ICS 35.100.40
L 79

中华人民共和国国家标准

GB/T 18231—2000
idt ISO/IEC TR 13594:1995

信息技术　低层安全模型

Information technology—Lower layers security model

2000-10-17 发布　　2001-08-01 实施

国家质量技术监督局　发布

目　　次

前言 …… Ⅲ
ISO/IEC 前言 …… Ⅳ
引言 …… Ⅴ
1　范围 …… 1
2　引用标准 …… 1
3　定义 …… 2
4　缩略语 …… 2
5　安全联系 …… 3
6　对现存协议的影响 …… 5
7　公共安全 PDU 结构 …… 5
8　安全服务和机制的确定 …… 6
9　保护 QoS …… 6
10　安全规则 …… 6
11　低层中安全的放置 …… 6
12　为提高(N)层安全而使用的(N－1)层 …… 10
13　安全标记 …… 10
14　安全域 …… 11
15　路由选择安全 …… 11
16　安全管理 …… 11
17　通信流量保密性 …… 12
18　SA 属性定义的准则 …… 12
19　差错处理 …… 12
附录 A(提示的附录)　安全规则商定集示例 …… 13

前　言

本标准等同采用国际标准 ISO/IEC TR 13594:1995《信息技术　低层安全模型》。

为适应信息处理的需要，本标准依据 OSI 参考模型的层次结构，它描述了这些层公共体系结构概念、与层间安全有关的交互作用的基础和低层中安全协议的放置。在制定标准时，根据正文内容，在引用标准中增加了两项标准。本标准在技术内容上与国际标准保持一致。

本标准的附录 A 是提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位：西安交通大学。

本标准主要起草人：邓良松、冯惠、邓勇。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术领域,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。

技术委员会的主要任务是制定国际标准,但在特殊情况下技术委员会可以建议以下类型之一的技术报告的出版:

——类型 1,当经多次努力,仍得不到出版国际标准所需要的支持时;

——类型 2,当主题仍处于技术开发,或者由于其他某原因,存在将来而非即刻就国际标准达成协议的可能性时;

——类型 3,当技术委员会从正式出版(例如,"最新出版")的国际标准中已收集了不同种类的数据时。

类型 1 和 2 的技术报告在出版后三年内应该经受复查,以决定它们是否能被转换为国际标准。类型 3 的技术报告没有必要复查直到它们提供的数据被认为不再有效或有用。

ISO/IEC TR 13594 是类型 3 的技术报告,它由联合技术委员会 ISO/IEC JTC 1"信息技术"与 ITU-T 合作制定。相同的文本作为 ITU-T 建议 X.802 出版。

引　言

本标准描述了在OSI参考模型低层(运输、网络、数据链路和物理层)中提供安全服务的跨层的内容。它描述了这些层的公共体系结构概念、与层间安全有关的交互作用的基础和低层中安全协议的放置。

中华人民共和国国家标准

信息技术　低层安全模型

GB/T 18231—2000
idt ISO/IEC TR 13594:1995

Information technology—Lower layers security model

1　范围

本标准描述了在OSI参考模型低层(运输、网络、数据链路和物理层)中提供安全服务的跨层的内容。

本标准描述:

a) 基于GB/T 9387.2中定义的低层公共的体系结构概念;

b) 低层协议之间与安全有关的交互作用的基础;

c) OSI的低层和高层之间与安全有关的任何交互作用的基础;

d) 与其他低层安全协议有关的安全协议的放置以及这种放置的有关作用。

在低层安全协议和本标准中描述的模型之间不应该存在冲突。

GB/T 16264.1标识了与OSI参考模型的每个低层有关的安全服务。

2　引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.1—1998　信息技术　开放系统互连　基本参考模型　第1部分:基本模型(idt ISO/IEC 7498-1:1994)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 15274—1994　信息处理系统　开放系统互连　网络层的内部组织结构(idt ISO 8648:1988)

GB/T 16262—1996　信息处理系统　开放系统互连　抽象语法记法一(ASN.1)规范(idt ISO/IEC 8824:1990)

GB/T 16263—1996　信息处理系统　开放系统互连　抽象语法记法一(ASN.1)基本编码规则规范(idt ISO/IEC 8825:1990)

GB/T 16264.1—1996　信息技术　开放系统互连　目录　第1部分:概念、模型和服务的概述(idt ISO/IEC 9594-1:1990)

GB/T 16723—1996　信息技术　提供OSI无连接方式运输服务的协议(idt ISO/IEC 8602:1995)

GB/T 16974—1997　信息技术　数据通信　数据终端设备用X.25包层协议(idt ISO/IEC 8208:1995)

