端口号的来向连接访问防火墙内的资源。NAT可以在交换机、路由器和防火墙等多数网络设备上实施。

4) 应用层网关：这些系统（见[b-ISO/IEC 10828-3]）包括基于硬、软件的设备和成套设备。这些设备的目的在于限制两个不同网络之间的互访。这些系统为限制网络间互访采用了状态封包检测和应用代理技术，也可使用这些技术的组合和变型（如电路层防火墙）。此外，应用层网关也可进行NAT。

5) 应用代理：这些系统（见[b-ISO/IEC 10828-3]）通过检查协议堆栈最高层的封包，使应用层了解连接企图。应用层的数据完全处于应用代理的监视之下。这一能力可使它们轻易地直接观察到每个连接企图的微小细节，根据观察到的情况实施安全策略。应用代理具有终止客户连接并与内部受保护网络新建连接的能力，从而通过使内外部系统分离提高安全性。

II.2.2 虚拟专用网（VPN）

[b-ISO/IEC 18028-5］全面介绍了利用VPN保证全网通信安全的问题。

VPN目前用于完成网络间互连的任务，也是一种远程用户与网络连接的方式。最简单的VPN具有在现有网络或点到点连接上建立一个或多个安全数据信道的机制。VPN能够动态地建立和拆除。主办网络既可以是专用网络，也可以是公共网络。

通过VPN的远程访问是在本地用户和远端地点（见[b-ISO/IEC 18028-5]）之间开通的常规点到点连接上实施的。VPN可以作为受管理的服务提供，即共用基础设施提供的其安全可靠性与专网相当的连接、管理和编址。

VPN的类型（见[b-ISO/IEC 18028-5]）可用多种方式表示，主要的形式有：

– 单一点到点连接（例如通过站址网关远程访问企业网络的客户设备）；或
– 点到云连接（利用MPLS技术）。

目前有三大类型的VPN（见[b-ISO/IEC 18028-5]）：

– 2层VPN通过主办网上运行的VPN将企业的站址联系在一起，或向机构提供远程连接，以此模仿LAN设施。提供商的服务项目通常包括提供模拟纯线路连接的虚拟专用线路业务（VPWS），或提供更全面模拟LAN业务的虚拟专用LAN业务（VPLS）。
– 3层VPN利用在网络基础设施上运行的VPN模仿WAN设施，具有在公共基础设施上使用专用IP编址计划的能力，而这种做法是公共IP连接所不允许的。然而，通过NAT在公共网络上使用专用地址，可能会使IPSec（见[b-ISO/IEC 2411] ）VPN的建立和使用复杂化。
– 4层VPN的作用是向公共网络交易提供安全保障。此类VPN的连接通常是通过作为4层协议的TCP建立的。这种类型的VPN在通信应用之间提供安全信道，以保证交易全程的数据机密性和完整性。

VPN既可以在所属公司控制的专网内建立，也可在公共领域网络中实施。实施中也可将这两种计划结合使用。另一方面，可以利用穿过互联网服务提供商网络的隧道，借助安全信道建立信道，此时的公共互联网实际上是起支撑作用的传送系统。因此，VPN承载的数据面临着更大的保密风险。

隧道是建立在现有网络基础设施之上的连接网络设备的数据通道，对网络运行是透明的。利用隧道创建的VPN通常较基于物理链路的网络具有更大的灵活性。隧道可用虚拟电路、标记交换或协议封装方式创建。

表II.2.2列出了各类VPN的安全形态（见[b-ISO/IEC 18028-5]）。

表 II.2.2 – VPN 的安全形态

VPN	技术	用户认证	数据加密	密钥管理	完整性核查
2层 VPN	帧中继、ATM, MPLS, PPP, L2F	未提供	未提供	未提供	未提供
	L2TP (见[b-IETF/RFC 2661])	类似CHAP	未提供	未提供	未提供
3层 VPN	IPSec	基于证书的（封包）预先共享密钥	可协商的多种算法（封包）	IKE	可协商
	配备L2TP的IPSec	基于证书的（封包）预先共享密钥	可协商的多种算法（封包）	IKE	可协商
	MPLS	未提供	未提供	未提供	未提供
4层 VPN	TLS	基于证书	可协商	可协商	可协商
	安全壳	系统生成的密钥对（未经认证）	可协商	交换给予数据发送方的公共密钥	可协商

注 1 – 可用 SSL 替换 TLS。

注2 – [b-IETF RFC 3031]概括介绍了多协议标记交换架构（MPLS）。[b-IETF RFC 1661]描述了点到点协议（PPP）。[b-IETF RFC 2427]探讨了帧中继的多协议互连。

II.2.3 认证

用户认证有多种方法可循。这一技术包括密码、一次性密码认证、生物识别技术、智能卡[b-ISO/IEC 7816-x]和证书。基于密码的认证必须使用较强的密码（如，长度至少八个字符，其中至少包含一个字母、一个数字和一个特殊字符）。仅靠密码认证恐怕还不够。根据对硬盘的评估，可能需要将密码认证与其它认证和授权方式相结合，其它方式包括轻量级目录访问协议（LDAP）（见[b-IETF RFC 3377]）、远程用户拨号认证系统（RADIUS）（见[b-IETF RFC 2869]、[b-IETF RFC 3579]和[b-IETF RFC 3580]）、Kerberos协议（见[b-IETF RFC 1510]）和公共密钥基础设施（PKI）（见[b-IETF RFC 2459]）。

认证系统可根据所需鉴别因素的数量进行分类。单因素鉴别是指利用一个因素（如用户ID/密码组合）确认身份的系统。双因素鉴别介绍了一种需要以两种组件获得系统访问权的程序，例如在掌握物理标记的同时又知悉某项秘密（如密码）。三因素系统又增加了一个生物识别或人体特征测量的鉴别因素。采用的鉴别因素越多，认证的安全性越高；但采用较多的鉴别因素会增加复杂性、成本和管理开销。在简单易行和安全之间找到最佳平衡是所有认证系统面临的关键挑战。

单因素用户ID/密码鉴别是当今最通用的认证系统。密码认证系统结构简单、易于管理也深为用户所熟悉。如果使用强密码，单因素鉴别系统可实现高度的安全性。遗留的密码体系遇到了一些挑战，因为用户很难记住多重强密码。正如以下建议将谈到的那样，可以最大限度地减少这些缺陷，利用“单一强密码”体系提供最佳解决方案。

许多鉴别系统增加了智能卡等令牌作为第二种鉴别因素。由于用户需要为鉴别目的证明实际拥有令牌，因此令牌可提供更高的认证安全性。攻击者同样也必须拥有用户的令牌才能获得系统访问权。但由于需要令牌和令牌识别器，随更高鉴别水平而来的是更高的系统费用。此外，令牌很容易丢失，而补发令牌又会是一笔可观的管理开销。

可利用发给用户并贮于令牌或用户电脑内存中的数字证书，提供基于强加密技术的鉴别方法。加密算法用于确保具体证书合法地发放到用户手中。公共密钥基础设施具有数字证书的发放和维护功能。基于强加密技术的系统固然能够提供极为可靠的认证，但它们价格昂贵并会生成额外管理开销，因此目前只在非常安全的环境中采用。

II.2.4 授权

一旦完成认证，授权机制便对用户访问相应系统资源进行控制。授权可以根据控制的粒度、即系统资源之间划分的细腻程度加以分类。细粒度授权通常是指以极微小增量控制访问的系统，例如具体的应用或服务。

授权通常是“基于角色”的，即对系统资源的访问是以某人在机构中承担的职务为依据的。系统管理员的角色使他拥有访问所有系统资源的极大特权，而普通用户的角色只能使他访问这些资源的子集。如果采用较细粒度授权，人力资源管理员的角色，可能使他独掌高度机密的人力资源数据库的访问权，而会计角色可能使他独具访问会计系统数据库的权利。

授权也可能是“基于规则”的，即对系统资源的访问是以与每个用户相关但又独立于其机构角色的规则为依据的。例如，制定的规则可允许只读访问，或对一系统内全部或部分文件的读/写访问。

II.2.5 认证和授权协议

有几项协议通常用于认证服务。RADIUS协议（远程用户拨号认证系统）（见[b-IETF RFC 2865]）广泛用于集中化的密码认证服务。起初为认证远程拨号用户开发的RADIUS协议，已应用于普通用户认证服务。LDAP（轻量级目录访问协议）在认证和授权系统中得到广泛使用。LDAP为存储用户认证和授权证书提供了一种便利方式。

RADIUS认证服务器经常与LDAP目录中的证书存储联袂提供一种统一的认证与授权系统。当用户希望访问这一系统中的某项具体应用时，该应用将在查询用户认证证书后，将证书转送统一的系统。于是，RADIUS服务器将提交的证书与存储于LDAP数据库的证书进行

