ICS 35.100.30
L 78

中华人民共和国国家标准

GB/T 17963—2000
idt ISO/IEC 11577:1995

信息技术　开放系统互连　网络层安全协议

Information technology—Open Systems Interconnection—Network layer security protocol

2000-01-03 发布　　2000-08-01 实施

国家质量技术监督局　发布

前　　言

本标准等同采用国际标准 ISO/IEC 11577:1995《信息技术　开放系统互连　网络层安全协议》。

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和 GB/T 15274 定义的网络层组织规定了网络层安全协议。本标准无论在技术内容上还是在编排格式上均与国际标准保持一致。

本标准的附录 A、附录 B、附录 C、附录 D 都是标准的附录；附录 E、附录 F、附录 G、附录 H 都是提示的附录。

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、中国电子技术标准化研究所。

本标准主要起草人：邓良松、冯惠、邓秦、丁峰。

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(他们都是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。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一个国际标准,至少需要75%的参与表决的国家成员体投票赞成。

国际标准ISO/IEC 11577是由ISO/IEC JTC1"信息技术"联合技术委员会、SC6"系统间远程通信和信息交换"分技术委员会与ITU-T合作制定的,该文本也以ITU-T建议X.273发布。

注:由于本国际标准最终版本编辑日期的缘故,在本国际标准引用的ISO/IEC 7498-1、ISO/IEC 9646-1、ISO/IEC 9646-2、ISO/IEC 10731、ISO/IEC 10745和ISO/IEC TR 13594的出版日期不同于相同的ITU建议X.273中引用的这些标准的出版日期。

附录A到附录D是本国际标准的组成部分。附录E到附录H仅提供参考信息。

引　　言

本标准定义的协议提供安全服务以支持较低层实体间的通信实例。本协议由GB/T 9387.1～9387.2中定义的层次结构和GB/T 15274中定义的网络层组织相对其他标准来定位，并按照ISO/IEC TR 13597(低层安全模型)来扩展。它提供连接方式和无连接方式网络服务的安全服务支持，尤其，本协议位于网络层，在其上边界处和下边界处有功能接口和定义清晰的服务接口。

为了评价特定实现的一致性，需要有对给定OSI协议已实现的能力和选项的声明，这种声明称为协议实现一致性声明(PICS)。

中华人民共和国国家标准

信息技术　开放系统互连　网络层安全协议

GB/T 17963—2000
idt ISO/IEC 11577:1995

Information technology—Open Systems Interconnection—Network layer security protocol

1　范围

本标准规定的协议将由端系统和中间系统使用，以在网络层提供安全服务，而网络层由GB/T 15126和GB/T 15274定义。本标准中定义的协议称为网络层安全协议(NLSP)。

本标准规定：

a) 支持GB/T 9387.2中定义的下列安全服务：

1) 对等实体鉴别；

2) 数据原发鉴别；

3) 访问控制；

4) 连接保密性；

5) 无连接保密性；

6) 通信流量保密性；

7) 无恢复的连接完整性(包括数据单元完整性，其中连接上的各个SDU具有完整性保护)；

8) 无连接完整性。

b) 声称与本标准一致的实现的功能要求。

本协议的规程根据下列定义：

1) 可用于本协议实例的加密技术的要求；

2) 用于通信实例安全联系中携带信息的要求。

尽管一些安全机制提供的保护程度取决于一些特定加密技术，而本协议的正确操作并不取决于某种特定的加密或解密算法的选择。这是通信系统的本地事情。

此外，特定的安全策略的选择和实现都不在本标准的范围之内。特定的安全策略的选择以及因此将达到的保护程度，留作使用安全通信的单个实例的系统之间的本地事情。本标准不要求涉及同一开发系统的多个安全通信的实例必须采用相同的协议。

附录D按照ISO/IEC 9646-2中给出的相关指导为网络层协议提供了PICS形式表。

2　引用标准

下列标准包含的条文，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

国家质量技术监督局2000-01-03批准　　2000-08-01实施

(idt ISO/IEC 7498-2:1989)

GB/T 15126—1994 信息处理系统 数据通信 网络服务定义(idt ISO 8348:1987)

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/IEC 8648:1988)

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 16264.8—1996 信息技术 开放系统互连 目录 第8部分:鉴别框架 (idt ISO/IEC 9594-8:1990)

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 16976—1997 信息技术 系统间远程通信和信息交换 使用X.25提供OSI连接方式网络服务(idt ISO/IEC 8878:1992)

GB/T 17178.1—1997 信息技术 开放系统互连 一致性测试方法和框架 第1部分:基本概念 (idt ISO/IEC 9646-1:1994)

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 17967—2000 信息技术 开放系统互连 基本参考模型 OSI服务定义约定 (idt ISO/IEC 10731:1994)

ISO/IEC 9646-2:1994 信息技术 开放系统互连 一致性测试方法和框架 第2部分:抽象测试套规范

ISO/IEC 9834-1:1993 信息技术 开放系统互连 OSI登记机构的操作规程 第1部分:一般规程

ISO/IEC 9834-3:1990 信息技术 开放系统互连 OSI登记机构的操作规程 第3部分:ISO/CCITT联合使用的客体标识符部件值的登记

ISO/IEC 9979:1991 数据加密技术 加密算法的登记规程

ISO/IEC 10745:1995 信息技术 开放系统互连 高层安全模型

ISO/IEC TR 13594:1995 信息技术 开放系统互连 低层安全模型

CCITT 建议X.25(1993) 用专用电路连接到公用数据网上的分组式数据终端设备(DET)与数据电路终接设备(DCE)之间的接口

3 定义

3.1 参考模型定义

本标准采用GB/T 9387.1中定义的下列术语:

a) 端系统 end system;

b) 网络实体 network entity;

c) 网络层 network layer;

d) 网络协议 network protocol;

e) 网络协议数据单元 network protocol data unit;

f) 网络中继 network relay;

g) 网络服务 network service;

h) 网络服务访问点 network service access point;

i) 网络服务访问点地址 network service access point address;

j) 网络服务数据单元 network service data unit;

k）协议数据单元　protocol data unit；

l）路由选择　routing；

m）服务　service；

n）服务数据单元　service data unit。

3.2　安全体系结构定义

本标准采用 GB/T 9387.2 中定义的下列术语：

a）访问控制　access control；

b）保密性　confidentiality；

c）无恢复的连接完整性　connection integrity without recovery；

d）无连接保密性　connectionless confidentiality；

e）无连接完整性　connectionless integrity；

f）数据原发鉴别　data origin authentication；

g）解密　decipherment；

h）数字签名　digital signature；

i）加密　encipherment；

j）对等实体鉴别　peer entity aughentication；

k）安全标号　security label；

l）安全服务　security service；

m）通信流量保密性　traffic flow confidentiality。

3.3　服务约定定义

本标准采用 GB/T 17967 中定义的下列术语：

a）服务提供者　service provider；

b）服务用户　service user。

3.4　网络服务定义

本标准采用 GB/T 15126 中定义的下列术语：

——子网连接点　subnetwork point of attachment。

3.5　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）中间系统　intermediate system；

b）中继系统　relay system；

c）子网　subnetwork；

d）子网访问协议　subnetwork access protocol；

e）依赖于子网收敛协议　subnetwork dependent convergence protocol；

f）独立于子网收敛协议　subnetwork independent convergence protocol。

3.6　无连接网络协议定义

本标准采用 GB/T 17179.1 中定义的下列术语：

a）初始 PDU　initial PDU；

b）本地事情　local matter；

c）重装　reassembly；

d）段　segment。

3.7　高层安全模型定义

本标准采用 ISO/IEC 10745 中定义的下列术语：

a）安全交互作用策略　secure interaction policy；

b）安全关系　security relationship。

3.8　一致性测试定义

本标准采用 GB/T 17178.1 中定义的下列术语：

a）PICS 形式表　PICS proforma；

b）协议实现一致性声明　protocol implementation conformance statement；

c）静态一致性概述　static conformance overview。

3.9　附加定义

本标准采用下列定义：

3.9.1　冻结 SA-ID　frozen SA-ID

由于要求防止重用，不能用来分配给某个安全联系的一种 SA-ID。

3.9.2　成对的密钥　pairwise key

用于特定双方间的一对相关的(公开密钥)或同一的(秘密密钥)密钥值。

3.9.3　安全控制信息　security control information

为了建立或维护安全联系的安全协议所交换的协议控制信息(PIC)。

3.9.4　SA 属性　SA-attributes

控制实体其远程对等实体之间通信安全所要求的信息汇集。

3.9.5　安全联系　security association

存在相应 SA 属性的通信低层实体之间的安全关系。

3.9.6　数据单元完整性　data unit integrity

连接完整性的一种形式，其中，各个 SDU 的完整性受到保护，但不检测 SDU 序列中的差错。

3.9.7　带内　in-band

使用本标准中定义的 SA PDU 的协议机制来执行。

3.9.8　带外　out-of-band

使用 SA PDU 以外的方法来执行。

3.9.9　安全规则　security rules

一种本地信息。它给出选择的安全服务，它规定要使用的安全机制及该机制操作所需的所有参数。

注：该信息可以组成如 ISO/IEC 10745 中定义的安全交互作用规则的一部分。

3.9.10　标号　label

与某一资源(可以是数据单元)密切相联的标号，为该资源命名或规定安全属性。

注：这种标号的结束可以是明显的，也可以是暗指的。

4　缩略语

4.1　数据单元

NPDU	网络协议数据单元
NSDU	网络服务数据单元
PDU	协议数据单元
SDU	服务数据单元

4.2　协议数据单元字段

LI	长度指示符

4.3　参数

QOS	服务质量

4.4　杂项

ASSR	安全规则商定集

CL	无连接方式
CLNP	无连接方式网络协议
CLNS	无连接方式网络服务
CO	连接方式
CSC PDU	连接安全控制 PDU
DU	数据单元
EKE	指数密钥交换(见附录 H)
ES	端系统
ICV	完整性检验值
IS	中间系统
ISN	完整性顺序号
KEK	密钥加密密钥
NLSP	网络层安全协议
NLSP CO	连接方式 NLSP
NLSP CL	无连接方式 NLSP
NLSPE	NLSP 实体
NS	网络服务
NSAP	网络服务访问点
PCI	协议控制信息
PDU	协议数据单元
SA	安全联系
SA-ID	安全联系标识符
SA-P	安全联系协议
SA-PDU	安全联系 PDU
SCI	安全控制信息
SDT PDU	安全数据传送 PDU
SN	子网
SNAcP	子网访问协议
SNICP	独立于子网收敛协议
SNPA	子网连接点
UN	底层网