GB/T 17179.1—1997　信息技术　提供无连接方式网络服务的协议　第1部分:协议规范(idt ISO/IEC 8473-1:1994)

GB/T 17180—1997　信息处理系统　系统间远程通信和信息交换　与提供无连接方式的网络服务协议联合使用的端系统到中间系统路由选择交换协议(idt ISO/IEC 9542:

国家质量技术监督局2000-10-17批准　　2001-08-01实施

1988)

GB/T 17963—2000 信息技术 开放系统互连 网络层安全协议(idt ISO/IEC 11577:1995)

GB/T 17965—2000 信息技术 开放系统互连 高层安全模型(idt ISO/IEC 10745:1995)

ISO/IEC 8073:1992 信息技术 系统间远程通信和信息交换 开放系统互连 用于提供连接方式运输服务的协议

ISO/IEC 9979 数据加密技术 加密算法的登记规程

ISO/IEC 10181-1 信息技术 开放系统互连 开放系统中的安全框架:安全框架概述

ISO/IEC 10181-3 信息技术 开放系统互连 开放系统中的安全框架:访问控制框架

ISO/IEC 10589:1992 信息技术 系统间远程通信和信息交换 与提供无连接方式网络服务协议(ISO 8473)一起使用的中间系统到中间系统域内路由选择信息交换协议

ISO/IEC 10736:1995 信息技术 系统间远程通信和信息交换 运输层安全协议

ISO/IEC 10747:1994 信息技术 系统间远程通信和信息交换 为支持转发 ISO 8473PDU 在中间系统之间交换域内路由选择信息的协议

3 定义

3.1 OSI 参考模型定义

本标准采用 GB/T 9387.1 中定义的下列术语:

——服务质量 quality of service

3.2 开放系统安全框架定义

本标准采用 ISO/IEC 10181-1 中定义的下列术语:

——安全域 security domain

3.3 网络层内部组织结构定义

本标准采用 GB/T 15274 中定义的下列术语:

a) 子网访问协议 subnetwork access protocol;

b) 端系统 end system;

c) 中间系统 intermediate system。

3.4 附加定义

本标准采用下列定义:

3.4.1 转向保护 reflection protection

当协议数据单元已被返回原发者时用于检测的保护机制。

3.4.2 安全联系属性 security association attributes

为了控制一个实体与其远程对等实体之间的通信安全所需要的信息汇集。

3.4.3 安全联系 security association

存在相应安全联系属性的低层通信实体之间的关系。

3.4.4 安全规则 security rules

本地信息,给定所选择的安全服务规定了要使用的低层安全机制,包括该机制的操作所需要的所有参数。

注:安全规则是如高层安全模型 GB/T 17965 中定义的安全交互作用规则的形式。

4 缩略语

ISN	完整性顺序号
SSAA	SA 属性集

NLSP	网络层安全协议
NLSP-CO	连接方式 NLSP
NLSP-CL	无连接方式 NLSP
QoS	服务质量(如 GB/T 9387.1 中定义)
SA	安全联系
SA-ID	安全联系标识符
SNAcP	子网访问协议(如 GB/T 15274 中定义)
SNISP	独立于子网安全协议
TLSP	运输层安全协议

5 安全联系

5.1 概述

5.1.1 任何安全协议都利用许多安全机制为上层提供安全服务。高层所要求的安全服务可以通过使用本地安全管理功能被指明给低层。安全协议及它的每个安全机制要求除 PDU 中编码的信息之外的信息能够安全通信。这种附加信息的例子有协议将要使用的机制的规范以及每个机制的特定信息,诸如加密机制所要求的密钥信息。每条附加信息被看作为安全联系属性。

5.1.2 安全联系属性可以使用许多机制放置于协议实体中。一些放置机制的例子是:

a) 设备制造期间放置;

b) 设备初始化期间放置;

c) 通过手动接口(如面板控制)放置;

d) 由 OSI 系统安全管理放置;

e) 由 OSI 层安全管理放置;

f) 由 OSI 操作安全管理放置。

5.1.3 SA 属性可以在与它们有关的通信前的任何时候放置。当相容的 SA 属性集(SSAA)放置到每一个协议实体中的相应位置时,一个安全联系就存在于协议实体之间了。

5.1.4 SSAA(和安全联系)可以以不同的粒度存在。有时候能引用具有不同粒度的 SSAA 是有用的。例如,由安全规则商定集(ASSR)定义的 SSAA 能以 SSAA ASSR 表示。或者可以在两个协议实体之间建立配对密钥以用于许多公共的源目的地址对实例。类似的,用于某一通信实例的 SSAA 能由通信的 SSAA 实例引用。同样,用于面向连接 PDU 的 SSAA 能由 SSAA CO PDU 引用。