比对，并向LDAP数据库查询认证规则信息。认证结果（合格或不合格）将与针对具体用户的认证规则信息一起返回应用。这时实施于应用的授权规则，使用户能够访问具体数据或服务。从最终用户角度看，这些认证和授权系统预计是自动运行和便于使用的。

II.3 反病毒和系统完整性

蠕虫病毒、恶意代码和特洛伊木马能够修改系统及其数据。因此，必须采用具有病毒扫描能力的技术，并确保系统的完整性得到维护。

蠕虫病毒是一种程序，无需人为参与就能实现自身的跨系统复制。病毒可以附着在用户的文件上，当毫无察觉的用户执行打开受感染文件等操作时，病毒就会被激活，通过将自己复制到其它文件而肆虐。而特洛伊木马则通常在无戒备的用户面前表现为一种有效程序，以此掩盖其有害代码。

反病毒技术有助于系统防范蠕虫病毒、恶意代码和和特洛伊木马病毒的攻击。软件可以装入用户设备，或作为网络或互联网服务提供商提供的一项服务。系统完整性技术所用的软件可以进行检查，确保只对关键的系统文件进行经授权的更新。

反病毒软件产品可采用String签名技术发现病毒和恶意代码。这项技术需要反病毒软件在发现恶意代码前，就对这类代码有所了解。因此，其签名数据库必须随时更新才能提供有效保护。

操作扫描器检查运行中的代码是否执行了未经授权的操作。软件将可疑操作通知用户。操作程序反病毒的成功率往往是有限的，但对于蠕虫和特洛伊木马病毒却可能较为有效。静态试探扫描器对代码的扫描，是试图发现与疑似病毒行为有关的操作。

系统完整性技术采用的软件可监测对重要文件所作的修改。IT管理人员可利用这类技术进行系统检查，确定黑客的系统渗透是否得手（黑客倾向于留下后门陷阱）。

II.4 审核和监测

审核和监测技术使IT管理人员能够对包括入侵检测和防范软件在内的整个系统安全作出评估。IT管理人员可利用这一技术开展系统分析，以确定其受到攻击后的薄弱环节。在某些情况下，可以在系统受到主动攻击期间进行系统分析。

可采用入侵检测和防范软件（IDS）（见[b-ISO/IEC 18043]）监测网络，确保没有未经授权用户访问网络。多数IDS应用将网络业务和主机记录项目与具有黑客特点的数据签名和主机地址描述文件进行比对。入侵监测软件可发现说明存在未经授权用户的流量模式。可疑操作会触发管理员报警及其它可配置响应。入侵监测系统（IDS）可按以下条件分为几大类别：

- 事件监测时间框架：有实时或离线两种方式，所用方式取决于是在事件发生过程中还是在非高峰时段以批量形式对系统日志或网络流量作出分析；

- 安装类型，基于网络或基于主机。基于网络的IDS通常包括安装在网络瓶颈处（可监测两点之间流量的位置）的多个监视器（通常为经预配置的设备）。基于主机的IDS要求将软件直接安装在受保护的服务器上，并在这些服务器上监测网络连接和用户操作；和
- 事件响应类型：IDS采取阻止攻击（如修改防火墙规则或路由器过滤器）的主动干预行动，还是直接将问题通报给职员或其它网络系统。

多数商用IDS产品提供网络和基于主机的综合监测能力，由一台集中式管理主机接收各监视器发来的报告并向网络支持人员报警。建议根据具体客户的需求，在多数网络设备中采用基于网络的IDS产品。

II.5 管理

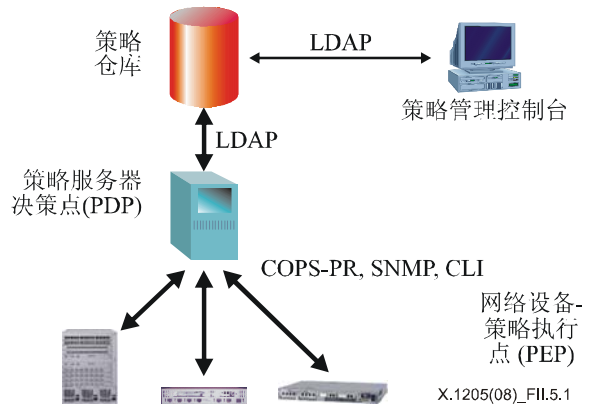
IT管理人员可利用配置管理技术对其网络设备进行安全设置与验证。他们利用策略管理制定业务驱动的安全和服务质量（QoS）策略，并在整个机构内付诸实施，但无须理解实施策略所需的与具体设备相关的规则和设置。在技术上，策略是一套使用、管理和控制IT资源访问的规则；它们必须脱胎于机构制定的商业政策。安全领域的策略管理是要解决这些技术（如防火墙、IDS、访问表和过滤器、认证技术）带来的复杂性、艰苦的学习过程以及系统无法观察网络不同部分（数据中心、远端办公室、校园）的问题。

虽然存在数不胜数的可部分解决问题的方案，最终的策略管理系统提供的集中式网络配置能够保证，对众多节点的安全参数进行统一设置，并减少网络隐患带来的风险。这并不意味着只有一种策略体系；一个拥有多个管理域的较大型网络可能需要多种策略体系，每个体系负责管理一个设备子集和域间统一性。

全面建成的策略管理体系的一大优势是易于使用，而且环境更加安全。理想的网络管理器希望利用非技术性词汇制定网络运行策略，而后再将策略体系自动转换成适于在全网推行的安全机制。

II.5.1 策略管理参考模型

图II.5.1描述了IETF的策略管理（[b-IETF RFC 2753]）体系框架。这一参考模型将作为安全和QoS管理的策略管理蓝图。因此，策略管理将以这一模型为基础，在全网络和架构的各个层面实施，并向雇员、网络技师、合作伙伴甚至用户等各类用户和应用提供。



图II.5.1 – 策略管理参考模型

模型的组件包括：

- 策略执行点（PEP）：接受来自策略制定点的策略（配置规则）并针对流经设备的网络流量实施这一策略的网络或安全设备。这项实施工作根据需要利用网络和网络辅助安全机制。
- 决策点（PDP）：PDP或策略服务器将网络策略抽象处理为具体的设备控制消息，再传送给策略执行点。这些策略服务器通常为独立系统，控制着具体管理域内所有的交换机和路由器；策略服务器通过控制协议（如COPS、SNMP子集命令、Telnet或设备的具体命令行界面（CLI））与这些设备交流。
- 通用开放策略服务（COPS）：COPS是一种基于TCP的简单查询和响应状态协议，可用于决策点（PDP）和客户政策执行点（PEP）之间的策略信息交换。在[b-IETF RFC 2748]中已有规定。COPS随时依靠PEP建立与主要数据点（并在无主要数据点提供时与次要数据点）的连接。另一方面，COPS代理设备可用于将策略服务器发出的COPS消息转换成网络和安全设备可识读的SNMP或CLI命令。

  COPS协议支持两种不同的政策管理扩展模型，即[b-IETF RFC 2749]规定的动态外包模型COPS-RSVP，和[b-IETF RFC 3084]规定的配置或提供模型COPS-PR。COPS协议的提供扩展允许PDP将策略“预先”装入PEP，从而使PEP能够根据这一预先提供的信息就数据包做出决策。PDP和 PEP之间需要进一步交流，源源不断地向数据仓库（即目录）提供策略，与发送到PEP的策略保持同步。
- 策略仓库：网络目录是存储所有策略信息的仓库，对网络用户、应用、计算机和服务（例如目标和属性）以及这些实体间的关系做了描述。IP地址与最终用户（通过动态主机控制协议-DHCP和域名系统-DNS）进行了紧密集成。目录通常在专用数据库设备上实施。轻量级目录访问协议是策略服务器用以访问目录的机制。

策略仓库用于存储相对静止的网络信息（如设备配置），而策略服务器则存储更多动态网络状态信息（如带宽分配或已有连接的信息）。策略服务器从目录中检索策略信息，并用于相应的网元。

目前还没有既定的标准可用于描述目录数据库的结构，即对网络目标及其属性的定义和表达方式作出说明。在多厂商应用共享同一目录信息的情况下，需要一种通用的目录计划；例如，所有厂商都需要一种解释和存储路由器配置信息的通用方式。DMTF（桌面管理任务组）正在开发的未来目录激活网络（DEN）标准将满足这一需要。DEN包括的信息模型可提供抽象化的配置文件与策略、设备、协议和服务，从而为整合用户、应用、网络服务以及可扩展的面向服务的框架提供了一个统一模式。