5 协议概述

5.1 导引

NLSP 协议有两种基本操作方式：

a) NLSP-CL——用于提供安全无连接网络服务；

b) NLSP-CO——用于提供面向安全连接网络服务。

NLSP 的两种方式都作为网络层的子层操作。提供给上面实体的服务称为 NLSP 服务，要提供给 NLSP 的所承担的服务称为底层网(UN)服务。原语和参数加上前缀 NLSP 或 UN 以明白地区分被引用的服务。UN 和 NLSP 服务是“概念接口”，即被描述成似乎是层服务但可能完全驻留在网络层中，取决于 NLSP 子层的位置(见附录 E)。

NLSP 的两种方式都能在端系统和中间系统中实现。两种方式都允许源和目的 NLSP 地址及其他 NLSP CONNECT 参数被任选地保护。可在网络层的任何处操作 NLSP-CO。可在依赖于子网收敛协议

(见 GB/T 15274)之上的网络层的任何处操作 NLSP-CL。

设计本协议是为了优化满足从主要关心高度安全环境到主要关心性能优化环境的一系列要求。特别地,尽管可能会降低安全,但 NLSP-CO 中提供的"无报头"选项可获得对通信效率的影响最小。

NLSP 协议使用了安全联系(SA)的概念,它可存在于某一特定的无连接或连接 UNITDATA 之外。为安全参数(例如算法、密钥等)定义的属性集是为 SA 而定义的。

本协议在其上、下边界上提供了相同的服务(CO 或 CL)方式。

本协议支持一系列特定安全机制(标准化的和非标准化的)的使用。用户和实现者将选择安全机制与协议配合使用以加强安全服务和要求的保护级别。第 9 章到第 12 章及附录 C 定义了对 NLSP 要求的所有安全服务的特定机制集的支持。

NLSP 试图提供的安全保护是从安全域管理所建立的安全服务要求导出的。

注:NLSP 服务保护 QOS 参数的使用是本地事情,超出本标准的范围。

5.2 提供的服务概述

NLSP 提供了在 GB/T 9387.2 中定义的那些安全服务与 GB/T 15126 中定义的 OSI 网络层服务,它们适用于网络层。

若选择 NLSP-CL,它可支持下列安全服务:

a) 数据原发鉴别;

b) 访问控制;

c) 无连接保密性——本保护任选地包括所有 NLSP 服务参数,取决于所选择的安全服务;

d) 通信流量保密性;

e) 无连接完整性——本保护任选地包括所有 NLSP 服务参数,取决于所选择的安全服务。

若选择 NLSP-CO,它可支持下列安全服务:

a) 对等实体鉴别;

b) 访问控制;

c) 连接保密性——本保护任选地包括所有 NLSP 连接参数,取决于所选择的安全服务;

d) 通信流量保密性;

e) 无恢复的连接完整性——本保护任选地包括所有 NLSP 连接参数,取决于所选择的安全服务。本保护也任选地包括 SDU 序列的完整性。

5.3 所承担的服务概述

NLSP 下面所承担的服务称为底层网(UN)服务。NLSP-CL 所承担的底层服务使用的原语与无连接网络服务(GB/T 15126)中定义的相同。

对于 NLSP-CO,UN 接口被模型化为两部分:

a) 一个服务,它使用与 GB/T 15126 相同的原语并且附加了一个称作为 UN 鉴别的参数;

b) 该服务的映象,它映射到标准网络服务,或直接映射到 GB/T 16974。

NLSP 原语中携带的网络地址称为 NLSP 地址。该服务参数标识 NLSP 用户实体,它可以是或不是一个传输实体,取决于 NLSP 上面是否使用其他网络层协议,也取决于 NLSPE 是位于 ES 中还是 IS 中。传递到底层网的网络地址称为 UN 地址。当且仅当 NLSP 实体与子网访问实体间无协议操作时,该 UN 参数(即 UN 地址)等价于 SNPA 地址。

5.4 安全联系与安全规则

5.4.1 安全联系

NLSP 的操作由称为安全联系属性(SA 属性)的安全管理信息(例如安全服务选择信息,安全算法标识符,密码密钥)的汇集所控制。为管理在通信实体间提供的安全服务所要求的安全联系属性汇集的存在称为安全联系。

ISO/IEC TR 13594(低层安全模型)中进一步描述了安全联系。

NLSP-CL 和 NLSP-CO 要求的 SA 属性在 6.2 中定义，NLSP-CL 要求的 SA 属性在 7.4 中定义，NLSP-CO 要求的属性在 8.4 中定义，进一步的机制特定属性在 10.2、11.2 和 12.2 中定义。

为了保护通信的实例(连接或无连接的 SDU)，可使用存在的合适 SA，若不存在合适的 SA，则需在通信方之间建立一个 SA。

安全联系在带外或使用 NLSP 带内 SA-P 来建立，NLSP SA-P 通过使用具有内容数据类型 SA-P 的 SA-PDU 和/或 SDT PDU 来交换安全控制信息(SCI)。若无阻碍携带 SCI，应使用 SA-PDU。若要保护 SCI，则应使用 SA-PDU 或 SDT PDU。该 SCI 用于完成建构于在任何预先建立的 SA 属性和安全规则的 SA 属性上。

NLSP-CO 也支持在连接建立中和连接期间的信息交换以更新“动态”SA 属性(例如工作密钥，见附录 G)。对动态 SA 属性的更新应不改变已提供的安全服务。

带内 SA-P 连同 NLSP-CL 一起的使用在 7.5 中定义。具有 NLSP-CO 的带内 SA-P 的使用在 8.5(连接建立期间)和 8.11(数据传送期间)中定义。体现带内 SA-P 的协议在本规范的附录 C 中定义。附录 H 给出了建立为本协议使用的密钥机制的例子。

5.4.2 安全规则

安全策略将约束许多 SA 属性的设置。该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将诸如字段长度、密码算法等的 SA 属性约束为单个值或要用其他手段进一步约束的值集(例如 OSI 系统管理或使用 SA-P 交换)。

在出现选择保护级处，安全规则集将定义选择约束以满足所要求保护的不同质量。

当用于 NLSPE 间的操作时，需要建立该安全规则集的唯一标识符，它称为安全规则商定集(ASSR)，ASSR 标识符可作为安全联系建立的一部分进行交换。

ISO/IEC TR 13594(低层安全模型)对安全规则作了进一步说明。

5.5 协议概述——保护功能

5.5.1 保护的范围

NLSP-CO 和 NLSP-CL 都有三种不同的操作方式以支持三种基本保护程度：

a) 所有 NLSP 服务参数的保护

在本方式中，保护所有的 NLSP 服务参数，包括地址和全部用户数据，不包括那些要与服务提供者协商的参数(QOS、接收保密性选择、加快数据选择)。

由为 TRUE 的 SA 属性 Param _ Prot(见 6.2)来选择本方式。

b) NLSP 用户数据保护

在本方式中保护用户数据但其他 NLSP 服务参数则不受保护。

由为 FALSE 的 SA 属性 Param _ Prot 来选择本方式。

对于 NLSP-CO，NLSP 用户数据的保护有进一步的子方式，下列方式之一：

1) 保护所用的 NLSP 用户数据(包括在 NLSP-CONNECT、NLSP-DATA 和 NLSP-DISCONNECT 服务原语中的 NLSP 用户数据)；

2) 保护在 NLSP DATA 中的 NLSP 用户数据。

由 SA 属性 Protect _ Connect _ Param(见 8.3)来进一步选择 NLSP 的子方式。若 Protect _ Connect _ Param 为 TRUE，则保护所有的 NLSP 用户数据，否则只保护在 NLSP-DATA 中的 NLSP 用户数据。若 Param _ Prot 为 TRUE，则强迫 Protect _ Connect _ Param 为 TRUE(即保护所有的 NLSP 用户数据)。

c) 无保护

在本方式中，所有的 NLSP 服务参数都直接复制成等价的 UN 服务参数，并旁路所有的 NLSP 规程。

在本地选择本方式是基于通信对等的地址和本地安全服务要求。

5.5.2 保护的质量

OSI 低层中的安全(保护)QOS 的实行通过实现来完成,这些实现选择了借助于本地受控的安全策略所施加的安全服务。通过隐式地使用安全标号或显式地用其他手段,以独立于通信实例的安全联系协议来运送选择的安全服务的任何带内指示。因此,任何与安全服务选择相关的交换独立于穿过服务接口边界的 QOS 参数的运输。

注:可能也有对高层指明安全服务的要求,但到目前为止,还没有建立特定保护 QOS 要求定义的直接要求。

5.5.3 数据保护功能

5.5.3.1 基于 SDT PDU

NLSP-CO 和 NLSP-CL 都能通过使用安全数据传送 PDU(SDT PDU)来保护 NLSP 服务参数。NLSP-CO 也有两种可供选择的保护 NLSP 用户数据的方法,它通过 SA 属性 No _ Header(见 8.3)为 TRUE 来选择。

使用基于规程的 SDT PDU 时通过下列方式保护 NLSP 服务参数:

a) 将 NLSP 服务参数编码为封装前八位位组串;

b) 若选择显式安全已加标号(SA 属性 Label 为 TRUE),则把安全标号放入封装前八位位组串中;

c) 如适于已选择的安全服务,可应用支持下列机制的封装(和解封)功能。本功能提供受保护的八位位组串:

——通信流量保密性;

——完整性和数据原发鉴别;

——保密性。

6.4.1.1 和 6.4.2.1 定义通用的、用于 SDT PDU 的机制独立规程以保护数据。第 11 章定义对基于封装的 SDT PDU 的机制一级的支持。其他专门定义封装的规程可与 SDT PDU 一起使用。

5.5.3.2 无报头(仅 NLSP-CO)

NLSP CO 无报头方式通过封装功能来保护 NLSP 用户数据,该功能不更新被保护数据的长度。NLSP 不向所保护的数据上加任何协议控制信息,支持的安全服务将取决于使用的机制但封装功能应至少提供保密性。无报头方式只可用于保护单个服务参数(NLSP 用户数据),因而只有当 Param _ Prot 为 FALSE 时可用。

6.4.1.2 和 6.4.2.2 定义通用的、用于无报头方式的机制独立规程来保护数据。第 12 章定义对无报头封装机制一级的支持。其他专门定义封装规程可与无报头方式一起使用。

5.5.4 连接安全控制(仅 NLSP-CO)

当建立连接时,交换连接安全控制 PDU 来标志 NLSP 连接建立方式(或与带内 SA-P,或映射 NLSP CONNECT 原语到 UN-CONNECT 或 UN-DATA 原语)。此外,CSC PDU 可支持对等实体鉴别,并且建立动态 SA 属性值,如密钥和完整性顺序号。这就允许重用先前建立的 SA,而不会导致 SA-P 的额外开销。在重新鉴别(证明共享知识的)SA 的连接或更新动态属性的生命期中的任何时候它都可用。

