国 际 电 信 联 盟

ITU-T

Y.2705

(03/2013)

国际电信联盟
电信标准化部门

Y系列：全球信息基础设施、
互联网的协议问题和下一代网络

下一代网络 – 安全

应急通信服务互连的最低安全要求（ETS）

ITU-T Y.2705 建议书

ITU-T

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
NGN中的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
未来的网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
运营商级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2705建议书

应急通信服务互连的最低安全要求（ETS）

摘要

应急通信服务（ETS）是一项国家服务，在发生灾害和紧急情况时向ETS授权用户提供优先通信服务。ITU-T Y.2705建议书介绍了EST互联网互连的最低安全要求。这将使灾害和应急情况出现时签订了双边和/或多边协议的不同国家网络间的ETS得到必要安全保护支持。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2705	2013-03-01	13

关键词

应急通信服务（ETS）、下一代网络（NGN）安全以及优先服务和能力。

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）和国际电工委员会（IEC）合作制定的。

注

本建议书为简要扼起见而使用的“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，这可能不是最新信息，因此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

引言

应急通信服务（ETS）是一项国家服务，在发生灾害和出现紧急情况时向ETS授权用户提供优先通信服务。ETS实施是一项国家事务。但是，灾害/紧急情况可能超越国与国之间的地理边界，因而国家/主管部门有可能签订双边和/或多边协议将它们各自的ETS系统连接起来。这将使灾害和应急情况出现时签订双边和/或多边协议的不同国家网络之间受ETS保护的优先通信服务（如话音、信息、视频和数据）得到支持。

互连国家网络间ETS的完整性、机密性和可用性将依赖于包含在端对端通信中的各个国家网络的安全性。为使网络具备不同国家（如国家/主管部门）网络间端对端ETS的安全性，需要规定最低的ETS互连安全要求。

ITU-T Y.2705 建议书

应急通信服务互连的最低安全要求（ETS）

1 范围

本建议书规定了ETS网络互连的最低安全要求。安全要求的范围包括跨网络边界（即不同国家网络间）ETS通信的完整性、机密性和可用性。

本建议书的这一目的是规定可用于增进对直接或间接互连网络间ETS支持的最低安全要求。

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。所有建议书和其他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他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。本建议书引用某个文件，并非确定该文件自成一体时具备建议书的地位。

[ITU-T E.106] ITU-T E.106建议书（2003年），《救灾运作的国际应急优先机制（IEPS）》。

[ITU-T E.107] ITU-T E.107建议书（2007年），《应急通信服务（ETS）和用于ETS国家级实施方案的互连框架》。

[ITU-T M.3342] ITU-T M.3342建议书（2006年），《SLA表示模版的定义指南》。

[ITU-T Y.2012] ITU-T Y.2012建议书（2006年），《下一代网络的功能要求和架构》。

[ITU-T Y.2205] ITU-T Y.2205建议书（2011年），《下一代网络 – 应急通信 – 技术考量》。

3 定义

3.1 其他地方规定的术语：

本建议书使用其他地方定义的下列术语：

3.1.1 authorization授权 [b-ITU-T X800]：权利的授予，包括基于接入权利的接入的授权。

3.1.2 availability可用性 [b-ITU-T X.800]：根据授权实体的要求可接入和可用的属性。

3.1.3 confidentiality机密性 [b-ITU-T X.800]：不向未经授权的个体、实体或进程提供或披露信息的属性。

3.1.4 data integrity数据完整性 [b-ITU-T X.800]：不以未授权方式更改或毁坏数据的属性。

3.1.5 emergency telecommunications service（ETS）应急通信服务 [ITU-T E.107]：指的是一项国家级服务，它在灾难和应急情况下为ETS授权用户提供优先电信服务。

3.2 本建议书规定的术语

本建议书规定下列术语：

3.2.1 Service Provider服务提供商：服务提供商（英文首字母大写）是授权提供ETS的公共电信服务提供商。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

ANI 应用网络接口
CVE 通用漏洞披露（Common Vulnerabilities and Exposures）
CVE 通用漏洞披露（Common Vulnerability and Exposure）
CVSS 通用漏洞评分系统
CWE 常见弱点列表
CYBEX 网络安全信息交换
DDoS 分布式拒绝服务攻击
DNS 域名服务器
DoS 拒绝服务攻击
DSCP 区分服务（Diffserv）代码点
ETS 应急通信服务
IDS 入侵防御系统
IEPS 国际应急优先机制
IP 网际协议
IPS 入侵防御系统
IPsec IP安全性
LAN 局域网
NE 网元
NGN 下一代网络
NNI 网络网络接口
PII 个人可识别信息
PSTN 公共交换电话网
QoS 服务质量
SLA 服务水平协议
SNI 服务网络接口
UNI 用户网络接口