- [b-IETF 3377］*轻量级目录访问协议*（LDAP第3版）做了说明：LDAP是一用于访问目录服务的客户机服务器协议。基于条目的LDAP信息模型包括某些目标（如某人）的信息，是由具有一种类型和一个或多个数值的属性构成的。每个属性的语法可以确定允许哪类数值进入属性，以及这些数值在目录运行期间的行为。
- *策略管理控制台*：人通过通常运行于个人电脑或工作站的管理控制台，与策略管理系统开展互动。另一方面，网络浏览器几乎可以从任意地点提供管理器接入，其策略目标级安全对个人能够修改的政策类型设置限制。管理控制台将策略开列于目录之中。控制台提供的图形用户界面和工具，是管理员定义作为商业规则的网络策略所必需的，而且还可供操作员访问各交换机和路由器内安全级别较低的配置。

策略管理参考模型元素之间的互操作可实现闭环策略管理，包括边缘设备配置、网上策略实施以及最终用户应用观察到的网络功能核查。对网络的策略实施包括对争相访问网络资源的应用或用户进行的接纳控制。策略管理可在某种程度上简化企业内部的配置管理环境，从而最大限度地减少人为失误的机会。

II.5.2 增强服务器操作系统

增强服务器操作系统（OS）是保证应用安全层信息系统安全的关键内容之一。通常，企业可能将多个不同的操作系统用于各种数据应用（包括网络管理），同时，支持IP电话和针对通信的应用服务器亦可能采用若干操作系统。将同一类型操作系统的数个版本用于信息技术（IT）基础设施的做法司空见惯，因此保障安全的工作难上加难。

最常见的数据操作系统往往还被广泛用于支持IP电话和针对通信的应用服务器。厂商提供此类系统的增强型版本，并采用现成的安全软件来实现防病毒、入侵发现和审核事件（login audit）等功能。对操作系统实行增强的第一步是避免对服务器进行克隆，并确保用于下载操作系统的媒介值得信赖。在此基础上，则可进一步开展工作。如果尚不了解操作系统具体得到增强的内容，应与操作系统厂商取得联系，以获得最新的增强操作系统的补丁和程序。

附录III

网络安全示例

（本附录不构成本建议书不可分割的一部分）

本附录旨在提出使用本建议书所述技术的机构或大型企业如何保障其各方面安全性的有关示例。

制定确保总部安全的分层安全解决方案的原则，包括网关到互联网、数据中心、远端办公室、远程访问和IP电话。我们采用本建议书阐述的技术，具体说明企业安全工作不存在万用良方。表III提供所需的解决相关安全问题示例。企业1的示例是小型企业示例，该企业各站点之间实际专用线路不多，雇员远程接入网络的情况有限，他们对网络的访问通过服务提供商（负责建立安全的环境）提供的数据中心实现。企业2的示例是开放型企业示例，该企业的业务模式是充分利用互联网，从而使合作伙伴、供货商和客户只能有限访问由企业管理的各项应用。在企业2的示例中，内部和外部用户使用有线或移动装置在家、远端办公室或通过其它网络访问企业网络。

表III.1 – 企业相关安全工作指南

网络领域	企业1示例	企业2示例
保障总部安全	是	是，代表最严格的安全要求
保障远端办公室的安全	选择在虚拟或物理专用线上进行加密	是，包括远端办公室互联网访问
保障远程访问安全	是，但仅涉及专用拨号访问	是，包括伙伴和客户
保障数据中心安全	是，内部数据中心	是，包括互联网数据中心
保障IP电话安全	是	是，充分利用VPN

III.1 保障远程访问安全性

远程访问技术方便企业或机构有效利用任何地点的人力或资源。但是，此类技术也可能给企业带来安全隐患。多数远程访问用户为出差在外或在家办公的企业员工，同时也包括按需与企业网络进行连接的小型办公室。通过开展网络安全工作和进行安全的访问管理，可以很好地解决这方面的主要挑战。网络管理安全工作可在总部以外的地点加以实施。应用安全也必不可少，因为远程装置需要通过病毒扫描软件和个人防火墙得到保护。

远程用户面临的一个重大威胁是用户设备（UE）盗窃。出现远程用户设备被盗情况时，应防止进而发生对企业网络其它部分的入侵，或对存储于系统上的信息进行访问。用户希望随身携带移动装置或终端，方便随时随地上网，因此有必要对远程访问系统存储的敏感信息进行加密，最好采用与普通应用无缝结合的系统。目前市场上提供的加密系统方便用户

正常操作，无须对文档进行手动或个别加密/解密。例如，可用加密形式对整个文档系统或“文件夹”进行存储，而解密则融入文档系统的正常访问之中。在远程访问用户在家或在酒店使用无线局域网时，可能出现另一种形式的威胁。在这种情况下，安装最新的个人防火墙和防病毒软件非常重要。

最常用的远程数据通信访问形式是直接到企业或到互联网服务提供商（ISP）的拨号访问，以及使用数字用户线路（DSL）、有线调制解调器、本征以太网（如在酒店）和无线局域网（如在机场）对互联网直接进行访问。支持互联网访问的公共无线数据服务发展迅速，为笔记本和手持计算机带来了更强的移动性。互联网与日俱增的可用性和经济效益都在促进拨号和直接接入方式远程访问VPN的迅速发展。图III.1提供如何保障远程访问安全性的示例。

图III.1 – 保障远程访问安全性

采用本建议书介绍的技术，并通过采取下列步骤可以保障远程访问的安全性。

1) 拨号访问企业中心网络

通过拨号进行远程访问的用户在与其计算机系统相连的调制解调器和位于企业总部或区域站址的调制解调器池（亦称远程访问交换机）之间建立电话呼叫。设置拨号接入系统时，应采用本建议书此前所述的、提供接入认证和授权的安全访问管理系统。直接交换接入虽然在上世纪80年代和90年代初得到广泛使用，但目前却被互联网远程接入VPN迅速取代。

2) 远程访问VPN

互联网远程访问灵活性极高，带宽极宽。此方面存在两种方式：使用远程接入VPN客户机的IPSec VPN，或以用户浏览器SSL功能为基础的SSL VPN。

3) IPSec VPN

IPSec是可跨应用使用的网络层方式（例如，如建立IPSec VPN连接，用户可以访问电子邮件和自我服务等应用，并浏览内部网络和访问经授权的应用）。需要在UE上装载IPSec客户机才能够进行远程访问。手持计算机也可以采用市场上提供的客户机。还应当为UE装载防病毒和病毒发现软件。

无论采用到ISP POP的拨号访问，还是有线或无线直接接入，VPN客户机均对用户进行认证，核证用户本身计算机系统的完整性，并与企业建立一条安全链路（或隧道）。

VPN客户机能够（例如通过防火墙）确保远端系统本身是安全系统，特别是在与企业建立连接之际。在会话建立阶段，对连接到企业的流量采用加密和认证手段。

设想远程访问VPN能够发现，并在可行的情况下，避开常见的互联网障碍，如NAT和去向防火墙（即，从另一个受到防火墙保护的网络建立一条至企业网络的链路），或至少告之远程用户，他们面临何种性质的障碍。

在企业边缘，来自互联网的远程访问连接由IPSec网关系统处理。在企业边缘，应当通过由多个网关提供的多重到达互联网的路径，避免单点故障造成的危害。我们建议根据企业规模，采用在地理位置上相互分离的网关。网关应通过若干功能特点支持企业范围内有效的远程访问。我们推荐的功能特点包括：简单的客户机配置；能将连接连至企业内部网络而非终止会话；能够提供具有状态功能的防火墙，以避免单独设立防火墙。此外，我们建议网关采用多种认证机制，如RADIUS、PKI和LDAP，提高选择用户认证等级的灵活性。网关还应当具备高度灵活性，使企业能够将可能已得到使用的、用户笔记本中的RADIUS、基于目录的用户ID/密码、甚至智能或令牌卡认证机制纳入网关之中。能够支持L2TP和PPTP将十分有益。