5.1.5 通常,SA 属性必须通过安全手段放置于协议实体中以维护安全。这隐含 SA 属性或者使用物理安全手段放置,或者可以利用一个现有的、为此而预先放置的安全联系来放置。

5.1.6 属于安全联系一部分的 SSAA,经常由一个具有本地意义并认为是 SA-ID 的标识符引用。在任何时刻,SA 属性集的一些成员可以无定义。典型的是在一个安全通信的初始化期间,SSAA 将不会完全在其中,同时在用户数据交换前,初始交换将被用来完整地放入 SSAA 中。

5.1.7 为了提供重播保护,必须对 SA-ID、它们引用的 SSAA 和 SA 属性的使用加以限制。

a) SA-ID 不可以以相同的加密密钥重用;

b) 当任何 SA 属性已放入到由 SA-ID 引用的 SSAA 中后,除非安全协议有某种方法示意通信实体之间的改变,否则该 SA 属性不应被改变。这隐含了为使密钥能换用,必须以旧 SA 属性的拷贝及一个新密钥来使用新的 SA-ID,除非安全协议有一个示意密钥改变的替换办法(例如,由 NLSP-CO CSC PDU 支持)。

5.1.8 从 SSAA 中去除任何 SA 属性将有效地关闭安全联系。

5.1.9 一些 SA 属性对于通信实例(无连接 PDU 或连接)具有重要意义。其他 SA 属性对连接上的单个 PDU 具有重要意义。完整性顺序号和安全标记是这样的 SA 属性的例子。它可以表现为这些 SA 属

性的改变违反了上述 5.1.7b)中的限制。然而，逻辑上包括这些 SA 属性的安全联系，仅在单个 PDU 的生命期中有效。ISN 成为 SA-ID 的一个逻辑扩展，从而改变了有效的 SA-ID。标记仅对扩展的 SA-ID 实例有效。因此，那些限制得以维护。这些 SA 属性有时称为“动态”SA 属性。

5.1.10 部分安全策略将限制协议实体的操作。这部分安全策略称为“协议实体的安全规则集”。协议实体的安全规则集可以限制诸如要使用的安全机制和 SA 属性的值与放置机制之类的事情。安全规则集也将定义所选择的安全服务映射到安全协议所用的安全机制。安全规则集是安全交互作用规则的一种形式。

5.1.11 当用于域内或域间操作时，对于该安全规则集需要建立一个唯一标识符并被称为安全规则商定集。ASSR 标识符可以作为安全联系建立的一部分被交换，以此定义或限制在安全规则集中定义的 SSAA ASSR。其余的 SA 属性，如果有的话，必须使用上述 5.1.2 中所列的其他方法建立。

5.2 为低层建立安全联系

5.2.1 为了保护通信实例(无连接 PDU 或连接)，必须在通信实体之间建立安全联系。

5.2.2 形成的 SA 信息要么是静态信息，它在 SA 建立时可以“协商”，然后在联系存在期间保持不变，要么是动态信息，它可在通信实例中被更新。

5.2.3 作为 OSI 的 1 层至 4 层协议，通过安全联系协议数据单元(PDU)的交换或 OSI 低层范围之外的机制来建立一个 SA。

5.2.4 在建立 SA 前，每个实体必须预先建立一个公共的、相互商定和唯一标识的安全规则集以及可以被选择的安全服务。

5.2.5 如果 SA 是通过安全联系 PDU 的交换来建立，那么下列内容也必须预先建立：

a) 安全服务的初始选择以及建立 SA 时要应用的安全机制；

b) 建立 SA 所需的基本定密钥信息。

5.2.6 建立 SA 时，实体建立下列与其远程对等实体共享的信息，该远程对等实体在联系的生命期必须保持不变(即静态)：

a) 本地和远程 SA-ID；

b) 用于通信实例的联系实体之间的所选择的安全服务；

注：要使用的安全服务可以在预先建立的安全服务中选择。

c) 通过所选择的安全服务隐含将要使用的机制及其特性；

d) 用于通信实例的完整性、加密机制和鉴别的初始共享密钥；

e) 为访问控制而在本联系上使用的安全标记与地址集。

5.2.7 SA-ID 和共享密钥[上述 a)和 d)项]必须基于每一个联系来建立。其他信息可以预先建立。另外，作为建立 SA 的一部分，远程对等实体的身份必须被鉴别以提供对等实体鉴别。

5.2.8 可为通信实例动态地更新下列信息：

a) 每个方向的正常和加速数据所需的完整性顺序号；

b) 从静态安全标记集中动态地选择安全标记；

c) 用于安全协议中加密/完整性机制的重密钥信息，该安全协议支持联系内的重新定密钥(例如，连接方式网络层安全协议)。

5.2.9 为获得对等实体鉴别或数据原发鉴别，每一通信实例都需要应用鉴别机制。

5.2.10 可以在安全联系的不同阶段建立不同的 SA 属性，如图 1 所示。前面条目中描述的有关安全联系使用预先建立项、静态项和动态项。所使用的项和鉴别形式如前面条目中描述的那样。