5 惯例

在本建议书中：

本建议书中字头大写的“服务提供商”是指获准提供ETS的公共电信服务提供商（见第3.2.1款）。

关键词“被要求”是指必须严格遵守且如果声明遵守本文件则不能背离的要求。

关键词“推荐”是指建议但非绝对必须的要求。

关键词“禁止”是指必须严格遵守且如果声明遵守本文件则不得背离的要求。

关键词“可选择”是指一项准许的选择性要求，没有任何推荐的意味。该术语并非有意暗示，厂商在落实过程中必须提供选项而且网络运营商/服务提供商能够选择性地激活该特性。相反，这意味着厂商可视情况提供该特性而且仍要求符合规范。

在本建议书的正文和附录中，有时会出现必须、不得、应当和可等词语，在这种情况下可对其分别做出如下解释：“须”、“不得”、“建议”和“视情况可”。附录或材料中出现的，明确标记为告知性的此类词语或关键词要被解释为无规范意图。

6 安全威胁和风险

由于通信的关键性质，ETS通信有可能受到网络安全攻击的威胁。参考[ITU-T E.107]、[ITU-T Y.2205]和[b-ITU-T Q-Sup.57]有关ETS的定义和信息。有意扰乱、滥用、操纵或危害ETS的威胁或恶意行为可能来源于包括互连网络在内的各种来源。例如，ETS可能成为网络安全攻击的目标，因为这些攻击会：

- 破坏灾害恢复人员的通信能力
- 通过窃听ETS呼叫/会话获得机密信息。

一种威胁被视为安全弱点或潜在漏洞，这种弱点如果暴漏有可能对ETS通信的可用性、完整性或机密性造成负面影响。

本建议书主要聚焦与ETS网络互连相关的威胁。有关网络互连的威胁例子包括，但不限于：

- 通用互连威胁：将网络（如NGN）与其他托管和非托管网络如公共互联网相连而造成的安全弱点或潜在漏洞。
- 设计和实施威胁：网络互连架构和实施设计方面的安全弱点或潜在漏洞。
- 管理、运营和内部威胁：在ETS指挥和控制功能及其底层基础设施方面的安全弱点或潜在漏洞。

- 传输和设施威胁：与底层传输网络（如路由选择、网络复制、多样性、弹性）、支撑系统（如能量、环境）和网络资产的实体保护相关的安全弱点或潜在漏洞。

7 ETS互连安全的参考架构

本建议书依靠[ITU-T Y.2012]界定的功能架构和网络互连模型。

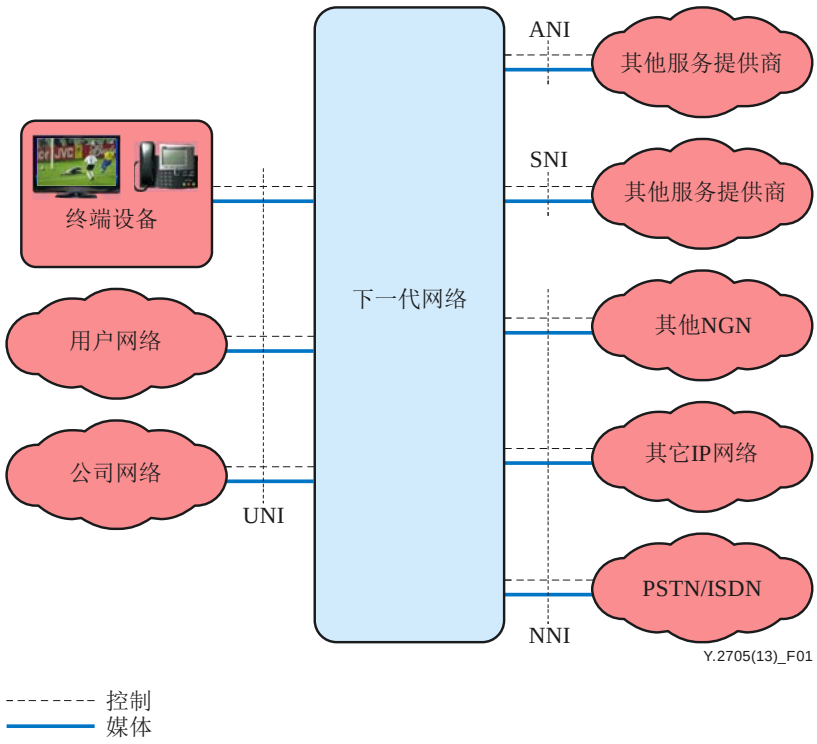


图1 – 连通下一代网络[ITU-T Y.2012]