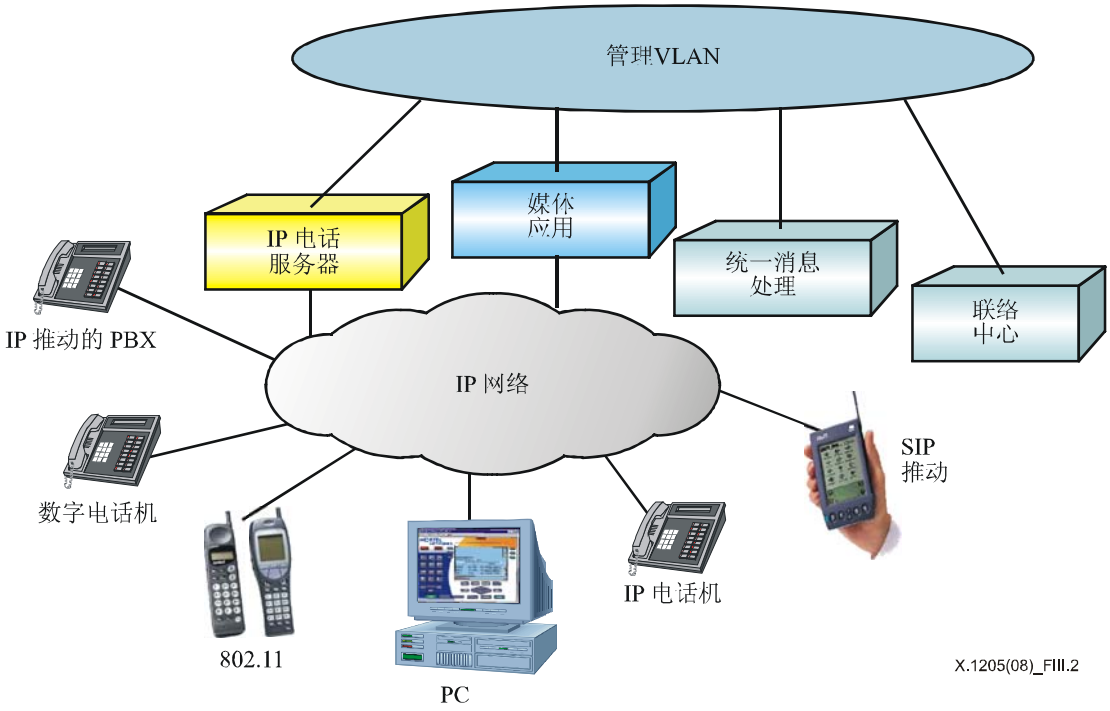
III.2 保障IP电话的安全性

各机构和企业均已开始推出IP电话解决方案，目的在于充分享受局域网和广域网（WAN）的融合以及融合的应用所带来的益处。每一种VoIP系统均是一种由四个逻辑功能组成的硬件/软件解决方案：

- IP电话和PC软客户机。
- 通信服务器（亦称作呼叫管理服务器或网守）。
- 提供灵活网络接入的媒体网关（例如，通过传统的专用小交换机（PBX），公众交换电话网（PSTN）和公众无线网络及未来技术）。
- 应用服务器（例如，统一消息处理，会议和由SIP推动的协作应用）。

这些功能以及相关通信应用服务器（例如支持联络中心和统一消息处理的服务器）在电话或企业级IP网络上广泛分布，提供人们所要求的可靠性、话音质量和拥塞管理。通过无线局域网和经IP VPN的互联网，可以扩大覆盖范围，增加移动性。

图III.2说明普通机构在保障IP电话安全性方面采取的方式。



图III.2 – 保障IP电话安全性

IP电话是运行于IP网络的应用，它充分利用网络所提供的安全功能。IP电话与多数数据应用不同，对时间十分敏感，这一点对业务管理十分关键。IP电话同其它数据应用一样，可能遭受若干攻击的影响，例如：

- 对路由器的攻击可能造成机构内语音和数据服务的关闭；
- 拒绝服务攻击可能造成IP电话通信服务器或客户机的过载；
- 死亡之Ping（Ping of death）向VoIP装置发送多个应答请求，干扰VoIP工作；
- 端口扫描可以使VoIP客户机和服务器的脆弱性一目了然；
- 数据包嗅探可能对对话做出记录和/或侦听；
- IP欺骗可能误传媒体或信息流的来源或目的地；
- 病毒、蠕虫、特洛伊木马和定时炸弹都可能对服务器和客户机形成攻击。

IP电话并非无坚不摧。例如，由于对密码管理不力，同时由于运行XML（见[b-W3C XML 1.0]）产生的漏洞，黑客接管IP客户机的情况时有发生。在跨互联网对VoIP进行本征运行时，这些攻击十分严重；如果将IP电话严格用于企业内部并在通过互联网时采用隧道式连接，则此类攻击并非十分严重。

如同任何其它应用一样，我们需要对IP电话的风险做出评估，以便明确IP电话为机构创造的价值，了解损失产生的影响，并制定相关的安全政策。电话是一项至关重要的企业职能，因此，电话系统同网络一样，必须在整体上得到保护，免受任何威胁和攻击的影响。

通常而言，电话用户进行网下接入时，只需要采用直接呼入系统（DISA）对自身进行认证。另一方面而言，要求数据用户使用多个用户身份和密码进行网络和应用访问的情况却屡见不鲜。这种复杂的局面完全与保障企业环境安全的要求相悖。在VoIP方面强调简洁性更为重要，因为人们期望一经拨号即能听到拨号音。毫无疑问，任何有关VoIP的安全机制均不能有碍于实现所要求的连通性和语音质量。

保障IP电话安全性的关键指导原则包括：

1) 企业IP电话解决方案仅限于企业内运行，并通过电路交换连接形式与公众网络实现互通。
2) 从数据角度而言，企业IP电话系统的安全性取决于IP网络基础设施，因此这一网络的设计和工程必须满足电话对时延和可靠性的要求。
3) 企业IP电话通信服务器与企业的业务休戚相关，因此必须保证系统的物理安全性，并防止内部和外部攻击对其造成影响。
4) 提供安全的VoIP客户机认证。
5) 只有在通过共用的媒体局域网或互联网时才需要对语音进行加密。
6) 针对整体电话环境采取全面的、保障安全的方式，包括VoIP客户机和服务器、应用服务器（如用于统一消息处理和联络中心的服务器）以及传统PBX。

保障IP电话解决方案的安全性需要在网络各层采取协调方式。相关的政策管理和安全的访问管理能够确保对用户进行认证并控制IP电话的特性和呼叫功能。应当采用安全的管理技术来保护通信服务器和媒体网关等VoIP装置。通过采用保障远程访问、小交换机连接和无线局域网访问安全的IPSec，可以将针对数据通信的安全机制用于VoIP。如果将VoIP状态检查加入到防火墙和网络地址转换功能之中，则可以通过政策管理加强安全性。应用安全性可以通过若干方式得以保障，包括增强操作系统，并防止UE感染病毒。

III.2.1 保障应用和IP电话通信服务器的安全

IP电话系统的核心部件是通信服务器。它既可以是自成一体的装置，也可以是与由IP推动的PBX企业通信管理器融为一体的设备。同样重要的装置是提供联络中心、多媒体应用、统一消息处理和自我服务互动式语音应答系统的应用服务器。增强操作系统的功能是保障这些服务器安全工作的第一步（如上所述）。

III.2.2 保障VoIP客户机的安全

VoIP解决方案支持众多的客户机和访问配置，包括IP有线和无线电话以及基于PC机的软客户机。这些装置一经与IP网络连接，则十分易于受到攻击的影响。

目前市场上提供包括SIP在内的、若干不同的电话信令协议。在传输层，信令流量通常使用TCP。未来而言，将能广泛提供保障VoIP层面信令流量安全的功能。在IP电话系统中，人们通过采用[b-ITU-T G.729]（8kbit/s）等标准以及语音活动发现算法对语音信号进行分组，并在传输层使用实时协议（RTP）与UDP一道工作。

对于如何最大程度地降低IP电话和基于PC机的软电话客户机的风险性，人们是仁者见人，智者见智。IP电话是为客户定制的、仅用于电话通信的电子装置。电话本身不存在任何需要保护的存储内容或资产（电话作为一种值得信赖的装置出现在网络上的情况除外）。需要保护的唯一资产是对主叫方和呼叫本身的确定。这些电话装置十有八九均采用专用的瘦客户机协议，其特点/功能和安全性取决于通信服务器。该方式与实际工作中采用的方式截然不同，后者依赖VoIP话机的XML进行功能运行，而这本身可能十分脆弱。

VoIP软客户机与其它应用和资产一道置于用户设备中，并运行市场上广泛提供的操作系统。能够得逞的攻击往往造成高昂代价，因为在UE上存在诸多的宝贵资产，包括应用和业务、财务及个人数据。目前人们的惯常做法是为UE平台专门编写一种或若干种安全应用，提供个人防火墙、病毒发现功能以及IP VPN客户机。可以将应用于数据的机制用于VoIP软客户机。

III.2.3 保障局部和总部的VoIP安全

可以通过两种方法将IP装置连线，组成总部网络：共用媒体和专用交换以太网。目前行业的总体趋势是在流量增长和易于管理的要求驱动下，采用专用交换以太网。此外，有关安全性和可管理性的要求也推进了人们在企业网络中对VLAN的部署（见[b-ISO/IEC 18028-5]）。无线局域网提供第三种可行方案，且在教育和卫生领域发展迅猛。