CSC PDU 仅用于连接方式 NLSP,第 8 章定义了一般的机制独立的用于 CSC PDU 的规程。第 10 章定义对鉴别机制一级的支持和密钥管理。其他专门定义的支持机制其他级的规程可与 CSC PDU 一起使用。

注:当使用鉴别的可供选择的机制时,若用到第 11 章中定义的 ISN 机制,该选择的机制将建立 ISN 的初始值。

5.5.5 NLSP 使用的 PDU

NLSP 使用下列 PDU:

a) 安全数据传送 PDU——通过 5.5.3.1 中概述的封装来保护 NLSP 服务原语参数和其他数据。13.3 中定义了该 PDU 的结构;

b) 连接安全控制 PDU——如 5.5.4 中概述的控制 NLSP-CO 连接建立方式,任选地提供对等实体

鉴别及更新动态SA 属性。13.5 中定义了该PDU 的结构；

注：CSC PDU 仅适合于NLSP-CO。

c) SA PDU——一种PDU，该PDU 允许如 5.4.1 中概述的为了SA 管理目的的安全控制信息带内交换。13.4 中定义了该PDU 的结构。

此外，对于NLSP-CO，可无需任何额外的如 5.5.3.2 概述的协议控制信息(即不用SDT PDU)来任选地保护数据。

5.6 协议概述——NLSP-CL

5.6.1 定义NLSP-CL

第 6 章和第 7 章中定义了NLSP-CL 规程，封装的任选机制特定规程定义在第 11 章中，这些规程使用如13.3 中定义的SDT PDU 和如13.4 中定义的任选的SA PDU。

下列条仅提供NLSP-CL 操作的概述；上面标识的特定章定义NLSP-CL 操作。

5.6.2 NLSP-CL 功能

要是ASSR 中的访问控制规则允许，NLSP 支持在对等的NLSP 用户间的传送保护能力或无保护的无连接数据的能力。NLSPE 本地确定是否需要保护(使用选择的安全服务，目的NLSP 地址或其他管理信息)，保护的数据传送可以是保护所有NLSP 服务参数或只由SA 属性Param-Prot 确定的NLSP 用户数据。

收到NLSP-UNITDATA Request 时：

a) NLSP 实体检验SA 并确定是否允许与目的地址的无保护通信，要是这样，是否要求保护；

b) 若不要求保护，NLSP 实体把所有的NLSP 原语和参数无改变地复制到对应的UN 原语和参数；

c) 若要求保护，NLSP 实体封装服务参数，形成SDT PDU 并作为UN-UNITDATA Request 的UN 用户数据连同UN 源地址、UN 目的地址和UN QOS 参数传送。这样仅能保护NLSP 用户数据或所有的NLSP 服务参数。

收到UN-UNITDATA Indication 时，NLSP 实体：

a) 使用UN 源地址和本地信息来确定是否允许与目的地址的通信，要是这样，是否要求保护；

b) 若不要求保护，UN 服务参数无改变地复制到NLSP 参数；

c) 若要求保护，NLSP 实体检验SDT PDU 并运用解封功能提取NLSP 用户数据和其他任选的NLSP 服务参数，用户数据、源地址、目的地址和QOS 参数传递给NLSP-UNITDATA Indication 中的NLSP 用户。

注：传递NLSP 可在GB/T 17179.1(CLNP)协议功能保护CLNP PDU 之后(接收之前)操作。传递NLSP 也可在CLNP 协议功能携带CLNP PDU 数据字段的NLSP PDU 之前(接收之后)操作，使用NLSP 和CLNP 的进一步的讨论见附录E。

由于一些CLNP 参数可能有安全相关性，NLSP 传递后对这些参数的选择必须考虑到本地安全策略。要考虑的一些任选参数为路由记录、部分和完全的源路由选择以及跳数。任何这些参数都可以给出该网络的信息，这些信息对于网络观察器不应该可用。

为了确定CLNP PDU 中携带有NLSP-CLPDU，在接收时，接收者将检验目的地址的选择符为 0 或CLNP PDU 数据字段中的NLSP 协议标识符如13.3 中定义的，两种检验都可以用来指明与直接把它送到传输层相比，该PDU 是由网络层处理的。

5.7 协议概述——NLSP-CO

5.7.1 定义NLSP-CO

第 6 章和第 8 章中定义了基于无报头的NLSP-CO 规程，封装的任选机制特定规程定义在第 12 章中，第 10 章中定义了连接安全控制规程，这些规程使用如13.5 中定义的CSC PDU 和13.4 中定义的任选SA PDU。

基于SDT PDU应用的NLSP-CO规程在第6章和第8章中定义，封装的任选机制特定规程定义在第11章中，第10章中定义了连接安全控制规程。这些规程使用13.3中定义的SDTD PDU，13.5中定义的CSC PDUT和13.4中定义的任选的SA PDU。

下列条仅提供NLSP-CO操作的概述；上面标识的特定章定义NLSP-CO操作。

5.7.2 NLSP-CO无保护连接

若在主叫和被叫地址间允许无保护通信，所有的NLSP/UN服务参数直接从NLSP服务接口拷贝到UN服务接口或直接从UN服务接口拷贝到NLSP服务接口。

5.7.3 NLSP-CONNECT

在接收NLSP-CONNECT Request时，NLSPE检验具有要求特征的SA当前是否存在。若存在，即可用于保护连接。否则，带内建立新的SA作为NLSP-CONNECT功能的一部分或在给出的超时中带外建立。若这些都不能进行，则返回NLSP-DISCONNECT。

支持两种建立NLSP连接的基本方式。一种是在UN-CONNECT服务原语中携带NLSP CONNECT参数。另一种是在SDT PDU封装后携带NLSP CONNECT参数；在UN连接建立后的UN-DATA中，建立NLSP连接的两种方式有不同之处。一种用于同携带在UN-DATD中的带内SA-P进行交换(使用具有SA-P内容数据类型的SA PDU和/或SDT PDU)；另一种用于带外建立的SA。

连接安全控制(CSC)PDU用来标志连接建立的方式，若不携带带内SA-P，CSC PDU交换也用于：

a) 为使用保护连接(例如密钥、完整性顺序号)建立机制特定安全属性；

b) 执行对等实体鉴别。

对基于鉴别和密钥管理的简单要求响应机制的任选支持在第10章中定义。

在NLSP-CONNECT借助带内SA-P正在携带UN-CONNECT的情况下，在执行携带有NLSP CONNECT参数的UN-CONNECT交换之前，建立UN连接以携带SA-P然后释放。在第二次UN-CONNECT交换时使用CSC PDU以再鉴别对等NLSP实体。

通过交换SA PDU或带有建立要求的SA属性所需的信息的SDT PDU可完成SA建立。附录C定义了用于该用途的SA协议。

若要求保护NLSP-CONNECT参数，在传送前封装这些参数。

5.7.4 NLSP-DATA

接收NLSP-DATA Request时：

a) 若选择基于保护的SDT PDU，NLSP实体封装合适的服务参数形成SDT PDU并作为UN-DATA的UN用户数据传送它；

b) 若选择基于保护的无报头，加密NLSP用户数据并传送到UN-DATA Request的UN用户数据。

接收UN-DATA Indication时：

a) 若选择基于保护的SDT PDU，NLSP实体检验PDU并使用解封功能提取NLSP用户数据，也可能提取NLSP保密性请求；

b) 若选择基于保护的无报头，解密UN用户数据以获取NLSP用户数据；

c) NLSP服务参数传递给NLSP-DATA Indication中的NLSP用户。

5.7.5 NLSP-EXPEDITED-DATA

以相似于NLSP-DATA Request的方法来处理。

注：当使用SDT PDU时，封装功能可能会扩大数据大小。因此，限制了用户数据字段的大小，可以要求保护的加快数据在通过底层网时进一步分段和重装。

5.7.6 NLSP-RESET

通过NLSP直接传递至底层网，重新鉴别安全连接，通过使用UN-DATA中携带的CSC PDU重建机制特定属性。

注：由于数据可能已丢失，可能需要重初始化某些安全机制。特别地，完整性序列机制必须在数据丢失后避免重演攻击。

5.7.7 NLSP-DATA-ACKNOWLEDGE

若要保护所有的NLSP服务参数(即Param-Prot为TRUE)，封装该服务原语，置于SDT PDU中并通过NLSP传递到UN子层。否则该服务原语直接映射到UN-DATA-ACKNOWLEDGE。

5.7.8 NLSP-DISCONNECT

接收NLSP-DISCONNECT Request时，若选择的保护方式(见5.5.1)要求保护服务参数，NLSP实体建造了包含NLSP-DISCONNECT Request、NLSP用户数据和任选的其他参数的安全数据传送PDU。该PDU在UN连接释放前，携带在UN-DATA中，或者若合适，SDT PDU可携带在UN-DISCONNECT的UN用户数据中。