与网络互连相关的接口是：

- 应用网络接口（ANI）；
- 服务网络接口（SNI）；
- 网络-网络接口（NNI）。

参考[ITU-T Y.2012]有关ANI、SNI和NNI的描述。

为使不同网络支持跨网络边界的ETS，在各个国家网络和国家网络间互连范围内需要采取针对ETS通信完整性、机密性和可用性保护的具体安全措施。

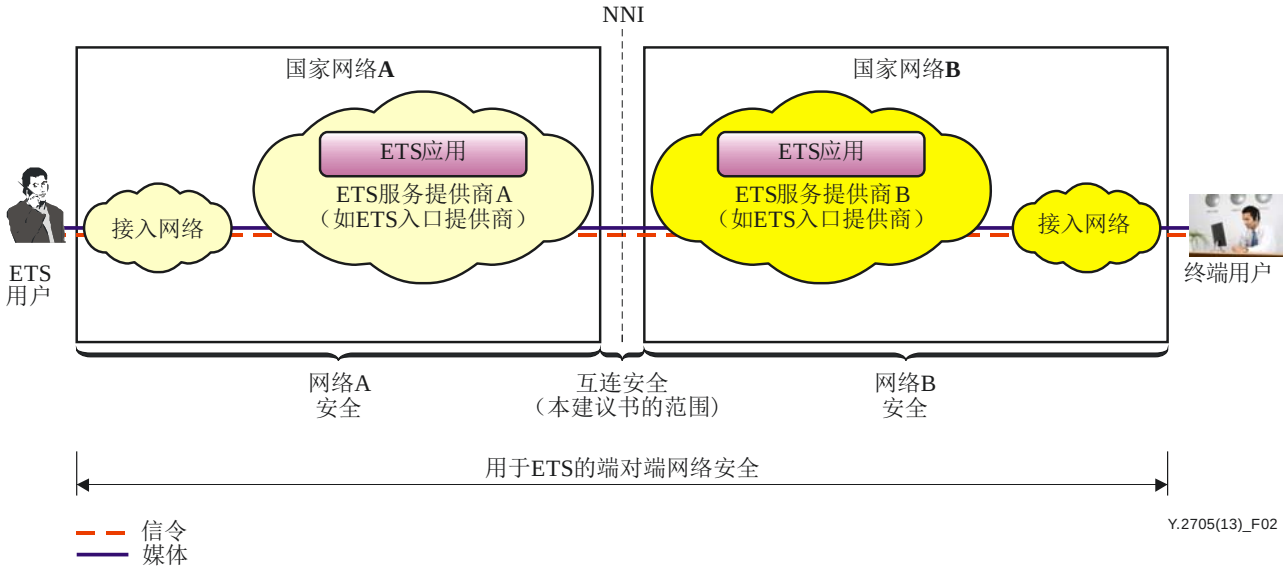


图2 – 适合ETS应用的端对端网络安全

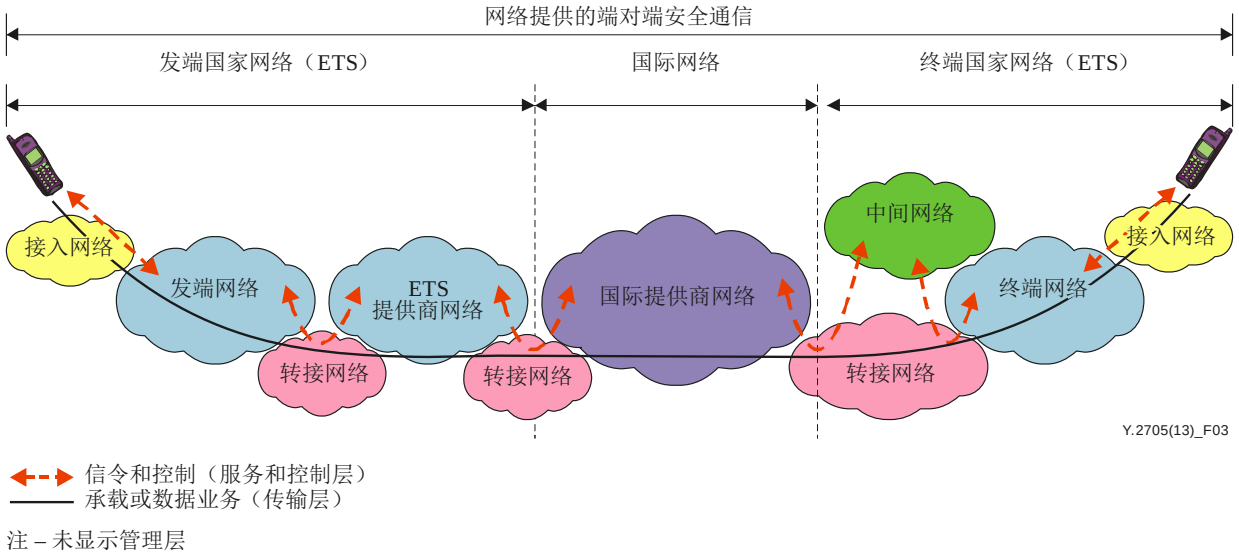
图2示出了穿过多个网络（国家网络A和B）的ETS通信的端对端安全将有赖于在各网络实施的安全措施以及两个网络间互连的安全保护。