5.2.11 实体将识别使用 SA-ID 的必要 SA 属性。

5.2.12 SA 应在保护通信实例前建立。

预先建立	静　态	动　态
安全规则商定集 可能的安全服务 初始安全服务 基本密钥信息	SA-ID 初始密钥 鉴别	ISN 安全标记 重密钥信息 鉴别
选择保护 QoS 的级 选择的机制 安全标记/地址集		

图 1　安全联系的属性说明

5.3　安全联系关闭

当 SA 不再有效时，关闭由 SA-ID 指明的 SA。

安全联系能用下列方法关闭：

a）作为 OSI 的 1 层至 4 层协议，通过安全联系协议数据单元(PDU)的交换；

b）使用 OSI 低层范围之外的外部机制；

c）用关闭一个连接(该方法仅对连接方式适用)而隐式关闭；

d）当一个密钥处于 SA 期满时而隐式关闭。

注：因为每一个对等实体中可以产生显著差异的值，方法 d)具有由对等实体间传送/接收数据包数目定义的密钥生存期，因此，使用方法 d)应谨慎。在使用上述 c)方法前，安全联系的属性必须指明本联系将通过关闭使用该联系的连接而关闭。

5.4　连接中的属性的修改

对于每一通信实例(无连接 PDU 或连接)，只能建立一个 SA。

在连接存在期间，用于该连接的安全服务和机制不能被修改(注意，这并不排斥改变密钥)。

新密钥的使用指示应由安全协议描述。

6　对现存协议的影响

6.1　总则

原则上，安全协议对现存协议的影响应为最小。

6.2　无连接 SDU 大小

在数据传送期间，根据所选择的安全机制，安全对于(N)层协议有下列影响：

a）(N)用户数据以及某些情况下(N)协议控制信息由运输前后的密码变换来操作。这样可能改变(N)用户数据的长度；

b）与(N)用户数据有关的协议控制信息(例如安全联系标识符、密码检验代码)可能需要由(N)协议携带。

注：这将对由 GB/T 15126—1994 的 15.2.3 及 GB/T 12453—1990 中定义的最大用户数据大小有影响。

6.3　PDU 的链接

只有在相同安全联系下被保护的 PDU 才可以被链接。

6.4　算法和机制独立性

低层安全协议被规定为独立于算法。而且，NLSP 已采用把安全协议分为依赖于机制部分和独立于机制部分的方法。预计将来的低层安全协议可以通过将通用抽象服务用于 OSI 的高层和低层公共安全来达到这一点。

7　公共安全 PDU 结构

7.1　公共的一般 PDU 结构将用于在低层安全协议中保护数据 PDU。虽然一般 PDU 结构对于所有低层安全协议是相同的，但这些低层安全协议却由于不同原因而不同，其中最主要的原因则是由特定的协

议层所施加的格式限制。

7.2 低层安全协议中 PDU 结构的公共部分可以是：

a) PDU 尾部的完整性检验值(ICV)(除任何加密填充外，见下面)；

b) 为实现通信流量保密性、完整性和加密机制所进行的填充可以放置于个别的字段内；

c) 顺序完整性使用的可变长数目；

d) 使用类型/长度/值的字段的灵活编码方法，该方法允许容易扩展并给予字段顺序的限制最小；

e) 由被保护 SA 的启动者对响应者方向标志提供的转向保护。

8 安全服务和机制的确定

安全协议要应用的安全服务如第 9 章中描述的那样来确定。给定选择的安全服务，通过使用第 10 章中描述的安全规则来确定要应用的安全机制。

9 保护 QoS

保护 QoS 是指服务提供者试图使用那些应用于低层的安全服务来防御安全威胁的程度。

保护 QoS 服务参数的处理是根据有效的安全策略来控制的本地事情。保护 QoS 不在服务用户之间协商。对于通信实例，服务用户可以向服务提供者指明其保护 QoS 要求。服务提供者可以指明在通信实例中提供给服务用户的保护 QoS。服务提供者提供的保护 QoS 不必和服务用户要求的相同。

开放系统之间传送有关被选择的安全服务信息的任何低层协议交换(指“带内”协议交换)，在独立于通信实例的安全联系协议内进行。这可以通过安全标记隐式进行，也可以通过其他方法显式进行。