随着IP电话的出现，我们强烈建议在桌面将VoIP软客户机和VoIP装置与交换以太网环境连接。该方式可以满足下列要求：

– 取消共用媒体以太网的CDMA操作，从而最大限度地减少VoIP的时延变化

– 禁绝其它桌面可能对VoIP呼叫的窃听，增强VoIP的安全性

此外，企业可选择以逻辑方式将VoIP电话组成为各自的VLAN，从而方便管理。

IP电话将电话特点/功能从桌面延伸至会议厅或教室，因此极大地提高了企业内使用无线局域网用户的生产效率。无线局域网极易受到影响，因此建议所用的体系结构确保无线部分信令和语音两方面的安全性。在笔记本上同时配置软客户机和IP VPN即可实现这一目标。另一种可行方式是在某些无线局域网IP电话上，内置加密和认证功能。这两种方法均为无线局域网环境提供强健的用户认证和加密能力。

III.2.4 保障IP电话小交换机的安全

人们可以通过若干方式支持远端办公室和VoIP小交换机解决方案，其中包括VoIP电话和软客户机支持的一体化办公设备解决方案。其它方式则在远离中心服务器的地方部署客户机，充分利用VoIP分布各处的特性。无论何种情况，我们均建议小交换机中的VoIP流量应经数据IP VPN运行，保障安全。

III.2.5 保障IP电话远程访问的安全

IP电话将电话特点/功能从桌面延伸至远端地点，大大提高了在家中、酒店或出差路上工作的远程用户的效率。经常处于移动状态的工作人员在笔记本中既配置VoIP软客户机，又安装IP VPN客户机。这种配置亦能使人们充分利用酒店、机场和会议中心安装的无线局域网接入点。VoIP电话为远程工作人员和联络中心代表提供功能丰富的通信手段，安全则由总部的IP VPN予以保证。

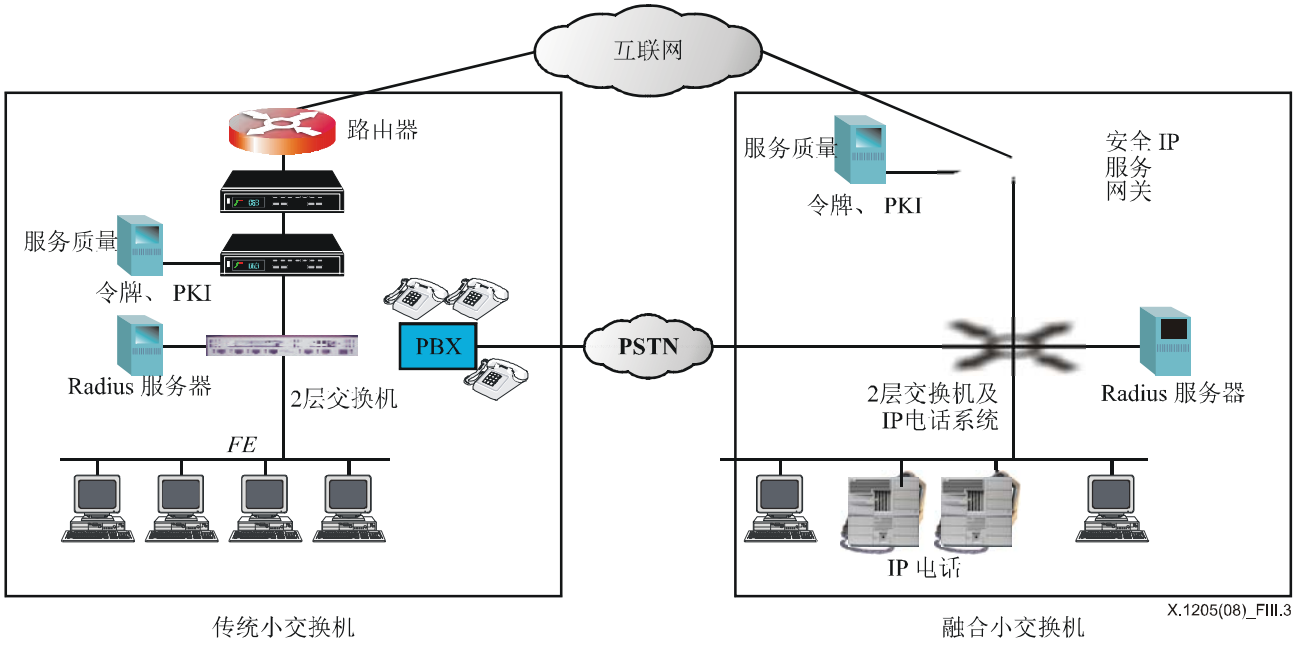
III.2.6 IP电话网络管理安全性

从管理角度而言，应配置专用以太网物理端口。它应成为管理VLAN的组成部分，通过访问清单和边界安全措施在路由层阻断所有非管理流量。可以利用IP VPN为供应商、系统集成商和/或VAR提供网下接入。应当关掉未用端口（如，用于控制面板或远程调制解调器访问的端口）。这些服务器应仅运行得到授权的应用软件。应当赋予得到认证的操作人员不同级别的特权（监督、配置、控制），确保安全等级多样化。用户密码必须得到安全存储，密码格式和变化管理应得到严格控制。作为可选功能，可通过IP VPN技术对内部传送的管理流量（如计费信息）进行加密。

III.3 保障远端办公室的安全性

从家庭工作人员桌面到大型企业总部网，远端办公室可谓规模迥异。尽管“远端办公室”和“远程访问”之间存在诸多相同之处，但是我们依然可以通过它们是否具备远端地点和企业其它地点之间进行双向通信的能力来对其加以区分。这就是说，远端办公室是一个工作场所，与企业其它地点随时连接，并能在办公时间与后者交换信息。而远程访问则是按照远程访问用户的需求，与企业建立临时连接。

在银行零售、卫生和政务等领域，分支机构连网是造价最为昂贵的服务提供手段。传统的分支机构网络环境采用各种局域网技术和多个协议路由器与帧中继网络连接，并以综合业务数字网（ISDN）电路交换设备作为备份。以下四个领域的重大发展为改造分支机构网络创造了很好的机遇：1) 局域网标准向以太网上集中；2) IP作为协议得到普遍采用；3) 互联网；4) 2层和3层VPN服务日益增多。然而，这些最新发展也特别为大型机构和企业带来了花样翻新的安全挑战。图III.3具体说明这一问题。



图III.3 – 保障远端办公室的安全性

分支机构网络广域网的边缘要求包括在本地VLAN之间和通至网络的路由、服务质量（Qos）、带宽管理和与广域网进行的、可扩展的连接。具体需要做到在广域网上支持封装机制，按需提供可靠性。保障低成本高效益的互联网（帧中继网）安全通信极为关键。由传统的相对安全的广域网向IP VPN转变亦非轻而易举。某些企业希望实现任何远端办公室均能直接访问互联网的目标，因此需要配置远程防火墙。其它企业希望在分支机构和企业骨干网之间建立可靠性高和动态实现路由的连接，并通过集中式防火墙手段访问互联网（有些情况下，帧中继为主要路径，互联网为备份路径；或企业正在将IP VPN作为首要途径）。动态路由通过下列方式增强可扩展性并提高可靠性：

- 自动学习网络拓扑；
- 自动了解企业各最终用户的地址；
- 自动调整，适应网络拓扑变化。

然而，在路由网中采取安全措施是一种亡羊补牢的做法，绝非由先见之明所引导。例如，过去并不存在行之有效的、在加密VPN隧道上进行动态路由的手段，因此管理工作异常困难。

总体而言，上述情况导致企业为远端办公室和分支机构网络购买、安装、维护和管理多个安全和网络装置，使环境变得极为复杂，管理成本高昂。

随着互联网通信向IP VPN的过渡，人们需要尽可能以低成本高效益手段满足一系列全新的安全要求，包括IP经源隧道路由和虚拟专用网（VPN）等网络安全功能，以及在网络辅助层进行加密和防火墙状态检查；在安全访问管理层进行远端办公室认证和提供目录服务。所有这一切均须以高度综合的方式加以提供。必须将安全政策管理的落实溶入该解决方案，从而为每一个用户提供独特的安全资料，无论用户是在家里通过UE经公众互联网进行登录，

还是仅在本地与分支机构办事处网络连接，资料均由用户个人掌控。还需将网络管理安全机制延伸至远端办公室，消灭可能损害网络安全的任何“后门”。最后，如果在远端办公室安装数据服务器和/或IP电话，则需保障其应用安全。