图2示出了本建议书的焦点是ETS的安全互连。

8 ETS互连的安全目标和导则

8.1 总体目标

总体目标是提供端对端ETS通信的网络安全保护，这种通信可遍历国内和国际网络（即国家/主管部门）的不同网络提供商网域，其中各个网络在逐跳基础上负责其网域范围内的安全。



注 – 未显示管理层

图3 – 跨不同国家ETS端对端通信的实施案例

图3对发端并终止于两个不同国家网络的端对端ETS通信（如优先级话音、视频、数据或信息通信）进行了举例说明。这个例子说明，ETS端对端优先级通信可能穿越多个网段和管理域（如接入网络、发端网络、ETS 提供商网络、国际提供商网络、中间网络和终端网络）。端对端ETS通信路径上的各个互连网络的总体目标是在其网域内包括与临近网络的互连中提供必要的安全保护，这样不会使端对端ETS通信的完整性、机密性和可用性遭到破坏。

8.2 通用导则

应在ETS互连网络间使用服务水平协议（SLA）建立一种结构性方式方法。这应当包括：

1 安全风险评估：ETS资产的风险评估、威胁及与ETS互连相关的能力分析。关键是定期进行安全风险评估并且当出现变化时，引入新技术、服务或应用。

2 安全架构和解决方案：确定安全政策、安全架构设计和解决方案规范以减轻确定的针对ETS的威胁。这包括确定必要的双边或多边ETS安全SLA（有关SLA信息的ITU-T M.3342]和[b-TMF GB917]建议书）。涉及的方面包括应纳入互连SLA的安全政策、要求、架构设计、态势感知和取证工具以及基础设施安全。

3 安全实施：基于适合ETS互连安全的单边或多边SLA的安全架构和解决方案落实和部署。

4 安全运行：应详细说明并实施对用于ETS互连的安全解决方案进行管理的运作措施。例如，内部威胁管理、可配置参数和默认值管理、回弹和故障恢复操作、ETS安全测试、ETS安全相关事件的记录和审计。

8.3 共同目标和需求

本段描述了共同要求和目标。

R-1 根据可商业化的最佳安全做法，服务提供商应在ETS业务穿越服务提供商网域时，保护ETS通信免遭可能破坏ETS真实性、完整性、机密性和可用性的入侵（如窃听、劫持和重放）。

在上面的要求中，一个网域就是一个实体或逻辑的“网段”，服务提供商在该网段上施加行政和运行控制、管理、维护并确保安全。

预计服务提供商将会支持并使用许多各种不同的安全工具和功能以保护ETS和整个网络及所有获得支持的应用。重要的是，应采取适当措施确保这些安全功能的使用不会对ETS的性能造成负面影响或给ETS安全带来任何意想不到的损害。

R-2 服务提供商对安全机制的使用（如入侵侦测系统和入侵防御系统[IDS/IPS]及加密技术）不应与用来支持ETS的优先处理机制相抵触（参考[ITU-T Y.2205]建议书有关优先处理机制的定义和描述）。

O-1 服务提供商在使用安全工具和功能时采取适当措施将对ETS服务质量（QoS）的负面影响降至最低（如引入不必要的延迟）是可取的。

8.4 ETS身份认证、授权和接入控制

本段包括：

- ETS用户的身份认证和授权
- ETS提供商的ETS用户认证和授权
- ETS数据源的认证。
- ETS提供商的相互认证和授权

8.4.1 相互认证

认证是验证参与某种形式通信的一方所声称身份的过程。认证确保参与通信的实体（如个人、设备、服务或应用）所声称身份的正确性并确保某一实体并非有意对此前的通信进行伪装或未经授权对其重放。

ETS端对端通信可以包括多个网段和管理域（如发端接入网络、ETS服务提供商网络、中间网络、终端接入网络）。当接收ETS业务时，服务提供商需验证接收到的业务的来源（如网络）的有效性和授权。当发送ETS业务时，服务提供商需验证其发送NGN业务（如网络）的实体的有效性和授权情况。目前，只有通过两个互连网络间的直接实体互连才能证实互连安全信任关系。