10 安全规则

给定选择的安全服务，安全规则规定了要使用的安全机制，包括该机制操作所需的所有参数。可以被登记为团体使用的安全规则例子的说明在附录 A 中给出。

由安全标记隐含选择的安全服务的情况下，安全规则也规定了从安全标记到所隐含的保护要求的映射。

注：目前，GB 没有将安全规则标准化。

11 低层中安全的放置

为了在运输层和网络层中的使用，当前定义了安全协议[运输层安全协议(TLSP 见 ISO/IEC 10736)和网络层安全协议(NLSP)]。

对于连接方式通信，TLSP 与 ISO/IEC 8073 连同运行(见图 2)。对于无连接方式通信，TLSP 与 GB/T 16723 连同运行(见图 3)。

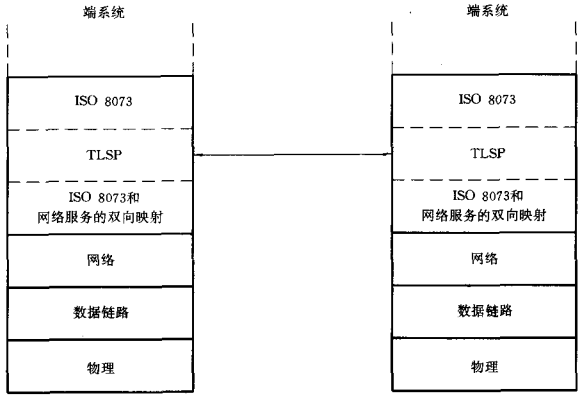


图 2　TLSP 与 ISO/IEC 8073 连同运行的说明

网络层中的安全可以由独立于子网安全协议(SNISP)提供,除了 GB/T 15274 中标识的任务外该 SNISP 完成独立于子网安全任务。下面描述中,对如像 NLSP 的 SNISP 和提供其他网络层协议任务(如 GB/T 15274 中标识)的协议之间的不同关系,存在许多选项。

对于端系统之间的无连接方式通信,NLSP 能运行在"正常"网络层协议之上。如图 4 所示,这样保护了网络服务数据单元。

另外,对于两个端系统之间、端系统和中间系统之间或两个中间系统之间的无连接方式通信,NLSP 运行在无连接网络协议(见 GB/T 17179.1)之下以及在子网收敛协议或者 GB/T 17179.1 之上。这在图 5 和图 6 中说明。两个 GB/T 17179.1 层和一个 NLSP 层的表示不必隐含分隔的协议机。这依赖于本地实现策略。这样保护了网络协议数据单元。

对于连接方式通信,NLSP 总是运行在独立于子网协议或者如 GB/T 16974 那样的子网访问协议之上。这在图 7、图 8 和图 9 中说明。这样保护了网络服务数据单元。NLSP 不必定位在网络层顶部。