III.4 保障无线局域网的安全性

公司总部、分支办事处、远程办公员工、顾问和业务伙伴之间进行通信的机会日新月异。各企业目前都在充分利用新的IEEE 802.11无线技术（见IEEE 802.11），随时随地开展业务活动。然而随着这些解决方案的采用，人们必须以集中方式有效管理用户访问，以保障机构资源的安全。

无线局域网（WLAN）的安全特别易于遭到破坏。在标准局域网（LAN）上侦听通信内容需要侦听者采用物理线缆与网络连接，而无线传输则在空中侦听方面留有后患，任何持有标准无线局域网卡的人均可对网络造成入侵。

WLAN通过无线装置和IEEE 802.11协议拓宽企业网的覆盖范围。WLAN的设备包括笔记本和台式计算机等移动设备（统称为移动单元（MU）或移动台（STA））使用的无线网络接口卡（NIC）。NIC能够使网络信号由连接装置通过中间装置–无线局域网网关（或被称作无线接入点（AP）的枢纽）进行传输，该装置将无线信号转换为将在有线网上进行传输的有线信号。

公司通过以太网枢纽或交换机，可以将无线局域网接入点连接至有线局域网，如增加有线用户一样轻而易举。接入点与交换机连接，即确保获得了一条10/100 Mbits的专用线路，使所有可用接入点均在无须争夺有线枢纽带宽的情况下，象交换机一样进行工作。

最初的[b-IEEE 802.11]标准由一系列规范构成，其中的IEEE 802.11a、IEEE 802.11b、IEEE 802.11g和IEEE 802.11i目前仍被用于网络信号环境，但需要人们在距离和带宽之间做出权衡。

III.4.1 无线局域网的安全问题

无论WLAN的安全机制如何，WLAN信号均通过无线电波在空中进行广播和接收，因此并不具备阻止未授权用户的任何实际手段。令人遗憾的是，这些信号极易被侦听，极易受到对公司网络入侵的影响。因此，在公司网络中增加无线节点意味着为保护WLAN网络资产而纳入适当的安全防范措施和良好的安全做法。

WLAN网络的基础设施层包括网络的各个部分、线缆、互连和传送媒介（覆盖空间），例如，接入点、移动站、网关和托存相关服务（如RADIUS和DNS等）的服务器。

服务层包括无线局域网接入服务和其它方便无线接入的服务，例如，认证、授权、记账（AAA）和密钥管理服务等。

WLAN带来的安全威胁包括：

- 破坏无线流量的机密性和完整性。发起攻击的人可以侦听移动计算机和无线接入点之间的通信，从而获取禁止向第三方透露的敏感或保密信息。与之相反的情形是，发起攻击的人在合法用户毫不知情的情况下，将信息加入正在进行的交易之中。

- 公司局域网面临破坏威胁。除非移动平台能够得到安全的认证，否则发起攻击的人可以使用符合IEEE 802.11的装置与WLAN连接，成为该网络上“得到授权”的移动台，进而获得对公司局域网的访问权。

可以利用X.800威胁模型对各种攻击总结如下：

X.800威胁模型	攻击方法
破坏信息和/或其它资源	AP入侵
破坏或修改信息	WEP密钥密码解读，中间人
信息和/或其它资源的盗窃、移动或丢失	AP入侵，WEP密钥密码解读，中间人，MAC地址欺骗，未授权装置，驾驶攻击（wardriving），3层劫持，自组织网络
信息披露	AP入侵，WEP密钥密码解读，中间人，MAC地址欺骗，未授权装置，驾驶攻击（wardriving），3层劫持，自组织网络
服务中断	射频干扰，数据泛洪，2层劫持，伪AP，欺骗性解除认证帧，FATA-Jack DoS

WLAN与有线网络一样，要求具备机密性、完整性和访问监控机制。无线网络的主要安全问题在于外部人员可以轻而易举地通过网络进行接收或发送，无论其是否在覆盖范围之内。

由于上述原因，发起攻击的人可以轻易通过窃听和加入非授权接入点（被称作非法接入点（rogue AP）），进行中间人和会话劫持等攻击，从而易如反掌地从WLAN内攻击WLAN用户。发起攻击的人利用这些手段蒙蔽用户，诱使他们与其接入点连接，在网络中强行纳入一个看似合法的节点，肆无忌惮地获取用户身份、密码和其它私人信息。

我们可以通过下列技术确保无线环境安全可靠：

- 网络名称：服务区标识符（SSID）
- 网卡注册：MAC访问控制清单（ACL）
- 共有密钥加密：通过使用安全协议（如WPA/WPA2）实现

此外，可以使用下列类型的认证方式：

- 开放系统认证：允许拥有接入点SSID的任何人接收访问。
- 共有密钥认证：用户处理大家共有的秘密才可以得到认证。

在最初的[b-IEEE 802.11]规范中，安全漫游通过移动至周围接入点的移动单元（MU）的预先认证得以实现。因为所有接入点和移动单元均使用相同的共有密钥，所以接入点之间不存在切换信息，由此，新的接入点可以预先假设移动单元的认证为有效认证。这一做法的优点是切换迅速，但缺点是认证安全性较低，因为管理过程未得到认证。

III.4.2 无线接入点之内和之前的安全要求与机制

鉴于无线环境的开放性质，加密解决方案与最终用户认证并举的方法是唯一能够真正对其施以保护的方法。对流向网关的流量进行加密，前者的身份可以通过加密手段予以核证。

保障WLAN安全的两项主要要求是流量安全，漫游安全。实现安全通信的最基本要求是对由移动装置到接入点、到接入点后的网关（如使用IPSec网关）、或到应用服务器（安全网站）的流量进行加密。而要实现安全的漫游，则移动用户必须在不丢失正在进行的会话，并无需针对新接入点重新进行认证的情况下，从一个接入点移动至另一个接入点。漫游的时间紧迫，对用户应用的影响被降至最低程度。用户期望且设想在不同领域之间传递其证书信息时，信息会得到适当保护。

III.4.3 IEEE 802.11规范得到增强的安全功能

上述各种安全风险促使人们对最初的[b-IEEE 802.11]标准做出增强，使其为无线局域网提供更加有效的安全手段。IEEE802.11i引入了IEEE 802.1X（见[b-IEEE802.1X]）访问控制、动态重置密钥、每会话密钥分配机制和强大加密算法。[b-IEEE 802.1X]通过采用可扩展的认证协议（EAP）（客户机和服务器之间的一套信息认证谈判和认证传送方法（见[b-IETF RFC 2716]、[b-IETF RFC 3748]和[b-IETF RFC 4017]）），加强了接入点的认证/访问控制。EAP支持包括MD5在内的若干认证方法。传输层安全（TLS）加MD5是得到最为广泛支持和可用性最强的方法。无论选择何种EAP，IEEE 802.1X（见[b-IEEE 802.1X]）的所有三个组成部分均必须支持相同的方法（见图III.4.3）。

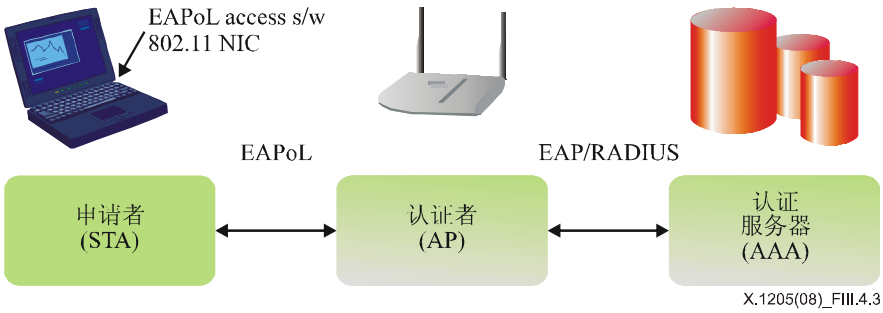


图 III.4.3 – IEEE 802.1X 的组成成份

保证IEEE 802.1X漫游的安全性需要用户总能针对即将漫游入的、新的接入点进行重新认证。每会话密钥和缓慢公共密钥基础设施（PKI）的操作使人们难以实现快速重新认证，因此，在漫游过程中，接入点切换之间的这些认证可选方法将会给人们带来一定的困难。

扩展认证协议 – 遂道传输层安全（EAP-TTLS）和受保护的扩展认证协议（PEAP）为[b-IEEE 802.1X]提供漫游快速重新认证，其主要手段是利用TLS握手协议提供的连接重建机制。在此并不需要彻底认证，因为人们的设想是，能够重新开始TLS会话已证明用户了解主密钥，这一认证已经足以。

III.4.4 以分层方式保障无线局域网的安全

好的无线局域网的安全体系结构同普通局域网环境一样，要求人们采用集多种技术于一体的分层方式，最终形成综合性无线局域网/局域网安全体系结构。在可行的情况下，应将现有的局域网安全机制应用于无线局域网。