R-3 服务提供商应相互认证来交换（如发送或接收）ETS业务。这包括跨NNI、ANI或SNI的两个服务提供商之间的任何ETS信令或媒体业务交换。

这可通过直接实体互连和服务水平协议（SLA）的验证完成。

注 – 这里的目的不是在每一个呼叫/会话基础上进行认证。目的是引入机制的概念从而在按需要的基础上或定期进行认证。

8.4.2 接入控制

接入控制措施是必要的，以防未经授权的网络资源使用，包括以未经授权方式使用资源。接入控制确保，只允许授权的用户或设备接入网元、存储的信息、信息流、服务和应用。

在NNI进行的接入控制指的是接收网络接受或拒绝从相邻网络进入的具体业务的能力以及限制网络外实体在网络范围内访问资源的能力。

R-4 服务提供商应确定规则并执行接入控制措施从而防范跨NNI的未经授权ETS通信。具体而言，SP应只允许NE之间已得到确认和事先授权的通信（如通过SLA）。

R-5 当从另一个服务提供商接收ETS信令业务时，服务提供商应验证自身与发送该业务的服务提供商之间的信任关系。

R-6 当从另一个服务提供商接收ETS媒体业务时，服务提供商应验证自身与发送ETS业务的服务提供商之间的信任关系。

R-7 当向另一服务提供商发送ETS信令业务时，服务提供商应验证其发送ETS业务的另一服务提供商的信任关系。

R-8 当向另一服务提供商发送ETS媒体业务时，服务提供商应验证其发送ETS业务的服务提供商的信任关系。

注 – 以上内容并非意在每一呼叫/会话基础上暗示进行验证。

授权是授予权利，包括基于访问权限的授权接入。授权是在经过认证和接入控制过程的验证后给予某一实体的。

R-9 服务提供商须提供安全保护以防止未经授权获取ETS。

可用来完R-9的手段包括，但不限于以下几方面（酌情）：

- ETS最终用户和设备的认证和授权。
- ETS通信数据来源的认证和授权（如，消息源或数据源）。
- 防范未经授权获取ETS信息和资源的安全功能（如认证服务器和管理系统中的用户信息）。

系统接入控制包括防范未经授权接入网元和系统及其相关接入点的安全措施。存在与未获授权接入支持ETS的网元和系统相关的威胁。因此，必须确定并执行适当的防范未经授权接入的接入控制措施。

R-10 服务提供商应确定并执行系统接入控制措施以防范未授权接入支持ETS的网元和系统。这包括逻辑和物理接入的安全保护。

R-11 服务提供商应防范未授权获取ETS数据和资源（即，服务提供商应只允许获授权的主管部门获取有关支撑ETS的网元和系统的ETS数据和资源[如文件、命令集、软件]）。

8.5 ETS完整性

本段包含：

- ETS信令的完整性保护
- ETS媒体的完整性保护。

8.5.1 信令完整性

必须保护网络间ETS信令免遭拦截、误用和操纵（如删除、创造或重播）。

R-12 服务提供商应保护跨NNI、ANI或SNI的所有网络间ETS信令业务的完整性。

可采取行动保护ETS信令业务的完整性，包括但不限于：

a) 实体安全措施（如网元、传输介质和设施的实体保护以及适当接入控制措施的执行）；

b) 密码保护；

c) 服务水平协议界定的适当完整性要求和目标的确定和执行；

d) 监控NNI配置的完整性。

8.5.2 媒体完整性

必须防范网络间ETS通信相关的媒体遭拦截、误用和操纵（如删除、创造或重播）。

R-13 服务提供商应保护所有跨NNI或SNI的网络间ETS媒体业务的完整性。

可以采取行动保护媒体业务的完整性，包括但不限于：

a) 实体安全措施（如网元、传输介质和设施的实体保护以及适当接入控制措施的执行）；

b) 密码保护；

c) 服务水平协议界定的适当完整性要求和目标的确定和执行；

d) 监控NNI配置的完整性。

8.6 ETS通信机密性和PII保护

必须为跨NNI、ANI和SNI的ETS通信提供机密性保护以防范未授权实体获取高度机密信息。这包括以下几方面的机密性保护：

- ETS信令和控制；
- ETS承载业务（如话音、视频或数据）；
- 个人可识别信息（PII）。

8.6.1 信令机密性

服务提供商必须保护跨NNI、ANI或SNI的获得支持的网络间ETS信令免遭未授权接入。必须保护信令信息免遭窃取以减少信令业务分析披露敏感信息从而造成滥用（如呼叫模式、位置信息和用户身份）的可能性。

R-14 服务提供商应保护跨NNI、ANI或SNI的所有网络间ETS信令的机密性。

可采取的保护信令和媒体业务机密性的行动包括，但不限于：

a) 实体安全措施（如网元、传输介质和设施的实体保护以及适当接入控制措施的执行）；

b) 密码保护；

c) 服务水平协议界定的适当机密性要求和目标的确定和执行。

尽管机密性保护通常与加密机制相关，但本段有关提供网络间信令机密性保护的要求并非意味着必须在所有情境中或针对所有端对端信令流时都必须使用加密方法。这一要求的目的是服务提供商必须规定并实施必要的措施以确保保护跨NNI、ANI和SNI信令通信免遭窃取。这意味着根据安全政策的要求，必须检查各个互连以确定用于提供机密性保护的适当机制。例如，有可能通过使用取决于IP互连架构和物理配置（如专用的物理链路场景）的实体性和相关操作提供机密性保护。