若不要求保护NLSP-DISCONNECT Request的参数，则把它们传送到UN-DISCONNECT Request中。

5.7.9 其他功能

NLSP也支持下列功能，在超时或其他外部事件时，启动这些功能：

a) CSC PDU交换以改变动态SA属性，如密钥；

b) 安全测试交换以检验SA的加密特征正确建立；

c) SDT PDU传送仅包含通信流量保密性的通信量填充字段。

6 NLSP-CL和NLSP-CO公共的协议功能

6.1 导引

本章描述NLSP连接和无连接方式公共协议功能。它们的使用如第7章和第8章中所述。

6.2 公共SA属性

下列SA属性控制连接方式和无连接方式NLSP的操作。它们的描述包含在本规范内涉及这些属性使用的助记符。

注1：SA属性是“ASSR约束”的地方，该约束可定义单个值或值的集合。在ASSR定义值的范围中，可由OSI系统管理、SA-P交换或本规范外的其他方法建立属性值。

a) SA标识：

My_SA-ID：0到(256 ** 最大长度)－1范围的整数。

SA的本地标识符，该属性的值应在SA建立时设置。

Your_SA-ID：0到(256 ** 最大长度)－1范围的整数。

SA的远程标识符，该属性的值应在SA建立时设置。最大长度是2到126中的一个整数。

注2：SA有多个相同本地标识符是个严重差错。

b) 是启动NLSPE还是响应SA建立的指示符：

Initiator：布尔类型

该属性指明如何置启动者到响应者标志以检测转向的PDU。

该属性的值应在SA建立时设置。

c) 对等NLSP实体的UN地址：

Peer_Adr：八位位组串来格式化在GB/T 15126中的定义。该属性的值应在SA建立时设置。

d) 通过远程对等服务实体的NLSP地址：

Adr_Served：八位位组串集，格式化在GB/T 15126中的定义。

该属性的值应在SA建立或预先建立时设置。

e) 为SA选择的安全服务：

AC： ASSR 约束范围的整数。

TF _ Conf：ASSR 约束范围的整数。

f) 参数保护：

Param _ Prot：布尔类型。

保护所有的 NLSP 服务参数除了那些可被底层网更新的(即 QOS、接收证实选择和加快数据选择)。

g) 标号机制属性：

Label：布尔类型

连接/无连接 PDU 的明显标号。

Label _ Set：

{Label _ Ref：整数。

Label _ Auth：客体标识符。

Label _ Content：格式化 Label _ Auth 定义的。}的集合

这些属性的值在 SA 建立或预先建立时设置。

注 3：根据国家标准定义的规程，期望这些标号要被登记。

6.3 通信实例请求的公共功能

6.3.1 初始检验

接收通信实例请求的 NLSPE(即 NLSP-CONNECT 或 UNITDATA Request)应检验：

a) NLSP 主叫或源地址是该 NLSPE 服务的 NLSP 地址；

b) 需要的安全服务可由该 NLSPE 提供。

6.3.2 安全联系的标识

接收通信实例请求的 NLSPE(即 NLSP-CONNECT 或 UNITDATA Request)在对它可用的 SA 间识别满足下列条件的 SA：

a) 任何本地派生的安全服务要求适应为该 SA 选择的安全服务；

b) 被叫 NLSP 或目的地址包含在 Adr-Served 中的 NLSP 地址集中；

c) 没有 NLSP 连接正使用该 SA(仅 NLSP-CO)。

若不止一个 SA 满足这些条件，要遵循的规程是本地事情。若不存在这样的 SA 且支持带内 SA 建立，那么如第 7 章和第 8 章所定义的那样可能选择 SA-P(SA 协议)选项。否则，要遵循的是带外 SA 建立规程。若在本地定义的超时间隔内这些规程都不能成功地完成，那么如 7.4 和 8.4 中定义的，要执行适于通信方式的差错恢复规程。

6.4 安全数据传送协议功能

6.4.1 产生

6.4.1.1 基于 SAT PDU

如在第 7 章和第 8 章中使用的，应执行下列：

a) 数据类型字段第 8 位应置为 SA 属性启动者的值；

b) 若从 8.6(NLSP-DATA)中调用这些规程，数据类型字段的第 7 位应根据这些规程设置，否则该位设置为指明的“last”值；

c) 为了适于第 7 章和第 8 章中的规程，数据类型字段 1～6 位应置为 13.3.4.2 中定义的值；

d) 根据第 7 章和第 8 章中的规程，与 NLSP 服务参数或其他协议交换相关的数据(例如测试数据)按要求放在合适的内容字段中(见 13.3.4.3)；

e) 若(Label 是 TRUE)并且在 NLSP-CO 情况下这是在当前连接上发送的第一个 SDT PFU 时，是下列之一：

1) 一个安全标号，包括定义权限，应放置于标号内容字段中并包含在 PDU 中；

2) 一个安全标号参考,应放置于标号参考内容字段中并包含在 PDU 中。

选择的标号应是 SA 属性 Label _ Set 中的一个值。

注 1:在 NLSP CO 的情况下,若 Protect _ Connect _ Param 仅 SDT PDU 携带的 NLSP CONNECT 参数将被加标号。否则,NLSP 数据传送阶段在任何方向发送的第一个 SAT PDU 将被加标号。

f) 应调用封装功能(例如第 11 章中描述的)且传递下列自变量:

1) SA-ID 应置为 My _ SA-ID;

2) unit-data-type 应置为:

- "expedited",若保护的数据来源于 NLSP-EXPEDITED-DATA 原语;
- "normal",否则;

3) 封装前八位位组串应被置为结构化的 PDU 字段。

g) 封装功能应返回一个差错或封装的八位位组串。在封装功能成功地完成后,如 13.3.2 中描述的,应创建 SDT PDU 的无保护报头,且封装的八位位组串应添加到报头上。

注 2:NLSP-CO 中不出现 SA-ID。

6.4.1.2 无报头出现(仅 NLSP _ CO)

如第 8 章中使用的,应执行下列:

a) 应调用不选择数据大小的封装功能(例如第 12 章中描述的)且传递下列自变量:

1) SA-ID 应置为 My _ SA-ID;

2) unit-data-type 应置为:

- "expedited",若要保护的数据来源于 NLSP-EXPEDITED-DATA 原语;
- "normal",否则;

3)封装前八位位组串应置为 NLSP 用户数据参数。

b) 封装功能应返回差错或封装的八位位组串。

6.4.2 检验

6.4.2.1 基于 SDT PDU

如第 7 章和第 8 章中使用的,应执行下列:

a) 从 PDU 中丢弃无保护的报头;

b) 应调用解封功能(例如第 11 章中描述的)且传递下列自变量:

1) SA-ID 应置为 My _ SA-ID;

2) unit-data-type 应置为:

- "expedited",若要解封的数据来源于 UN-EXPEDITED-DATA 原语;
- "normal",否则;

3) 封装的八位位组串应置为 PDU 中的余下部分。

c) 解封功能应返回差错或封装前八位位组串。在解封功能完成时,执行下列处理;

d) 应检验数据类型字段第 8 位(启动者或响应者)标志 NOT 等于 SA 属性启动者的值;

e) 要检验数据类型字段 1～6 位和第 7 位为适合于第 7 章和第 8 章中所给规程的值;

f) 若(Label 为 TRUE),并在 NLSP-CO 的情况下,这是在当前连接上接收的第一个 SDT PDU,那么,应检验 PDU 以确保一个且仅一个标号或标号参考内容字段出现。若出现,应检验该标号的值以确保它包含在 Label _ Set 的集中;

g) 应检验与 NLSP 服务参数相关的内容字段或其他协议功能,如第 7 章和第 8 章中的规程要求的那样出现。从这些字段中恢复数据并根据第 7 章和第 8 章中的规程处理。

6.4.2.2 无报头出现(仅 NLSP-CO)

如第 8 章中使用的,应执行下列:

a) 应调用使用该 SA 定义的解封功能(例如第 12 章中描述的)且传递下列自变量:

1) SA-ID 应置为 My _ SA-ID；

2) unit-data-type 应置为：

- “expedited”，若要解封的数据来源于 UN-EXPEDITED-DATA 原语；
- “normal”，否则；

3) 封装的八位位组串应置为 UN 用户数据参数。

b) 解封功能应返回差错或封装前八位位组串。

6.5 安全联系协议的使用

当两个 NLSPE 没有建立 SA 时，它们可能使用安全联系协议(SA-P)或其他方法建立 SA。SA-P 在 NLSPE 之间交换其内容数据类型置为 SA-P 的 SA PDU 或 SDT PDU，以建立、更新或终止 SA。

NLSP 第 7 章和第 8 章定义如何使用可能调用的 SA-P，但没有 SA-P 规程，SA-P 的规程和包含在 SA PDU/SDT PDU 中的 PCI 取决于用来提供 SA-P 的特定机制(附录 C 中定义了合适的协议机制)。任何 SA-P 应提供下列特征：

a) 选择的保护形式所要求的所有 SA 属性的派生；

b) 来自鉴别过的源的密钥；

c) 若要求，用于鉴别和完整性的初始信息的建立。

若不支持特定的 SA-P，NLSPE 应丢弃 SA PDU。

SA-P 可能基于对称的或不对称的算法。建议使用不对称算法。附录 C 包含该机制的例子。

7 NLSP-CL 的协议功能

7.1 NLSP-CL 提供的服务

NLSP 提供的服务可用带前缀“NLSP”来引用。原语是：

原语	参数
NLSP-UNITDATA Request	NLSP Destination Address(目的地址)
Indication	NLSP Source Address(源地址)
	NLSP Quality of Service(服务质量)
	NLSP Userdata(用户数据)

服务原语和参数直接相当于 GB/T 15126 中定义的。

7.2 所承担的服务

由 NLSP 在其低边界上所承担的服务可用带前缀“UN”(即“底层网”)来引用。原语是：

原语	参数
UN-UNITDATA Request	UN Called Address(被叫地址)
Indication	UN Calling Address (主叫地址)
	UN Quality of Service(服务质量)
	UN Userdata(用户数据)

所承担的服务原语和参数相当于 CLNS 中定义的(见 GB/T 15126/ADI)。

7.3 安全联系属性

下列属性控制了 NLSP-CL 的操作。它们的描述包括在本规范内涉及这些属性使用的助记符。

注：SA 属性是“ASSR 约束”的地方，该约束可定义单个值或值的集合。在 ASSR 定义值的范围中，可由 OSI 系统管理、SA-P 交换或本规范外的其他方法建立属性值。

为 SA 选择的安全服务：

DOAuth：由 ASSR 数据原发鉴别级别约束范围的整数。

该属性的值应预先建立或在 SA 建立时设置。

CLConf：由 ASSR 无连接保密性级别约束范围的整数。

该属性的值应预先建立或在SA 建立时设置。

CLInt：由 ASSR 无连接完整性级别约束范围的整数。

该属性的值应预先建立或在SA 建立时设置。

7.4 检验

下列叙述的许多点中，NLSP-CL 实体检验一些被满足的条件。除非另外规定，每当这样的一个检验失败，NLSP-CL 实体应丢弃当前正在处理的数据。任选地，该实体也可以存档审计报告，要审计的故障被认为是本地事情。

7.5 带内 SA 建立

使用安全联系协议(SA-P)可以带内的建立一个SA。本规范附录C 定义了SA-P。

注：目前，SA-P 不包括任何恢复规程，因此要小心当 NLSP-CL 使用本协议时提供的请求的可靠性。

7.6 处理 NLSP-UNITDATA Request

7.6.1 SA 的初始检验和标识

收到 NLSP-UNITDATA Request 时，NLSPE 检验是否允许基于本地安全服务要求和源/目的地址对的无保护通信。若允许无保护通信，NLSP 服务参数应直接拷贝到 UN-UNITDATA Request 中相同的 UN 服务参数上，并且 NLSPE 不再产生进一步动作。

若需要保护的通信，应执行 6.3 中所述的初始检验和SA 规程的标识，并跟在下列规程后。

7.6.2 NLSP-UNITDATA 保护

NLSPE 应执行 6.4.1.1 定义的“产生 SDT PDU 功能”，其数据类型“NLSP-UNITDATA reg/in”包含：

a) 若 Param _ Prot 为 TRUE，源 NLSP 地址；

b) 若 Param _ Prot 为 TRUE，目的 NLSP 地址；

c) NLSP 用户数据参数。

Last/Not last 标志应置为 Last(即，数据类型字段的第 7 位=0)。

7.6.3 网络请求

SDT PDU 应作为 UN-UNITDATA Request 的 UN 用户数据参数传递给下一低层协议。

若 Param _ Prot 为 TRUE，UN 源地址应是本地 NLSP 实体 UN 地址，否则 NLSP 源地址应拷贝到 UN 源地址。

若 Param _ Prot 为 TRUE，UN 目的地址应是 Peer _ Adr，否则 NLSP 目的地址应拷贝到 UN 目的地址。

UN QOS 应由本地策略确定，但可以从 NLSP QOS 拷贝来。

注：若记录路由和源路由参数在 NLSP QOS 参数中，且不作为 UN QOS 参数传递，那么规定的 QOS 不能提供源和目的 NLSP-CL 实体间的路由部分。