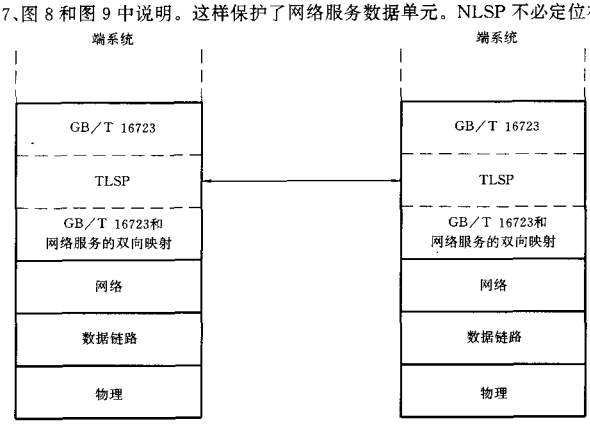


图 3　TLSP 与 GB/T 16723 连同运行的说明

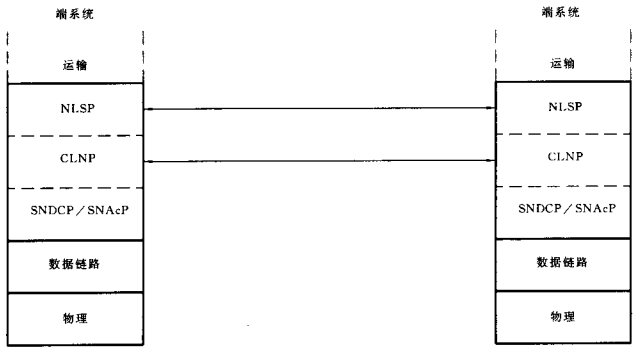


图 4　端系统之间的 NLSP-CL 的说明

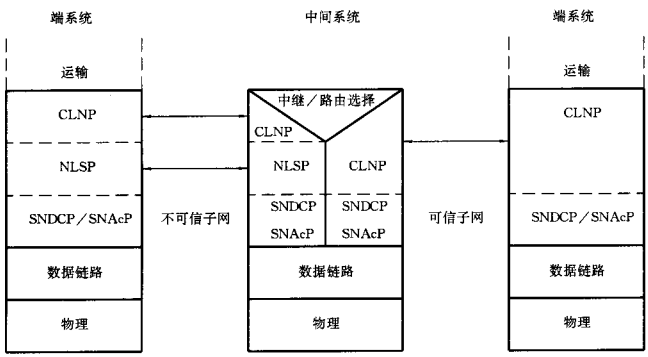


图 5　具有不可信子网的 NLSP-CL 的说明

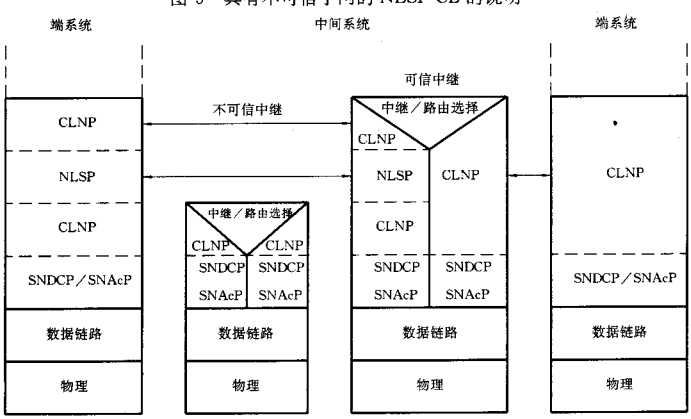


图 6　具有不可信中继系统的 NLSP-CL 的说明

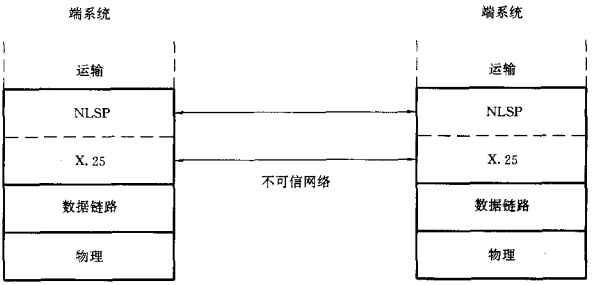


图 7 端系统之间的 NLSP-CO 的说明

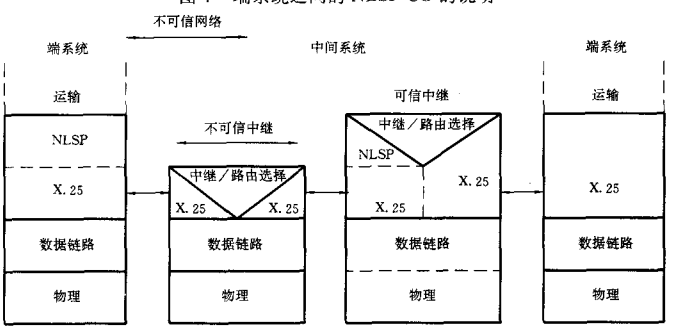
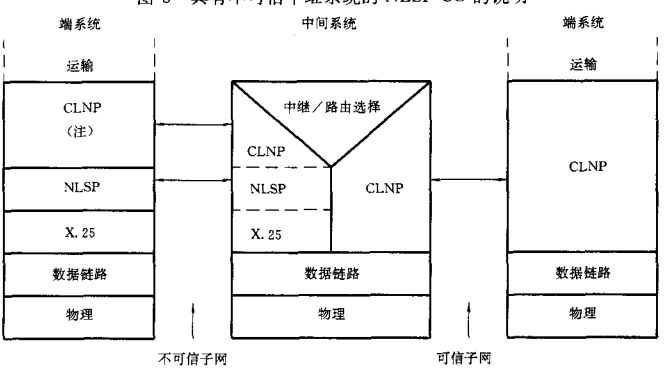


图 8 具有不可信中继系统的 NLSP-CO 的说明



注：这包括对 CO 方式的收敛功能。

图 9 多网络环境中的 NLSP 的说明

没有包括在该模型中的其他放置也是可能的。

域间路由选择协议(IDRP)(ISO/IEC 10747)交换可利用 NLSP 在 IDRP 之下以及 GB/T 17179.1 之上的运行(见图 10)得以保护。这样保护了 IDRP 协议数据单元。