8.6.2 媒体机密性

必须保护媒体流（如话音、视频和数据）免遭未授权接入，因为窃听ETS媒体流有可能泄漏敏感安全信息（即在媒体通信中被窃取）。

R-15 服务提供商应保护所有跨NNI或SNI的网络间ETS媒体业务的机密性。

可采取的保护信令和媒体业务机密性的行动包括，但不限于：

a) 实体安全措施（如对网元、传输媒体和设施的实体保护以及适当接入控制措施的执行）；

b) 密码保护；

c) 服务水平协议中适当机密性要求和目标的确定和执行。

8.6.3 PII保护

必须保护与ETS相关的个人识别信息（PII）免遭未授权观察或披露（如ETS最终用户身份、相互通信的实体身份、ETS订购信息以及ETS最终用户位置）。

R-16 服务提供商应允许选择的ETS用户匿名使用ETS。

R-17 服务提供商应保护选择的ETS用户身份的机密性。

R-18 服务提供商应保护选择的ETS用户位置的机密性。

需要保护ETS使用信息（如ETS业务量、位置、时间、频率等使用模式）免遭未授权监视。这包括支持并使用安全功能以保护从网络活动观测中得到的敏感信息，如某一最终用户访问的网站、某一最终用户的地理位置以及服务提供商网络中设备的域名服务器（DNS）名称和IP地址。

O-2 服务提供商保护ETS使用信息（如观测某一ETS用户一直访问的网址、ETS用户IP地址等网络活动，或ETS业务量、位置、时间、频率等使用模式）免遭未授权观测或披露是可取的。