7.7 处理 UN-UNITDATA Indication

7.7.1 初始检验和处理

若不出现 SDT PDU，NLSPE 检验是否允许基于本地安全服务请求和源/目的地址对的无保护通信。若允许无保护通信，UN 服务参数应直接拷贝到 NLSP UNITDATA Request 中相同的 NLSP 服务参数，并且 NLSP 不再产生进一步的动作。若不允许无保护通信，则执行 7.4 中描述的规程，NLSP 不再产生进一步动作。

若出现 SDT PDU，NLSP 应在 SA 之中识别对它可用的一个 SA，其 My _ SA-ID 等于收到的 SDT PDU 中的 SA-ID 字段。所有进一步的操作与该标识的 SA 相关。

NLSP 应执行 6.4.2.1 中定义的公共处理。此外，应执行下列检验：

a) 若数据类型字段“与任何 NLSP 服务原语无关”，则在这些规程下，应不再处理 SDT PDU。否则数据类型字段应检验为 NLSP-UNITDATA。

注

1 忽略“Last/Not last 标志”的值(即数据类型字段的第7位)。

2 对通信量填充或无连接方式中的测试交换的支持不在NLSP的范围内。

b) 若Param _ Prot为TRUE,应检验SDT PDU以确保出现下列字段:

1) 目的地址;

2) 源地址。

NLSP UNITDATA Indication应被传递给NLSP用户,其参数设置和地址检验如7.7.2中定义。

7.7.2 NLSP-CL Indication中的参数

7.7.2.1 地址参数

若Param _ Prot为TRUE,则NLSPE应置NLSP服务参数为包含在SDT PDU中的值。

若Param _ Prot为FALSE,则应从UN指示参数中取值如下:

a) NLSP源地址=UN源地址;

b) NLSP目的地址=UN目的地址。

检验上面置的NLSP目的地址是本地安全策略确定的该NLSP实体服务的NLSP地址。

检验上面置的NLSP源地址是包含在SA属性Adr _ Served中的NLSP地址。

7.7.2.2 QOS

QOS参数从UN服务拷贝到NLSP服务。

7.7.2.3 用户数据

用户数据字段中的数据应从SDT PDU的封装前八位位组串中传递到NLSP-UNITDATA Indication的NLSP用户数据参数中的NLSP用户。

8 NLSP-CO的协议功能

8.1 NLSP-CO提供的服务

NLSP-CO提供的服务原语是:

原语	参数
NLSP-CONNECT Request Indication	NLSP Called Address(被叫地址) NLSP Calling Address(主叫地址) NLSP Receipt Confirmation Selection(接收证实选择) NLSP Expedited Data Selection(加快数据选择) NLSP QOS Parameter Set(参数集) NLSP Userdata(用户数据)
NLSP-CONNECT Response Confirm	NLSP Responding Address(响应地址) NLSP Receipt Confirmation Selection(接收证实选择) NLSP Expedited Data Selection(加快数据选择) NLSP QOS Parameter Set(参数集) NLSP Userdata(用户数据)
NLSP-DATA Request Indication	NLSP Userdata(用户数据) NLSP Confirmation Request(证实请求)
NLSP-DATA-ACKNOWLEDGE Request Indication	
NLSP-EXPEDITED DATA Request	NLSP Userdata(用户数据)

Indication	
NLSP-RESET Request	NLSP Reason(原因)
NLSP-RESET Indication	NLSP Originator(原发者) NLSP Reason(原因)
NLSP-RESET Response Confirm	
NLSP-DISCONNECT Request Indication	NLSP Originator(原发者) NLSP Reason (原因) NLSP Userdata(用户数据) NLSP Responding Address(响应地址)

注：原发者不用于请求。

服务原语和参数直接相当于GB/T 15126中定义的那些。

8.2 所承担的服务

由 NLSP 在其低边界上所承担的服务可用带前缀“UN”(即“底层网”)来引用，这是概念接口(见5.1)。

UN 接口被模型化为两部分：

a) UN 服务原语和参数的定义(见下)；

b) 从UN 服务(见5.1)到标准网络服务或直接到GB/T 16974 的映射。

附录A 和附录B 定义了从概念服务接口到网络服务和到GB/T 16974 的映射。

NLSP-CO 假定的UN 原语是：

原语	参数
UN-CONNECT Request Indication	UN Called Address(被叫地址) UN Calling Address(主叫地址) UN Receipt Confirmation Selection(接收证实选择) UN Expedited Data Selection(加快数据选择) UN QOS Parameter Set(参数集) UN Userdata(用户数据) UN Authentication(鉴别)[1)]
UN-CONNECT Response Confirm	UN Responding Address(响应地址) UN Receipt Confirmation Selection(接收证实选择) UN Expedited Data Selection(加快数据选择) UN QOS Parameter Set(参数集) UN Userdata(用户数据) UN Authentication(鉴别)[1)]
UN-DATA Request Indication	UN Userdata(用户数据) UN Confirmation Request(证实请求)
UN-DATA-ACKNOWLEDGE Request Indication	

1) UN 鉴别参数用于运送CSC PDU。当NLSP 用于与GB/T 16974 连接，而DTE 保护设施字段可运送UN 鉴别参数时，这是有效编码(见附录B)。

UN-EXPEDITED-DATA Request Indication	UN Userdata(用户数据)
UN-RESET Request	UN Reason(原因)
UN-RESET Indication	UN Originator(原发者) UN Reason(原因)
UN-RESET Response Confirm	
UN-DISCONNECT Request	UN Reason(原因) UN Userdata(用户数据) UN Responding Address(响应地址)
UN-DISCONNECT Indication	UN Originator(原发者) UN Reason (原因) UN Userdata(用户数据) UN Responding Address(响应地址)

附录A和附录B定义UN鉴别到GB/T 15126和GB/T 16974上的映射。

注：当NLSP用于与GB/T 16974充分紧密耦合时，它可能使用能获得全部优点的底层协议的选择编码，而到GB/T 15126的不同映射假定只使用底层网服务。

8.3 安全联系属性

下列属性控制NLSP-CO的操作。它们的描述包括在本规范内涉及这些属性使用的助记符。

注：SA的属性是“ASSR约束”的地方，该约束可以定义单个值或值的集合。

在ASSR定义值的范围中，可由OSI系统管理、SA-P交换或本规范外的其他方法建立属性值。

a）SA选择的安全服务：

PE Auth：

ASSR约束范围的整数；

对等实体鉴别级别。

CO Conf：

ASSR约束范围的整数；

连接保密性级别。

CO Int：

ASSR约束范围的整数；

无恢复的连接完整性。

这些属性的值应预先建立或在SA建立时设置。

b）相关的CO协议属性：

Retain _ On _ Disconnect：布尔类型

SA属性是否保持在断开状态。

该属性的值应在SA建立时或预先建立设置。

Protect _ Connect _ Param：布尔类型

保护在NLSP _ CONNECT和NLSP _ DISCONNECT中NLSP用户数据，若Param _ Prot为TRUE，也保护NLSP-CONNECT和NLSP-DISCONNECT中的其他服务参数。

ASSR约束该属性的值。

注：若Protect _ Connect _ Param为FALSE，Param _ Prot不能为TRUE。

No _ Header：布尔类型

若为真，基于无报头的保护将用于保护数据(例如使用第12章中定义的规程)。

ASSR 约束该属性的值。

8.4 检验和其他公共功能

在下列描述的许多点上，说明了要满足的一些条件。除非另有规定，每当NLSP 连接或NLSP 断开规程中的检验失败，应适当地发出UN-DISCONNECT Request 和NLSP-DISCONNECT Indication。若该情况发生在连接建立后面，NLSPE 应丢弃当前正在处理的数据，作为本地判定，应调用下列之一：

a) NLSP 启动如8.8.5 中定义的UN-RESET 规程；

b) UN-DISCONNECT Request 和NLSP-DISCONNECT Indication。

实体也可以任选地存档审计报告。决定记录什么审计信息是本地事情。

类似的，事件的期望序列在下面描述的规程中给出。若不跟随该序列，则不期望事件应以与检验失败相同的方法处理。

在下列描述涉及的生成或CSC PDU 检验或安全数据传送PDU，应执行合适的机制特定规程，例如本规范中的第9 章到第12 章中描述的那些规程。

8.5 NLSP 连接功能

8.5.1 初始规程

8.5.1.1 初始检验——NLSP CONNECT Request

收到NLSP-CONNECT Request，NLSPE 应检验是否允许基于本地安全服务要求和主叫/被叫地址对的无保护通信。若允许无保护通信，NLSP 和UN 服务参数直接拷贝到所有后继NLSP 和UN 服务原语的相同的UN 和NLSP 服务参数，直到收到UN-DISCONNECT Indication 后。NLSPE 在连接持续期间不产生进一步的动作。

若要求保护通信，NLSPE 应跟随初始检验规程和6.3.1 及6.3.2 中各自描述的安全联系的标识。8.5.2、8.5.3 或8.5.4 中定义的规程跟随在这后，适当的规程取决于8.5.1 中定义的选择的连接建立方式。UN 连接的后继UN-CONNECT 和NLSP-CONNECT 服务原语使用相同的条。

8.5.1.2 NLSP 连接建立方式

若SA 当前存在具有要求的特性，则可用于保护连接。否则，应建立新的SA，作为NLSP-CONNECT 功能部分的带内或在给出的超时间隔内的带外。若这两者都不执行，应返回NLSP-CONNECT。

有两种建立具有变化的NLSP 连接的基本方式来支持下列带内SA 建立：

a) UN-CONNECT 中的NLSP-CONNECT，其中协议交换以提供鉴别，并且在UN-CONNECT 参数中携带交换NLSP-CONNECT 参数；

b) UN-CONNECT 中具有SA-P 的NLSP-CONNECT，在建立具有鉴别的第二UN 连接前，其中在预先建立上的UN-DATA 中携带带内SA 建立，且如上面a)中的在UN-CONNECT 中携带在NLSP-CONNECT 参数；

c) UN-DATA 中的NLSP-CONNECT，其中鉴别交换携带在UN-CONNECT 中，UN-DATA 中的NLSP-CONNECT 参数的交换跟随着；

d) UN-DATA 中具有SA-P 的NLSP-CONNECT，其中SA-P 交换携带在UN-DATA 中，接着交换UN-DATA 中的NLSP-CONNECT 参数。