III.4.4.1 接入点

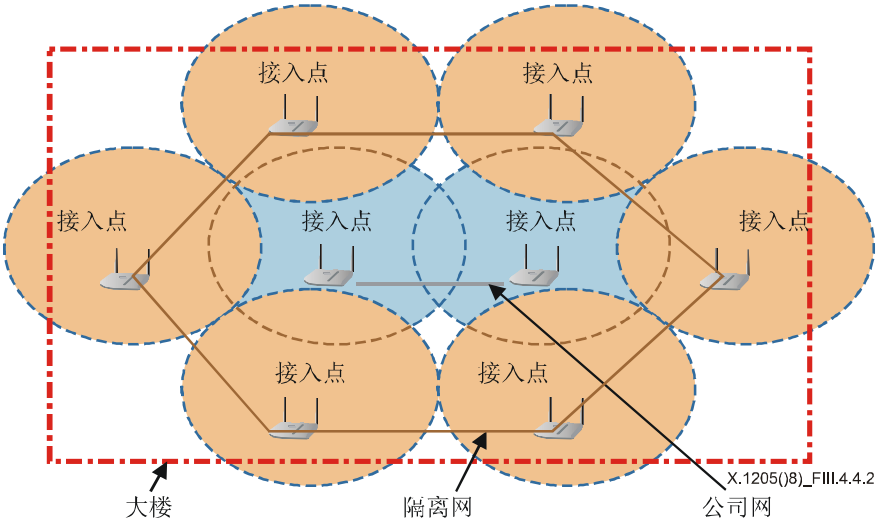
虽然扩展服务区标识符ID（ESSID）和MAC ACL系统的安全功能很弱，但是人们还是可以使用这两种手段。在配置中使用相同ESS ID的所有移动单元和接入点均可以自由地相互关联。[b-IEEE 802.11]支持“广播ESSID”，即允许移动单元在不了解ESS ID的情况下与接入点相关联，如果关闭这一功能，则可加强安全性。MAC ACL包含得到允许的MAC地址清单，同时可能包含被禁止的地址清单，因此我们不应忘记，当涉及到大量计算机时，这种情况将难以管理。

目前具有标准前和专有安全机制的接入点产品包括：WPA、WPA2、动态WEP高级加密标准（AES）和动态密钥完整性协议（TKIP），并可方便使用128位加密。动态WEP是一种按照预先确定的时间间隔、更经常的改变WEP密钥的手段。AES是一项新批准的美国联邦信息处理标准（FIPS）标准，用于取代数据加密标准（DES）加密算法。TKIP加强了密钥排列算法，以防范传统WEP遭受的密钥恢复攻击。由于该手段存在弱点，因此[b-IEEE 802.11]建议，除了对旧的设备进行打补丁之外，不应当采用TKIP手段。

注 – Wi-Fi 保护接入（WPA）最初只是一项行业倡议，旨在具体规定如何改进无线局域网（LAN）的安全性。WPA-PSK（WPA–预共享密钥）是家庭用户使用的特殊 WPA，这些用户不具备企业认证服务器，因此特殊 WPA 为其提供强大的加密保护。在 WPA-PSK 中，加密密钥在特定时间内，或在特定数量数据包传送之后，自动改变（密钥重置），并在装置之间自动认证。WPA-PSK 使用的共享密钥，必须在无线接入点外层（outer）和 WPA 客户机均得到输入。该共享密钥的长度为 8 至 63 个字符。动态密钥完整性协议（TKIP）在最初于无线装置输入共享密钥之后启动，旨在处理加密工作并自动进行密钥重置。WPA 是一种软件更新。无线产品厂商和网络安全工作专业人员期望现有的 WPA 和 WPA-PSK 能够长期有效。WPA 使用高级加密标准（AES）作为一种补充的、替代 WEP 加密的可选手段。

III.4.4.2 空域

通过高增益定向天线，未经授权的外来人员可以从远处获得对无线局域网的访问权，因此最好防止此类行径得逞。阻止外部人员通过高增益定向天线利用无线网络空中信号的方法可以是，在企业所属地边界或WLAN边界，采用未与内部网络连接的接入点（见图III.4.4.2）。外来人员之所以无法看到内部无线局域网是因为企业的外接入点与企业内接入点采用相同载频，并实际上对外部提供更强的信号，对外来人员“干扰”内部信号。将这些外部接入点与孤立网络进行连接，并增加入侵发现系统（IDS），和发现入侵及收集证据的蜜罐（honeypot），可大大强化这一设置。



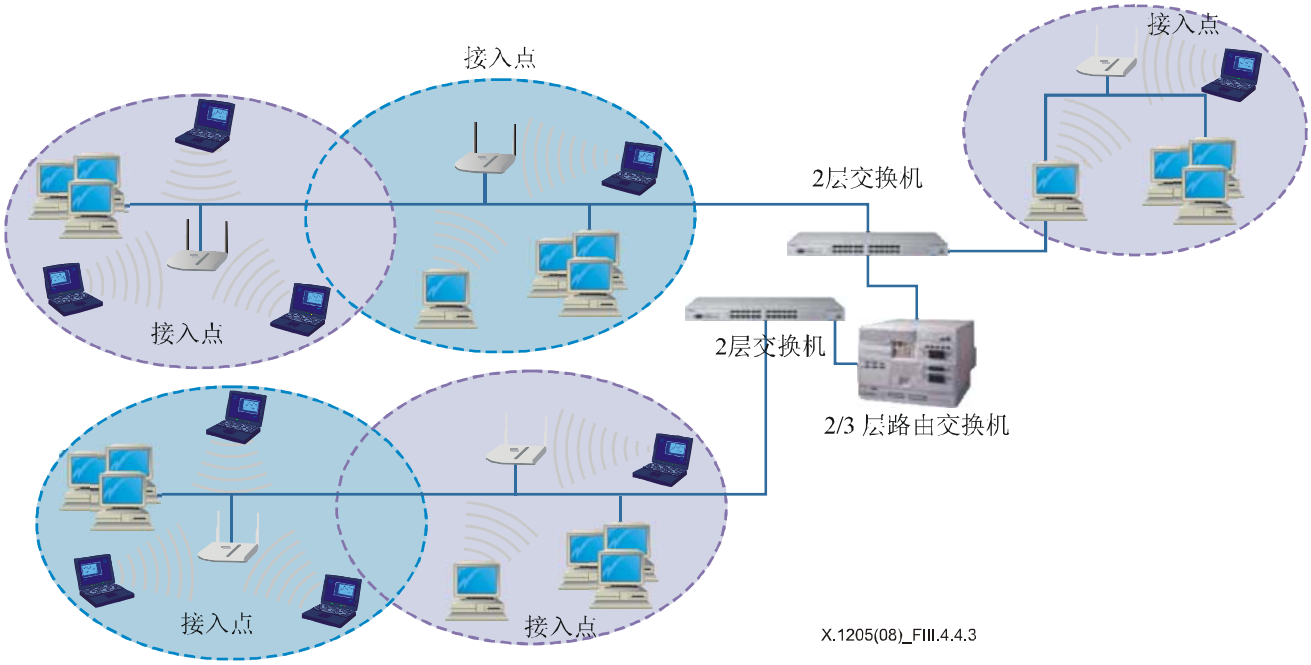
图III.4.4.2 – 保障边界安全的Sentry 接入点

10.4.4.3 条块分割

应尽可能将现有的局域网安全机制用于无线局域网。此外，无论[b-IEEE 802.1X]增强与否，人们都可以采用更多的有效机制，如通过VPN和TLS的加密、通过虚拟局域网（VLAN）的无线网络的条块分割和通过防火墙的边界保护。图III.4.4.3具体显示带有公共SSID或子集的通用WLAN IEEE 802.11接入点与2层交换机的连接情况。2层交换机能够智能地限制流向其它接入点的流量，有些甚至具备虚拟局域网能力。对于置于另一个子集或SSID的接入点而言，可以通过2/3层路由交换机进行连接。在这一体系结构中，应将安全通信、安全漫游和切换以及边界防卫作为安全无线局域网/局域网环境不可或缺的组成部分。

IPSec协议是得到实践证明和值得信赖的安全通信协议。对于能够在移动装置上充分利用IPSec客户机，或应用超出网络前端的环境而言，IPSec是保障通信安全的最适宜手段。IPSec VPN的主要优点是，强有力的安全政策尽在企业掌控之中，与局域网相连的任何人都拥有与本地局域网用户相同的各种特权。

同样的技术对于“热点”无线局域网同样行之有效。例如，如果雇员从酒店的经ISP远程访问企业网络，他可以使用酒店提供的PPPoE客户机和用户ID/密码通过DSL实现连接，并访问ISP。之后，雇员通过IPSec客户机与企业网相连接。