8.7 网间IP传输

8.7.1 概述

两个服务提供商之间的IP到IP互连将具备含有不同安全意义的架构和物理连接变化。

两个服务提供商间IP到IP互连的完整性和可用性将取决于诸如架构、物理互连和服务水平协议等因素。

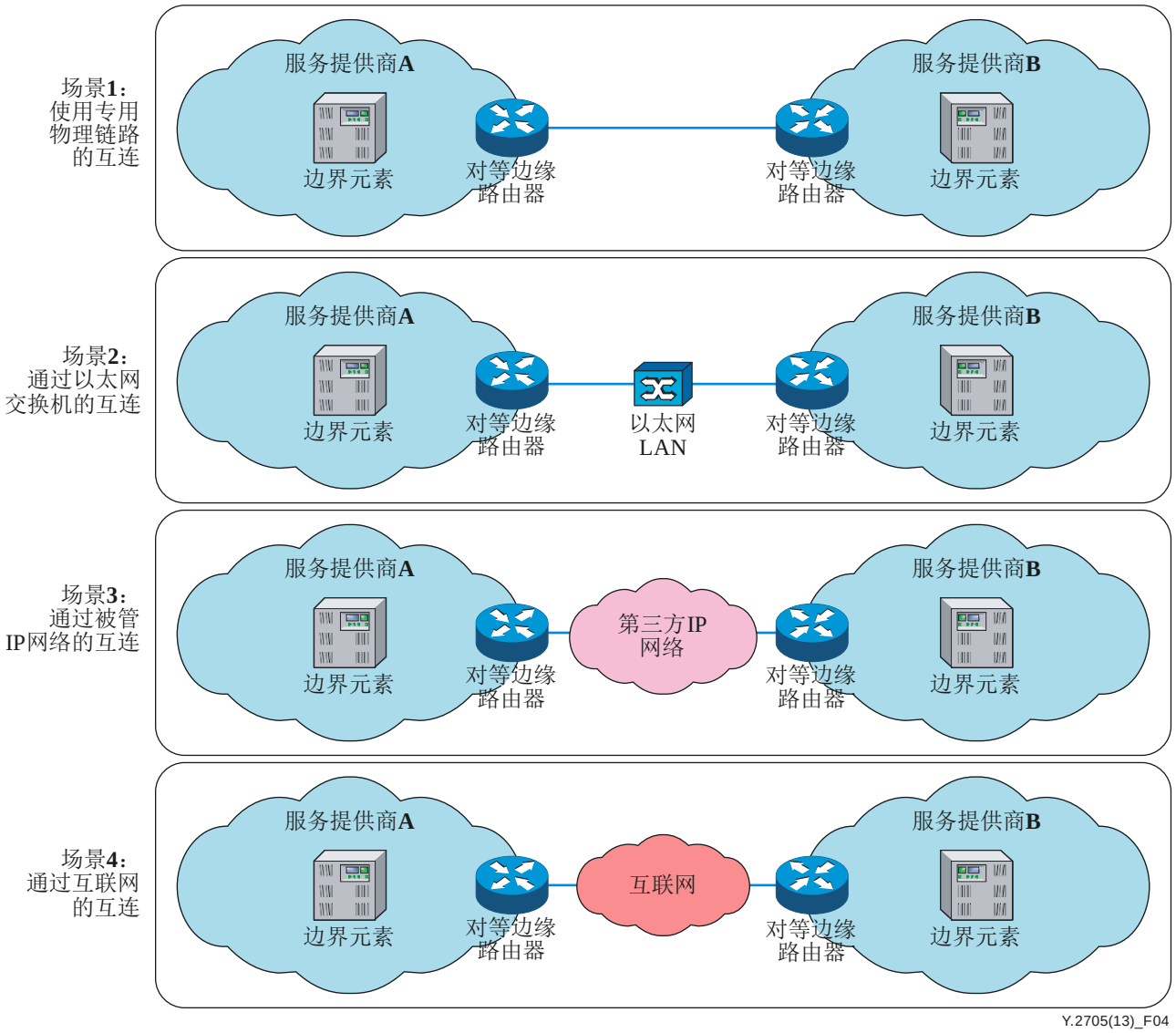


图4 – IP到IP互连配置

图4展示了一套可能的IP到IP互连配置：

1 使用专用物理链路的互连：在这一配置中，用某一专用的物理链路连接服务提供商A对等边缘路由与服务提供商B的对等边缘路由。

2 通过一个以太网交换机进行的互连：在这一配置中，服务提供商A的对等边缘路由和服务提供商B的对等边缘路由在物理上通过一个局域网（LAN）以太交换机实现连接。

3 通过一个受管理的IP网络进行的互连：在这一配置中，服务提供商A与服务提供商B之间的IP互连经由一个受管理的IP网络实现。这个IP网络可以是第三方提供商管理的IP网络。

4 通过互联网实现的互连：在这一配置中，服务提供商A与服务提供商B之间的IP互连通过开放的互联网实现。

图4描述了各种场景下不同的ETS安全影响。

在本文件中没有对用于实现服务提供商互连的IP互连做出规定或限制。总体目标是服务提供商有义务基于具体的IP到IP配置支持和实施适当的安全措施以保护互连并防止因IP互连的受损而对服务造成影响。

R-19 服务提供商应根据可商业化的最佳安全做法，保护两个互连服务提供商网络之间的IP传输网络免遭有可能损害ETS可靠性、完整性、机密性和可用性的入侵（如拦截、劫持和重放）。

为满足这一要求，服务提供商应确定并执行保护互连服务提供商网络间IP传输网络的规则，并将这些规则记录在SLA中。

R-20 服务提供商应保护所使用IP业务优先机制、功能和相应协议数据（如Diffserv代码点）的完整性以支持服务提供商间通过IP网络互连提供的ETS。

注 – 这包括任何ETS相关配置数据或IP互连相关参数以及涉及的任何映射关系（如基于单个互连服务提供商正在使用的方案建立的DiffServ代码点映射关系）的完整性保护。

CR-1 如果ETS信令正穿过一个不受信任的IP传输网段（如第三方IP传输），服务提供商应使用加密（如IPsec）以保护完整性和机密性。

CR-2 如果ETS媒体正穿过一个不受信任的IP传输网段（如第三方IP传输），服务提供商应使用加密（如IPsec）以保护完整性和机密性。

8.7.2 加密的使用

安全机制的使用（如加密）不应干涉或遮掩适用于优先处理机制的信息。

在将IPsec隧道用于网间ETS业务（即跨NNI、ANI和SNI）时适用下列要求：

R-21 在将IPsec隧道用于网间ETS业务时，服务提供商应确立并执行填充并保护优先信息（如DSCP值）完整性的规则。具体而言，应在SLA中明确从附加信息头协议中得出的diffserv代码点（DSCP）值如何填充进Psec入口点IPsec隧道头协议中的规则并执行这一规则以实现入口和出口IPsec点之间的优先处理。

8.8 ETS可用性

8.8.1 总体目标

为确保提高ETS的可用性，各个服务系统（支撑ETS）的故障必须维持在较小程度上，而且服务恢复必须是迅速的（一旦出现服务终端或故障）。应在ETS整体可用性规划和设计中考虑安全性遭破坏造成的故障。以下是安全环境中ETS可用性的总体目标：

O-3 由于安全事件影响网络间互连，服务提供商在ETS端对端服务可用性（即穿越多个服务提供商网络的ETS呼叫/会话）的总体规划和设计时考虑可能出现的故障或服务中断是可取的。这包括从安全事件造成的故障中快速恢复的措施。

8.8.2 可用性保护

必须保护ET免遭拒绝服务（DoS）攻击、分布式拒绝服务（DDoS）攻击和可能影响ETS可用性的其他类型攻击。这包括保护免遭影响ETS个体用户、某一ETS群体用户、特定位置或网址ETS用户（如政府机构企业网络站点）、目标地域或区域ETS用户或作为整体的ETS的ETS可用性的攻击。

R-22 服务提供商应根据可商业化的最佳安全做法保护ETS的可用性（如，保护免遭DoS、DDoS和其他类型影响ETS可用性的攻击）。这应当包括保护免遭影响ETS个体用户、某一ETS群体用户、特定位置或网址ETS用户（如政府机构企业网络站点）、目标地域或区域ETS用户或作为整体的ETS的ETS可用性的DoS、DDoS和其他类型攻击。