最合适的方式选择是基于NLSP 连接建立要求(或期望的要求)主叫NLSPE 和NLSP 操作的轮廓环境做出的本地判定。

SA-P 的选择由CSC PDU 中的SA-P 标志指明，UN-CONNECT 中的NLSP-CONNECT 或UN-DATA 中NLSP-CONNECT 的选择由UNC-UND 标志(见表2)对远程NLSPE 指明。

在后两种方式中(有或没有SA-P 的UN-DATA 中的NLSP-CONNECT)在SDT-PDU 中编码NLSP-CONNECT 参数。因此，这些方式不能用于无报头方式。

在前两种方式中(有或没有SA-P 的UN-CONNECT 中的NLSP-CONNECT)，若No _ Header 为

FALSE 且 Protect _Connect _Param 为 TRUE，在 SDT PDU 中要保护 NLSP-CONNECT 参数。但是，若结果的 SDT PDU 大于 UN-CONNECT UN 用户数据中的可用空间，这些方式不能使用。

表 1 指明了上面定义的连接建立的不同方式的限制，它可用于确定呼叫建立的哪些规程对给定的轮廓是合适的。

8.5.1.3 初始检验——UN-CONNECT Indication

收到在 UN 鉴别参数中不出现 CSC PDU 的 UN-CONNECT Indication，NLSPE 应检验是否允许基于本地安全服务请求和主叫/被叫地址对的无保护通信。若允许无保护通信，NLAP 和 UN 服务参数直接拷贝到所有后继 NLSP 和 UN 服务原语相同的 UN 和 NLSP 服务参数上，直到收到 UN-DISCONNECT Indication 后。在连接持续阶段 NLSPE 不产生进一步的动作。

若不允许无保护通信且不出现 CSC PDU，则为检验故障执行 8.4 中定义的规程。

若出现 CSC PDU，则执行 8.5.2、8.5.3 或 8.5.4 中定义的规程，这取决于表 2 中给出的 PDU 类型字段中的 SA-P 和 UNC-UND 标志位的值。正设置的 SA-P 标志指示来指明带内 SA-P 交换要由 NLSP 携带。正设置的 UNC-UND 标志指明 NLSP-CONNECT 由 UN-DATA 携带而不是 UN-CONNECT。UN 连接的后继 UN-CONNECT 和 NLSP-CONNECT 服务原语使用相同的条。

表 1 给出 NLSP 连接建立方式限制的表

SAP	无报头	Protect _ Connect _ Params	SDT PDU 长度限制（见注）	方 式	连接建立规程
TRUE	TRUE	EITHER		UN-CONNECT 中具有 SA-P 的 NLSP-CONNECT	先 8.5.2.2 8.5.2.4 后 8.5.3
	FALSE	TRUE	SDT〈＝最大 UN 用户数据	UN-CONNECT 中具有 SA-P 的 NLSP-CONNECT	先 8.5.2.2 8.5.2.4 后 8.5.3
TRUE	FALSE	FALSE		UN-CONNECT 中具有 SA-P 的 NLSP-CONNECT	先 8.5.2.2 8.5.2.4 后 8.5.3
TRUE	FALSE	EITHER		UN-DATA 中具有 SA-P 的 NLSP-CONNECT	8.5.4
FALSE	TRUE	EITHER		UN-CONNECT 中的 NLSP-CONNECT	8.5.2
FALSE	FALSE	TRUE	SDT〈＝最大 UN 用户数据	UN-CONNECT 中的 NLSP-CONNECT	8.5.2
FALSE	FALSE	FALSE		UN-CONNECT 中的 NLSP-CONNECT	8.5.2
FALSE	FALSE	EITHER		UN-DATA 中的 NLSP-CONNECT	8.5.4

EITHER：表示在 Protect _Connect _Param 栏目下面的该处是 TRUE 或 FALSE。

注

1 SDT 涉及 SDT PDU 的最大可能长度，它可能在 NLSP 操作的轮廓环境的连接建立期间产生。

2 假定与 UN 用户数据相同的限制用于 NLSP 用户数据的长度。

3 对于映射到 GB/T 15126“最大用户数据”的 UN，可携带在网络服务 UN-CONNECT 服务原语中的最大用户数据（例如，对 GB/T 16976 和 GB/T 16974 为 128）小于 CSC PDU 的长度。

4 对于直接映射到 GB/T 16974“最大 UN 用户数据”的 UN 是 128。

表 2　识别 NLSP 连接建立规程的 CSC PDU 标志

UNC-UND 标志	SA-P 标志	NLSP 连接建立规程
置位	置位	8.5.4(UN-DATA 中的 NLSP-CONNECT)
置位	清除	8.5.4(UN-DATA 中的 NLSP-CONNECT)
清除	置位	8.5.3(UN-CONNECT 中具有 SA-P 的 NLSP-CONNECT)
清除	清除	8.5.2(UN-CONNECT 中的 NLSP-CONNECT)

8.5.2　UN-CONNECT 中的 NLSP-CONNECT

UN-CONNECT 中具有 NLSP-CONNECT 参数的 NLSP 连接建立期望的事件序列在图 1 中说明。

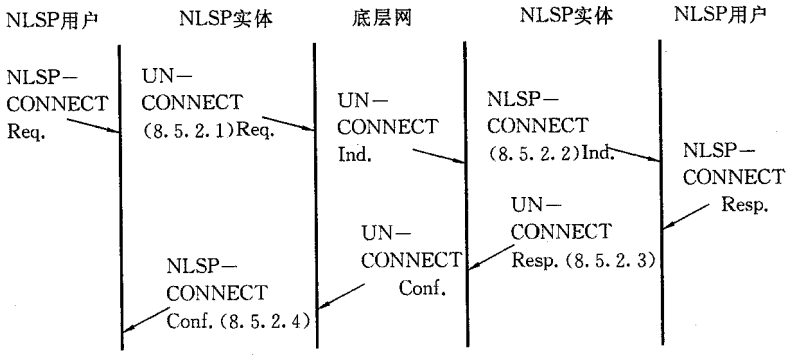


图 1　UN-CONNECT 中 NLSP-CONNECT 的服务原语时序图

8.5.2.1　NLSP-CONNECT Request

若 NLSP-CONNECT 参数携带在 UN-CONNECT 中，在 NLSP-CONNECT Request 上应执行下列规程：

a）若 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 TRUE，则如 6.4.1.2 中所述的那样封装任何 NLSP 用户数据，把它放置于 UN 用户数据中；

b）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则产生 SDT PDU，包含 6.4.1.1 中所述的被叫 NLSP 地址、NLSP 主叫地址和 NLSP 用户数据，它具有数据类型“NLSP-CONNECT req/ind”。把它放置于 UN 用户数据中；

c）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 FALSE，则产生 SDT PDU，若出现的话，包含 6.4.1.1 中所述的 NLSP 用户数据，它具有数据类型“NLSP-CONNECT req/ind”，把它放置于 UN 用户数据中；

d）若 Protect _ Connect _ Param 为 FALSE，则 NLSP 用户数据放置于 UN 用户数据中；

e）准备 CSC PDU 且：

1）UNC-UND 标志清除；

2）当前 SA 的 SA-ID 放在 SA-ID 字段中；

3）SA-P 标志清除；

4）按机制特定规程的要求，CSC 内容置为 CSC 第一交换，如 10.3 中所述的。

f）应调用 UN-CONNECT Request 且：

1）若 Param _ Prot 为真则 UN 被叫地址置为 Peer _ Adr，否则 NLSP 被叫地址置为 Peer _ Adr；

2）若 Param _ Prot 为真则 UN 主叫地址置为本地 NLSPE UN 地址，否则 NLSP 主叫地址置为本地 NLSPEUN 地址；

3）UN 接收证实选择和加快数据选择置为从 NLSP 接收证实选择和加快数据选择本地确定的值；

4）UN QOS 参数置为从 NLSP QOS 参数本地确定的值；

5) UN 用户数据置成如上面 a)至 d)中所述的；

6) UN 鉴别置成如上面 e)中所述的 CSC PDU。

g) 主叫 NLSP 等待如 8.5.2.4 中所述的 UN-CONNECT Confirm 或如 8.10 中所述的 UN-DISCONNECT Indication。

8.5.2.2 UN-CONNECT Indication——UNC-UND 清除和 SA-P 清除

收到 UN-CONNECT Indication，其 UN 鉴别包含 CSC PDU，其 UNC-UND 标志清除且 SA-P 标志清除：

a) NLSPE 应在可用的 SA 间标识一个 SA，其 My _ SA-ID 等于收到的 CSC PDU 中的 SA-ID 字段，所有进一步的操作涉及该标识了的 SA；

b) 按 10.3 中所述的机制特定规程的要求检验 CSC PDU 内容，应保持返回的响应 CSC PDU 内容，以便用于处理如 8.5.2.3 中所述的 NLSP-CONNECT Response；

c) 若 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 TRUE，则如 6.4.2.2 中所述的那样解封任何 UN 用户数据。它放置于 NLSP 用户数据中。从 UN-CONNECT Indication 参数拷贝其他 NLSP-CONNECT Indication 参数；

d) 若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则如 6.4.2.1 那样检验 UN 用户数据中的 SDT PDU。应检验数据类型字段为 NLSP-CONNECT req/ind。NLSP 被叫地址、NLSP 主叫地址及 SDT PDU 中的 NLSP 用户数据内容字段应放置于 NLSP-CONNECT Indication 参数中。UN 收到证实选择、加快数据选择以及 UN QOS 参数集应拷贝到相同的 NLSP-CONNECT Indication 参数中；

e) 若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 FALSE，则 UN 用户数据中的 SDT PDU 若出现，按 6.4.2.1 所述检验。应检验数据类型字段为 NLSP-CONNECT req/ind。SDT-PDU 中的用户数据内容字段应放置于 NLSP 用户数据中。应从 UN-CONNECT Indication 参数拷贝其他 NLSP-CONNECT Indication 参数；

f) 若 Protect _ Connect _ Param 为 FALSE，则所有的 UN-CONNECT Indication 参数拷贝到 NLSP-CONNECT Indication 参数中；

g) 应检验如上所述设置的 NLSP 被叫地址是为本地确定的 NLSP 实体服务的 NLSP 地址；

h) 应检验如上所述设置的 NLSP 主叫地址是 SA 属性 Adr _ Served 中的 NLSP 地址；

i) 若为连接建立了任何安全标号，应检验它不是 SA 属性 Label _ Set 中授权的标号集；

j) NLSP-CONNECT Indication 应传递给 NLSP 用户；

注：在传递给 NLSP 用户之前，NLSP 接收证实选择、加快数据选择和 NLSP QOS 参数集可以被更新为本地确定的值。

k) 被叫 NLSPE 等待 8.5.2.3 中所述的 NLSP-CONNECT Response 或 8.10 中所述的 NLSP-DISCONNECT Request 或 UN-DISCONNECT Indication。