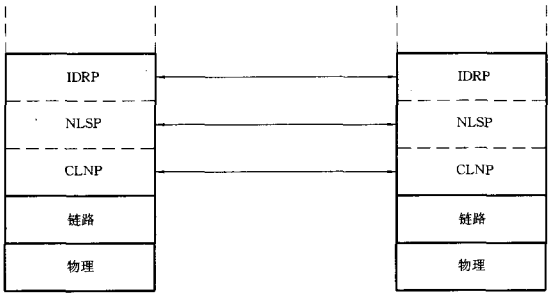


图 10　与 IDRP 连同运行的 NLSP 的说明

为了使用定义于 GB/T 15629 中的局域网(LAN)协议那样的链路层协议，可以定义 NLSP 低层网络服务原语到数据链路服务的映射(见图 11)。

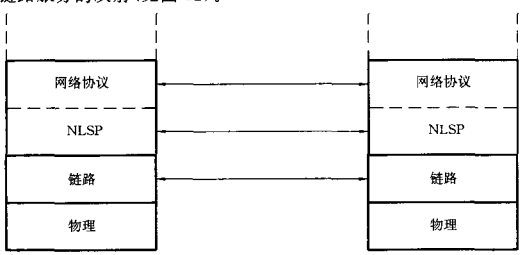


图 11　NLSP 运行在链路层之上的说明

GB/T 9387.2 包括了数据链路层中的保密性要求。对于数据链路安全协议，要求保护 LAN 环境下 2 层网桥之间的通信(见图 12)。

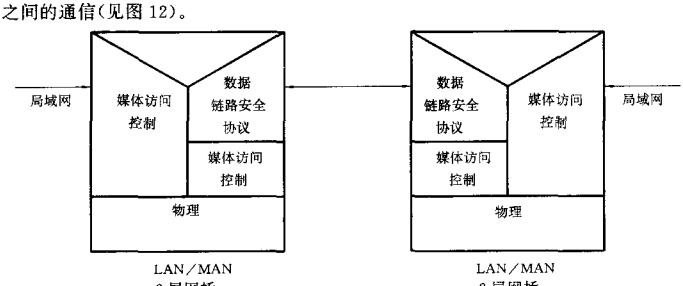


图 12　用于保护两网桥之间通信的数据链路层安全协议的说明

12　为提高(N)层安全而使用的(N－1)层

在给定层中提供安全功能时，可能要利用该层下面提供的安全服务。提供给(N)层用户的所有安全服务能由低层中的机制实现。

13　安全标记

安全标记可以用于指明所选择的安全服务的要求(见第 9 章)以及访问和路由选择控制。

在安全联系下，一对实体可以预先建立安全标记集，该安全标记集可以分配给两实体之间的连接/无连接协议数据单元。

安全标记的使用作为安全策略的一部分定义。

安全框架的第3部分为访问控制，描述了对访问控制的安全标记的应用。

安全标记的第一字段应标识定义该标记的安全权限。该标识符是一个客体标识符(如GB/T 16262中定义)，采用基本编码规则编码(见GB/T 16263)。

安全标记一般结构将与安全信息客体方面的有关安全标准一致。

14 安全域

ISO/IEC 10181-1(安全框架概述)定义的安全域不是与对等协议直接相关。然而，对域的使用将在安全管理的上下文中考虑。

15 路由选择安全

15.1 网络层安全协议(NLSP)(见GB/T 17963)能用来保护域间路由选择协议数据单元(ISO/IEC 10747)的交换(见第11章IDRP的放置)。

15.2 像不支持多对等通信一样，NLSP(如GB/T 17963定义)不能用于支持基于ISO/IEC 10589(中间系统到中间系统，IS-IS)和GB/T 17180(端系统到中间系统，ES-IS)的域内路由选择交换的安全。可以为IS-IS域内及ES-IS路由选择交换协议的安全定义一个基于扩展NLSP的标准协议。任何关于IS-IS域内和ES-IS路由选择交换协议的标准协议将独立于这些路由选择协议。

15.3 要注意，应用于通信的访问控制(例如GB/T 16974封闭用户群，GB/T 17179.1安全标记，NLSP)可以影响可利用的路由。为了得到安全环境中使用的路由选择信息，可以要求关于路由安全状况的信息。

15.4 此外，有必要考虑路由选择的要求以支持访问控制/路由选择控制。

注：GB/T 9387.2将路由选择控制定义为“在路由选择进程期间规则应用以避免特定的网络、链路或中继”。例如，路由选择控制可以基于地址，并且禁止所有数据到某一子网的路由选择，除给定的授权地址以外。另外，路由选择控制能基于安全标记，例如，加标记“商业秘密”的包将不会被发送到公共网络。