图III.4.4.3 – 带有公共SSID的通用WLAN IEEE 802.11接入点

III.4.4.4 管理层

还应当通过管理和操作对策确保无线局域网的安全性，例如扩大机构的安全政策，将无线局域网纳入其中。应当尽可能将现有的局域网安全机制用于无线局域网，不然，则需要将新的机制与现有机制相结合。例如，利用IPSec解决方案，企业可以对无线局域网用户、远程用户和防火墙规则进行集中管理，而且在存在外联网访问管理应用的情况下，不需要再增加这类管理应用。产品厂商也正在努力，使网络发现、脆弱性扫描和IDS等机制能够意识到无线局域网的存在。

III.4.4.5 对WLAN访问协议的分析

可以利用ITU-T X.805所述的维面对上述各节讨论的各种Wi-Fi协议（即IEEE 802.11i、WPA2[2]、WPA和WEP）的相对优缺点做出分析。在此仅利用两三个维面进行了分析，我们可以将此扩大到所有八个维面。

我们使用下列符号从质的角度对每一维面的结果用表进行了总结：

√	满意
P	部分满意
X	标准未予解决

访问控制

[b-IEEE 802.11]最初的规范（包括WEP）不包括内在的访问控制机制，因此在广泛部署WLAN时利用WLAN网关进行业务层访问控制。基于这一假设，最终用户对WLAN服务的访问控制被评定为部分充分。

---

2 虽然WPA2和IEEE802.11i具有相似的安全功能，但是WPA2可以与安全程度较低的WPA结合，反映出WPA2在安全方面存在弱点。

[b-IEEE 802.1X]是IEEE 802.11i、WPA和WPA2的最终用户Wi-Fi服务访问控制机制。

表III.2 – 访问控制维面的覆盖范围

访问控制安全维面								
安全面	安全层							
	基础设施				服务			
	IEEE 802.11i	WPA2	WPA	WEP	IEEE 802.11i	WPA2	WPA	WEP
最终用户	√	√	√	X	√	√	√	P
控制	√	X	X	X	√	√	√	X
管理	X	X	X	X	X	X	X	X

认证

IEEE 802.11i、WPA2和WPA均使用IEEE. 802.1X/EAP进行认证，与此相反，WEP使用“公开”或“共享秘密”进行认证（使用与加密相同的static密钥），因此WEP认证被评定为“部分认证”。如果其它标准在[b-IEEE 802.1X]方面使用存在弱点的EAP协议（如MD5），可能得到相同的评定等级。

只有802.11i阐述了跨接入点和其它网元（以支持漫游）的控制信息认证问题。支持其它标准的AP通常使用专有机制来在漫游过程中交换这一信息，认证此类实施的安全性问题不属于本建议书的范围。

表III.3 – 认证维面的覆盖范围

认证安全维面								
安全面	安全层							
	基础设施				服务			
	IEEE 802.11i	WPA2	WPA	WEP	IEEE 802.11i	WPA2	WPA	WEP
最终用户	√	√	√	P	√	√	√	P
控制	√	X	X	X	√	√	√	X
管理	X	X	X	X	X	X	X	X

可用性

诸如射频干扰、数据泛洪和2层会话劫持等DoS攻击都是针对可用性的攻击。由于WLAN的安全标准在2层和2层以上运行，因此根本无法防止此类攻击。同样没有任何一项WLAN标准能够应对AP失效。

表III.4 – 可用性维面的覆盖范围

可用性安全维面								
安全面	安全层							
	基础设施				服务			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
最终用户	P	P	P	X	P	P	P	X
控制	P	P	P	X	P	P	P	X
管理	X	X	X	X	X	X	X	X

显而易见，利用IEEE 802.11i或WPA2可以设计、部署和维护相对安全的WLAN网络，但是，仅仅实施这些标准还不能确保WLAN网络的端到端的安全，因为正如该案例研究所示，可用性维面的安全问题尚未得到解决。

参考资料

[b-ITU-T G.729] Recommendation ITU-T G.729 (2007), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005), *Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification* <http://www.ietf.org/rfc/rfc0854.txt?number=854>.

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)* <http://www.ietf.org/rfc/rfc0959.txt?number=959>.

[b-IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm* <http://www.ietf.org/rfc/rfc1321.txt?number=1321>.

[b-IETF RFC 1510] IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)* <http://www.ietf.org/rfc/rfc1510.txt?number=1510>.

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)* <http://www.ietf.org/rfc/rfc1661.txt?number=1661>.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats* <http://www.ietf.org/rfc/rfc1991.txt?number=1991>.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication* <http://www.ietf.org/rfc/rfc2104.txt?number=2104>.

[b-IETF RFC 2196] IETF RFC 2196 (1997), *Site Security Handbook* <http://www.ietf.org/rfc/rfc2196.txt?number=2196>.

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification* <http://www.ietf.org/rfc/rfc2311.txt?number=2311>.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap* <http://www.ietf.org/rfc/rfc2411.txt?number=2411>.

[b-IETF RFC 2427] IETF RFC 2427 (1998), *Multiprotocol Interconnect over Frame Relay* <http://www.ietf.org/rfc/rfc2427.txt?number=2427>.

[b-IETF RFC 2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* <http://www.ietf.org/rfc/rfc2459.txt?number=2459>.

[b-IETF RFC 2510] IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocols* <http://www.ietf.org/rfc/rfc2510.txt?number=2510>.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol -- HTTP/1.1* <http://www.ietf.org/rfc/rfc2616.txt?number=2616>.

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method* <http://www.ietf.org/rfc/rfc2631.txt?number=2631>.

[b-IETF RFC 2661] IETF RFC 2661 (1999), *Layer Two Tunnelling Protocol "L2TP"* <http://www.ietf.org/rfc/rfc2661.txt?number=2661>.

[b-IETF RFC 2716] IETF RFC 2716 (1999), *PPP EAP TLS Authentication Protocol* <http://www.ietf.org/rfc/rfc2716.txt?number=2716>.

[b-IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol* <http://www.ietf.org/rfc/rfc2748.txt?number=2748>.

[b-IETF RFC 2749] IETF RFC 2749 (2000), *COPS usage for RSVP* <http://www.ietf.org/rfc/rfc2749.txt?number=2749>.

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control* <http://www.ietf.org/rfc/rfc2753.txt?number=2753>.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary* <http://www.ietf.org/rfc/rfc2828.txt?number=2828>.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)* <http://www.ietf.org/rfc/rfc2865.txt?number=2865>.

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions* <http://www.ietf.org/rfc/rfc2869.txt?number=2869>.

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture* <http://www.ietf.org/rfc/rfc3031.txt?number=3031>.

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)* <http://www.ietf.org/rfc/rfc3084.txt?number=3084>.

[b-IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)* <http://www.ietf.org/rfc/rfc3174.txt?number=3174>.

[b-IETF RFC 3377] IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification* <http://www.ietf.org/rfc/rfc3377.txt?number=3377>.

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3579.txt?number=3579>.

[b-IETF RFC 3580] IETF RFC 3580 (2003), *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* <http://www.ietf.org/rfc/rfc3580.txt?number=3580>.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3748.txt?number=3748>.

[b-IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* <http://www.ietf.org/rfc/rfc4017.txt?number=4017>.

[b-IETF RFC 4252] IETF RFC 4252 (2006), *The Secure Shell (SSH) Authentication Protocol* <http://www.ietf.org/rfc/rfc4252.txt?number=4252>.

[b-IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions* <http://www.ietf.org/rfc/rfc4366.txt?number=4366>.

[b-IETF RFC 4557] IETF RFC 4557 (2006), *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* <http://www.ietf.org/rfc/rfc4557.txt?number=4557>.

[b-ISO/IEC 7816-x] ISO/IEC 7816-x, *Identification cards – Integrated circuit(s) cards with contacts* <http://www.iso.org/iso/search.htm?qt=7816&searchSubmit=Search&sort=rel&type=simple&published=on>.

[b-ISO/IEC 18028-2] ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40009>

[b-ISO/IEC 18028-3] ISO/IEC 18028-3:2005, *Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40010>

[b-ISO/IEC 18028-5] ISO/IEC 18028-5:2006, *Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.*
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40012>

[b-ISO/IEC 18043] ISO/IEC 18043:2006, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[b-IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control*
<http://www.ieee802.org/1/pages/802.1x.html>.

[b-W3C XML 1.0] W3C XML 1.0 (2004), *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), <http://www.w3.org/TR/REC-xml/>.

[b-SSL3] The SSL Protocol Version 3.0, <http://wp.netscape.com/eng/ssl3/draft302.txt>

[b-WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*, <http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/>

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
2009年，日内瓦