8.5.2.3 LSP-CONNECT Response

收到 NLSP-CONNECT Response 时：

a) 若 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 TRUE，则如 6.4.1.2 中所述那样封装 NLSP 用户数据，把它放置于 UN 用户数据中；

b) 若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则产生 SDT PDU，包含 NLSP 响应地址以及 6.4.1.1 中所述的 NLSP 用户数据，它具有数据类型“NLSP-CONNECT res/conf”，把它放置于 UN 用户数据中；

c) 若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE，Param-Prot 为 FALSE 且出现 NLSP 用户数据，则产生 SDT PDU，它包含 6.4.1.1 中所述的 NLSP 用户数据，具有数据类型“NLSP-CONNECT res/conf”，把它放置于 UN 用户数据中；

d）若 Protect _ Connect _ Param 为 FALSE，则 NLSP 用户数据放置于 UN 用户数据中；

e）若在 UN 用户数据中不能符合上面 a)到 d)产生的数据，则如 8.4 中所述夭折这些规程；

f）应产生 CSC PDU 且：

1）SA-P 和 UNC-UND 标志清除；

2）SA-ID 到 SA-ID，如同 UN-CONNECT Indication 中接收 CSC PDU 中的；

3）CSC 内容置为从 8.5.2.2 b)中机制特定规程的先前调用所返回的值；

g）发送 UN-CONNECT Response 且：

1）若 Param _ Prot 为 TRUE，UN 响应地址置为本地 NLSP 实体 UN 地址，否则为 NLSP 响应地址参数；

2）UN 接收证实选择和加快数据选择置为从 NLSP 接收证实选择和加快数据选择本地确定的值；

3）UN QOS 参数置为从 NLSP QOS 参数确定的值；

4）如上面 a)到 d)中所述的 UN 用户数据；

5）UN 鉴别置成上面 g)中所述的 CSC PDU；

h）若在机制特定规程下要求鉴别和 CSC 交换(如 10.3 中所述)，在完成 NLSP 连接建立和从 NLSP用户处理 NLSP-DATA 原语之前，被叫 NLSPE 可等待 UN-DATA 中的 SDT PDU。否则，被叫 NLSPE现已完成 NLSP 连接建立规程，并可进入数据传送阶段。

注：若 CSC 交换机制要求多于两个 CSC-PDU 的交换，则连接建立完成前在 UN-DATA 中交换它们。

8.5.2.4 UN-CONNECT Confirm——UNC-UND 清除和 SA-P 清除

收到 UN-CONNECT Confirm，其 UN 鉴别包含 CSC PDU 同时 UNC-UND 和 SA-P 标志都清除：

a）用机制特定规程检验 CSC PDU 内容，如 10.3 中所述；

b）若 Protect _ Connect _ Param 为 TRUE，且 No _ Header 为 TRUE，则如 6.4.2.2 中所述的那样解封任何 UN 用户数据。把它放置于 NLSP 用户数据中，其他 NLSP-CONNECT Confirm 参数从 UN-CONNECT Confirm 参数中拷贝；

c）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则如 6.4.2.1 中所述那样检验 UN 用户数据中的 SDT PDU。检验数据类型字段为 NLSP-CONNECT res/conf。NLSP 响应地址和 SDT PDU 中的 NLSP 用户数据内容字段应放置于 NLSP-CONNECT Confirm 参数。UN 接收证实选择和加快数据选择参数及 UN QOS 参数集被拷贝到 NLSP-CONNECT Confirm 参数；

d）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 FALSE，则若出现，UN 用户数据中的 SDT PDU 如 6.4.2.1 中所述那样检验。检验数据类型字段为 NLSP-CONNECT res/conf。SDT-PDU 中的用户数据内容字段应放置于 NLSP 用户数据。其他的 NLSP-CONNECT Confirm 参数应从 UN-CONNECT Confirm 参数拷贝；

e）若 Protect _ Connect _ Param 为 FALSE，则所有的 UN-CONNECT Confirm 参数应拷贝到 NLSP-CONNECT Confirm 参数；

f）若出现 NLSP 响应地址，应对包含在 SA 属性 Adr _ Served 中的 NLSP 地址进行检验；

g）NLSP 连接证实应传递给 NLSP 用户；

h）若在机制特定规程下请求鉴别和 CSC 交换(如 10.3 中所述的)，则如 6.4.1.1 所述那样创建 SDT PDU，其数据类型“与任何 NLSP 服务原语无关”不包含内容字段而不同于第 6 章中要求的那样。这应发送 UN-DATA 原语的 UN 用户数据。

注：若 CSC 交换机制要求多于两个 CSC-PDU 的交换，则在连接建立完成前在 UN-DATA 中交换它们。

现在，完成了 NLSP 连接建立规程。

8.5.3 UN-CONNECT 中具有 SA-P 的 NLSP-CONNECT

期望的事件序列在图 2 中说明。

8.5.3.1 NLSP-CONNECT Request

在 **NLSP-CONNECT Request** 上，若 **NLSP-CONNECT** 携带在 **UN-CONNECT** 中，且选择了带内 **SA** 建立，应执行下列规程：

a) 应准备 **CSC PDU** 且：

1) **UNC-UND** 标志清除；

2) 置 **SA-P** 标志且 **SA-ID**、内容长度和 **CSC PDU** 内容不出现；

b) 应发送 **UN-CONNECT Request** 且：

1) **UN** 被叫地址设为 **Peer _ Adr**；

2) **UN** 主叫地址置为本地 **NLSP** 实体 **UN** 地址；

3) **UN** 接收证实选择置为本地确定的值；

4) **UN** 加快数据选择置为本地确定的值；

5) **UN QOS** 参数置为本地确定的值；

6) **UN** 用户数据空；

7) **UN** 鉴别置为 **CSC PDU**；

c) 主叫 **NLSPE** 应等待 **8.5.3.3** 中所述的 **UN-CONNECT Confirm** 或 **8.10** 中所述的 **UN-DISCONNECT Indication**。

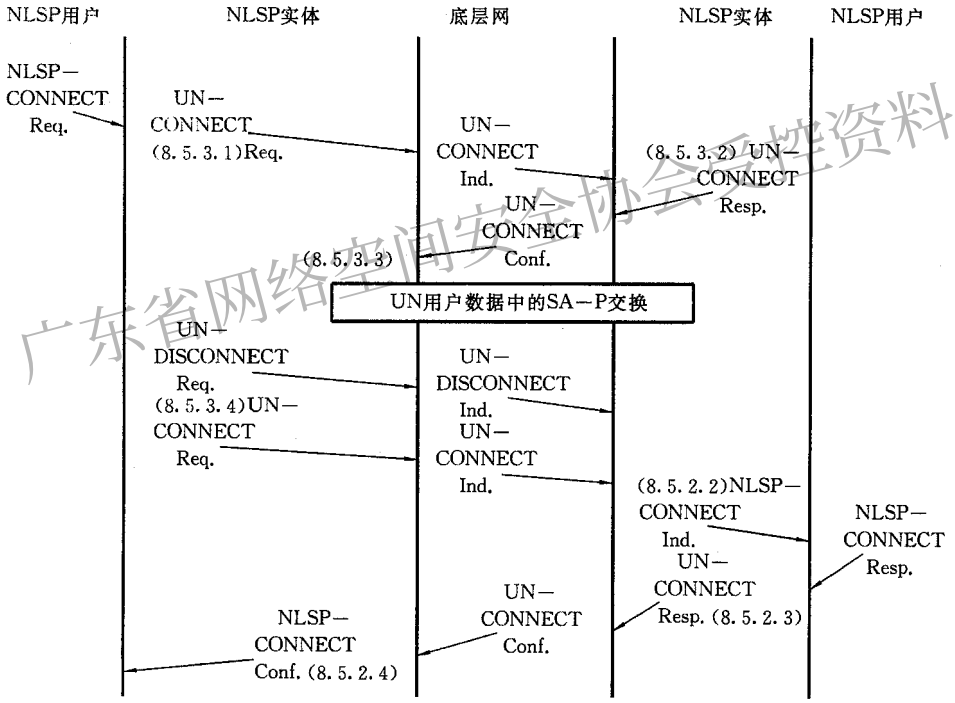


图 2 **UN-CONNECT** 中具有 **SA-P** 的 **NLSP-CONNECT** 的服务原语时序图

8.5.3.2 UN-CONNECT Indication——UNC-UND 清除和 **SA-P** 设置

收到其 **UN** 鉴别包含 **CSC PDU** 的 **UN-CONNECT Indication**，**UNC-UND** 标志清除且 **SA-P** 标志设置：

a) **NLSP** 应准备 **CSC PDU** 且：

1) **UNC-UND** 标志清除；

2) **SA-P** 标志设置；

3) **CSC** 内容空；

b) NLSPE 应接着应答 UN-CONNECT Response 且：

1) UN 响应地址置为本地 UN 地址；

2) UN 接收证实选择和加快数据选择置为从 UN-CONNECT Indication 中的参数本地确定的值；

3) UN QOS 参数置为从 UN-CONNECT Indication 中的 UN QOS 参数本地确定的值；

4) UN 用户数据空；

5) UN 鉴别置为 CSC PDU。

被叫 NLSPE 应等待 8.10 中所述的 SA-P 交换或 UN-DISCONNECT Indication，SA-P 中的任何差错应当作 8.4 中所述的差错处理。

8.5.3.3 UN-CONNECT Confirm——UNC-UND 清除和 SA-P 设置

收到其 UN 鉴别包含响应 CSC PDU 的 UN-CONNECT Confirm，UNC-UND 标志清除且 SA-P 标志设置：

a) 应执行带内 SA-P；

b) 主叫 NLSPE 等待如 8.5.3.4 中所述的 SA-P 完成或 8.10 中所述的 UN-DISCONNECT。

8.5.3.4 SA-P 完成

在 8.5.3.3 中所述的 SA-P 的完成中，主叫 NLSPE 应执行下列规程：

a) 主叫 NLSPE 应发送 UN-DISCONNECT Request 且原因置为“disconnect-normal-condition”。接着，具有服务参数的 UN-DISCONNECT Request 设置如下；

b) 若 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 TRUE，则如 6.4.1.2 中所述封装任何 NLSP 用户数据。把它放置于 UN 用户数据中；

c) 若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则产生 SDT PDU，包含 6.4.1.1 中所述的 NLSP 被叫地址、NLSP 主叫地址和 NLSP 用户数据，具有数据类型“NLSP-CONNECT req/ind”。把它放置于 UN 用户数据中；

d) 若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 FALSE，则产生 SDT PDU，若出现的话，包含 6.4.1.1 中所述的 NLSP 用户数据，具有数据类型“NLSP-CONNECT req/ind”。把它放置于 UN 用户数据中；

e) 若 Protect _ Connect _ Param 为 FALSE，则 NLSP 用户数据放置于 UN 用户数据中；

f) 准备 CSC PDU 且：

1) UNC-UND 标志清除；

2) 当前 SA 的 SA-ID 放置于 SA-ID 字段中；

3) SA-P 标志被清除；

4) CSC 内容按机制特定规程的要求置为 CSC 第一交换，如 10.3 中所述；

g) 应调用 UN-CONNECT Request 且：

1) 若 Param _ Prot 为 TRUE，则 UN 被叫地址置为 Peer _ Adr，否则 NLSP 被叫地址置为 Peer _ Adr；

2) 若 Param _ Prot 为 TRUE，则 UN 主叫地址置为本地 NLSP 实体 UN 地址，否则 NLSP 主叫地址置为本地 NLSP 实体 UN 地址；