可采取的保护ETS可用性的行动包括但不限于：

a) 接纳控制和节流机制的使用；

b) DoS和DDoS 缓解工具和功能；

c) 入侵监测系统和入侵防御系统（IDS/IPS）的使用；

d) 安全监控工具的使用；

e) 态势感知工具的使用。

R-23 服务提供商对保护可用性的安全工具和功能的使用（如DoS和DDoS机制）应包括预防合法ETS呼叫/会话遭意料外拒绝的适当措施（如阻塞或妨碍完成某一合法ETS呼叫/会话或丢弃合法的ETS包）。

8.9 管理和运行安全

本段包含与以下几方面相关的一些主题：

- 管理操作的安全性（如与ETS互连的提供相关的可配置和默认参数），
- ETS安全相关事件的记录，
- 当安全漏洞已经出现或可能已经出现时发出的警报和警告。

8.9.1 ETS数据完整性

必须为存储的ETS数据提供完整性保护以防误用或操纵数据，影响ETS完整性或可用性。

R-24 服务提供商应保护ETS供应数据的完整性。这包括各种ETS具体数据，如供应的订购数据。

8.9.2 可配置参数和默认值

有许多与厂商与设备供应商设定的默认值和可配置参数管理相关的安全威胁。例如，必须调整厂商交付的各种可配置参数的默认值，以满足服务提供商的要求。必须适当地分配并持续更新可配置参数从而使其能够令人满意地发挥作用。必须适当地对这一行政主管部门进行授权以进行安全管理。

R-25 服务提供商须确立并执行在支持ETS环境中管理可配置参数及其默认值的规则。应实施并强制执行接入控制措施，因此这些功能的执行只能留给授权主管部门（即，所有其他用户应无法得到这一许可）。

8.9.3 内部威胁的管理

某一个体（如一位雇员、承包商或其他工人）也许能够在未经授权情况下得到管理权限或滥用他们的管理权进入支撑ETS的网元和系统。因此，需要将内部威胁最小化。

R-26 服务提供商应确立并执行最小化ETS内部威胁的过程。

可考虑的缓解方法包括：

- 用于远程、控制台、工艺和自动系统访问的认证控制、基于角色的特权、功能分离及安全的访问方式；
- 与管理行动相关的安全事件的记录；
- ETS信息、应用和共享系统和应用访问的分隔；
- 为记录并暴露未经授权的改变而对网元和数据库配置数据（如订购配置文件）进行的审计。

8.9.4 网络安全信息交换方面的合作

服务提供商应与合作伙伴建立协作关系，分享网络安全事件相关信息（包括网络安全攻击期间的实时信息交换）。有关网络安全事件的信息的一次交换能够实现双方互惠互利并可用于预见ETS威胁，使服务提供商处于提供有效对策的位置。

O-4 服务提供商确立并实施足以建立共享和交换网络安全事件相关信息的协作关系的管理和运作流程是可取的。该流程应考虑分析功能从而使这些信息用作安全行动的输入意见和保护ETS的应对措施。

请参考下列ITU-T建议书了解有关网络安全信息交换的信息：

- [b-ITU-T X.1500]
- [b-ITU-T X.1500.1]
- [b-ITU-T X.1520]
- [b-ITU-T X.1521]
- [b-ITU-T X.1524]
- [b-ITU-T X.1570]

8.9.5 安全事件反应和恢复的管理

ETS的可用性取决于用于从安全事件中恢复和复原恢复的适当运作程序。至关重要的是要清晰地界定、存档和实施这些程序。这包括在服务提供商网域内以及针对互连和网络间服务的跨域范围内用于服务恢复和复原的必要政策和做法。保护运作程序存档和实施免遭入侵和内部威胁是必要的。

R-27 服务提供商须有一个存档备查的描述从安全事件中恢复和复原服务的政策、管理、运作步骤、过程和程序的响应与恢复计划。这包括服务提供商网域和针对互连与网络间服务的跨网域范围内用于服务恢复和复原的必要政策和做法。

参考资料

[b-ITu-T Q-Sup57] ITU-T Q系列建议书增补57（2008年），《支持IP网络中应急通信服务的信令要求》。

[b-ITU-T X.800] ITU-T X.800建议书（1991年），《适合CCITT应用的开放系统互连的安全架构》。

[ITU-T X.1500] ITU-T X.1500建议书（2011年），《网络安全信息交换综述》。

[b-ITU-T X.1500.1] ITU-T X.1500.1建议书（2012年），《用于网络安全信息交换的对象识别符弧的注册程序》。

[b-ITU-T X.1520] ITU-T X.1520建议书（2011年），《通用漏洞披露》

[b-ITU-T X.1521] ITU-T X.1521建议书（2011年），《通用漏洞评分系统》

[b-ITU-T X.1524] ITU-T X.1524建议书（2012年），《常见弱点列表》

[b-ITU-T X.1570] ITU-T X.1570建议书（2011年），《网络安全信息交换的发现机制》

[b-TMF GB917] GB917（2012年），《SLA管理手册》，3.1版，TM论坛

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	终端和主观与客观评估方法
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、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2013年，日内瓦