16 安全管理

16.1 安全策略

下列信息作为安全策略准则的一部分建立，为(N)层中给定的(N)实体选择安全服务和机制：

——为包括可接受的最大和最小级的(N)层建立所选择的安全服务的准则；

——把选择的安全服务映射到机制和低层保护要求的准则(即第10章中描述的安全规则)。

在使用安全标记的地方，对于安全标记的使用(见第13章)，信息作为安全策略的一部分被建立。

为了审计层协议有关方面的安全并为了提供恢复，信息作为安全策略的一部分被建立。

16.2 安全联系管理

安全联系管理在第5章中讨论。

16.3 密钥管理

密钥的分配与选择可以由下列方式(方法)之一来完成：

a) 作为SA的一部分建立；

b) 在一个安全协议内；

c) 通过OSI低层范围之外的机制。

16.4 安全审计

安全审计信息的收集与分析在ISO/IEC 10181中有关安全框架的第7部分即安全审计中描述。

17 通信流量保密性

通信量填充的处理未被很好地理解。在CONS环境中可以提供与通信流量保密性相关联的三种类型的填充：

a）填充存在的安全数据PDU；

b）生成伪安全数据PDU；

c）生成与其他NLSP对等实体的伪连接。

必须定义每种类型填充的可能的参数(例如，所有PDU将有1 024个八位位组的长度；每500毫秒在连接处将有一个PDU；当该NLSP实体与特定对等NLSP实体连接时，这6个NLSP实体也将被连接并且与它们交换等量的通信量)。这些参数未被很好地理解，但在前两种填充情形中，它们应包括作为安全联系的一部分。因此布尔属性是不够的。有关所需参数的类型要进一步的研究。

18 SA属性定义的准则

SA属性是控制通信安全及其远程对等实体要求的一个信息项。第5章中描述了三种不同类别的SA属性。

控制安全协议要求的SA属性被定义为安全协议的一部分。该定义应包括：

a）用于引用安全协议中的属性的助记符；

b）属性的数据类型；

c）属性语义的描述；

d）如何建立属性值的描述。

安全协议要求的许多属性将依赖于支持的机制。

SA属性定义的例子是：

Encipher：	布尔类型
	使用加密来提供保密性
	给定所选择的安全服务，该属性的值由安全规则商定集定义。
Enc-Alg：	ISO 9979分配的客体标识符
	加密算法
	给定所选择的安全服务，该属性的值由安全规则商定集定义。
Enc-key：	安全规则商定集定义的形式
	加密密钥
	由安全联系建立设定的值

19 差错处理

当安全协议中发生差错时采取的动作由本地安全策略决定。选项包括：

——丢弃差错中的PDU；

——发布差错PDU；

——执行重置或断开规程；

——提出审计报告。

附 录 A
（提示的附录）
安全规则商定集示例

安全规则商定集(ASSR)建立了要使用的安全机制，包括对给定所选择的安全服务而定义机制的操作所必需的全部参数。

ASSR-ID　　OBJECT IDENTIFIER

SA-ID-Length　　4

所选择的服务定义模块

PE Auth：　　无，低，高

AC：　　无，低，高

Confid：　　无，低，高

Integ：　　无，低，高

安全标记映射

Lable _ Def _ Auth　　XYZ

Lable->Sensitivity=Unclass

隐含

PE Auth 无，AC 无，Confid 无，Integ 无

Lable-Sensitivity=Confidential

隐含

PE Auth 低，AC 低，Confid 低，Integ 无

Lable-Sensitivity=Secret

隐含

PE Auth 高，AC 高，Confid 高，Integ 高

所有服务参数的保护

对所选择的安全服务：　　Integ=高或 Conf=高

机制模块——访问控制的安全标记

对所选择的安全服务：　　AC=高或 Conf=高

Lable _ Def _ Auth　　XYZ

明确指示　　是

机制模块——完整性检验值

对所选择的安全服务：　　Integ>无或 PE Auth=高或机制安全标记

ICV _ Alg _ Id　　XYZ

ICV _ Block _ Size　　8 个八位位组

Re-key after　　10,000PDU

密钥分配机制　　非对称

机制模块——完整性顺序号

对所选择的安全服务：　　Integ=高或 Auth=高

ISN _ Len　　4 个八位位组

机制模块——加密

对所选择的安全服务： Conf＞低
Enc _ Alg _ ID XYZ
方式 链接
Enc _ Block _ Size 8 个八位位组
Re-key after 1，000PDU
密钥分配机制 非对称
机制模块——无报头
对所选择的安全服务： Conf＝低且 Integ＝无且无标记机制
机制模块——连接鉴别
对所选择的安全服务： AC＞低或 PE Auth＞低
Enc _ Alg _ ID XYZ
机制模块——非对称密钥分配
对于机制加密或完整性检验值
PKC _ Alg _ ID RSA