3) UN 接收证实选择和加快数据选择置为从 NLSP 接收证实选择和加快数据选择本地确定的值；

4) UN QOS 参数置为从 NLSP QOS 参数本地确定的值；

5) UN 用户数据按上面 a)到 d)所述的设置；

6) UN 保密性置为如上面 e)中所述的 CSC PDU；

h) 主叫 NLSPE 等待 8.5.2.4 中所述的 UN-CONNECT Confirm 和 8.10 中所述的 UN-

DISCONNECT Indication。

在SA-P 的完成中，NLSP 等待 UN-DISCONNECT，且原因置为“disconnect-normal-condition”。在该 UN-DISCONNECT Indication 上，被叫 NLSPE 接着等待 8.5.2.2 中所述的 UN-CONNECT Indication。

主叫和被叫 NLSPE 接着应处理 8.5.2.2 到 8.5.2.4 中所述的后继 NLSP 和 UN-CONNECT 原语。

8.5.4 UN-DATA 中的 NLSP-CONNECT

期望的事件序列在图 3 中说明。

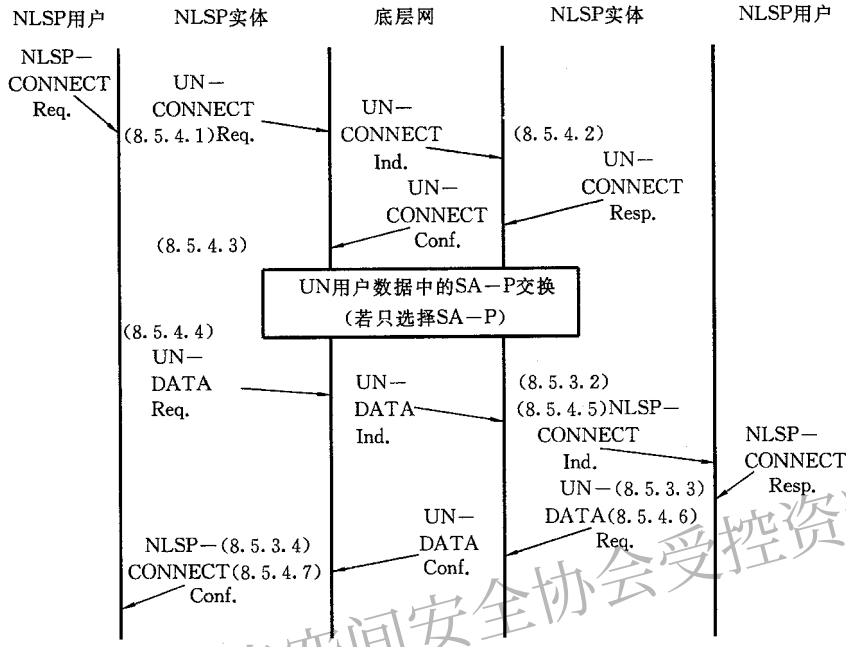


图 3 UN-DATA 中 NLSP-CONNECT 的服务原语时序图

8.5.4.1 NLSP-CONNECT Request

在 NLSP-CONNECT Request 中，若 NLSP-CONNECT 参数携带在 UN-DATA 中，应执行下列规程：

a）应准备 CSC PDU 且：

1）UNC-UND 标志设置；

2）若选择了带内 SA-P，则置 SA-P 标志且 SA-ID、内容长度和 CSC PDU 内容字段不出现；

3）若不选择带内 SA-P，则 SA-P 标志清除，按照 10.3 中所述的机制特定规程的要求，SA-ID 置为 Your _ SA-ID 且 CSC PDU 内容置为 CSC 第一交换；

b）应发送 UN-CONNECT Request 且：

1）UN 被叫地址置为 Peer _ Adr；

2）UN 主叫地址置为本地 NLSP 实体 UN 地址；

3）UN 接收证实选择置为从 NLSP 接收证实本地确定的值；

4）UN 加快数据选择置为从 NLSP 加快数据选择本地确定的值；

5）UN QOS 参数置为从 NLSP QOS 本地确定的值；

6）UN 用户数据空；

7）UN 鉴别置为 CSC PDU；

c）主叫 NLSPE 应等待 8.5.4.3 中所述的 UN-CONNECT Confirm 或 8.10 中所述的 UN-DISCONNECT Indication。

8.5.4.2 UN-CONNECT Indication——UNC-UND 设置

收到其 UN 鉴别包含 CSC PDU 的 UN-CONNECT Indication 时，标志设置：

a）若 SA-P 标志清除，则：

1）NLSPE 应在可用的 SA 之间标识一个 SA，它的 My _SA-ID 等于收到的 CSC PDU 中的 SA-ID 字段，所有进一步的操作涉及这个被标志了的 SA；

2）应按 10.3 中所述的机制特定规程要求的检验 CSC PDU 内容。

若设置或清除 SA-P 标志，执行本条中的下列规程：

b）NLSPE 应准备 CSC PDU 且：

1）UNC-UND 标志设置；

2）若选择了带内 SA-P，则应缺省 SA-ID 字段，否则它应置为 CSC PDU 中接收的 SA-ID；

3）若选择了带内 SA-P，则设置 SA-P 标志，否则清除它；

4）若选择了带内 SA-P，则不出现 CSC PDU 内容和内容长度字段，否则 CSC PDU 内容置为从 10.3 中定义的机制特定规程返回的 CSC 交换。

注：当前规程不提供比任选地跟随 SDT-PDU 的 CSC PDU 双向交换更多要求的 CSC 交换机制。

c）NLSPE 应响应 UN-CONNECT Response 且：

1）UN 响应地址置为本地 UN 地址；

2）UN 接收证实选择和加快数据选择置为从 UN-CONNECT Indication 中的参数本地确定的值；

3）UN QOS 参数置为从 UN-CONNECT Indication 中的 UN QOS 参数本地确定的值；

4）UN 用户数据空；

5）UN 鉴别置为 CSC PDU。

d）被叫 NLSPE 应等待 SA-P 交换或 8.5.4.5 中所述的包含 SDT PDU 的 UN-DATA Indication 或 8.10 中所述的 UN-DISCONNECT Indication 或 8.9 中所述的 UN-RESET。

8.5.4.3 UN-CONNECT Confirm——UNC-UND 设置

收到其包含响应 CSC PDU 的 UN 鉴别的 UN-CONNECT Confirm，且 UNC-UND 标志设置：

a）检验 CSC PDU 中的 SA-P 标志以匹配带内 SA-P 的选择；

b）若不选择 SA-P：

1）使用 10.3 中所述的机制特定规程检验 CSC PDU 内容；

2）继续 8.5.4.4 中 c)所述的规程。

注：若不选择 SA-P 且 CSC 交换机制要求多于两个 CSC-PDU 的交换，则在连接建立规程继续之前，在 UN-DATA 中交换它们。

c）选择带内 SA-P：

1）应执行 SA-P 交换；

2）主叫 NLSPE 等待 8.5.4.4 中所述的 SA-P 完成或 8.10 中所述的 UN-DISCONNECT Indication 或 8.9 中所述的 UN-RESET Indication。SA-P 中的任何差错应按 8.4 中所述的差错处理。

8.5.4.4 SA-P 完成/无 SA-P

在 SA-P 完成时：

a）若 SA-P 成功，已建立的 SA 接着用于完成 NLSPE 连接建立和按下列条所述的安全通信；

b）若 SA-P 不成功，主叫和被叫 NLSPE 应调用 UN-DISCONNECT 且应夭折 NLSP 连接建立规程；

SA-P 的完成或随后的 UN-CONNECT Confirm 没有如 8.5.4.3 b)中所述的 SA-P。

c）下列 NLSP-CONNECT 参数被传递给 8.5.4.1 所述事件中主叫 NLSP，然后应放置于 6.4.1.1 所述的 SDT PDU，其数据类型为“NLSP-CONNECT req/ind”：

1）NLSP 主叫地址；

2）NLSP 被叫地址；

3）NLSP 用户数据。

注 1：尽管 Param _ Prot 为 FALSE，NLSP 地址参数携带在保护格式中。

d）SDT PDU 应传递给 UN-DATA Request 的 UN 用户数据中的 UN 服务提供者；

注 2：这可提供对等实体鉴别交换的第三部分。

e）主叫 NLSPE 等待 8.5.4.7 中所述的包含 SDT PDU 的 UN-DATA Indication 或 8.10 中所述的 UN-DISCONNECT Indication 或 8.9 中所述的 UN-RESET Indication。

SA-P 完成时，被叫 NLSPE 应等待 8.5.4.5 中所述的包含 SDT-PDU 的 UN-DATA Indication 或 8.10 中所述的 UN-DISCONNECT Indication 或 8.9 中所述的 UN-RESET Indication。

8.5.4.5 在被叫 NLSPE 上包含 SDT PDU 的 UN-DATA

在被叫 NLSPE 上，收到包含安全数据传送 PDU 的 UN-DATA Indication 时，应如 6.4.2.2 中所述检验它。

注：这可提供对等实体鉴别交换的第三部分。

应检验 SDT PDU 中的数据类型字段是 NLSP-CONNECT req/ind。

应检验 NLSP 被叫地址是本地确定的 NLSP 实体服务的 NLSP 地址。

应检验 NLSP 主叫地址是包含在 SA 属性 Adr _ Served 中的 NLSP 地址。

若有为连接建立的安全标号，则对照 SA 属性 Label _ Set 中授权的标号集检验它。

NLSP-CONNECT Indication 应传递给被叫 NLSP 用户且参数设置如下：

a）NLSP 主叫地址、NLSP 被叫地址、NLSP 用户数据设置为收到的 SDT PDU 中的内容字段；

b）NLSP 接收证实选择和 NLSP 加快数据选择设置为在 8.5.4.2 规程下发送的 UN-CONNECT Response 中的相同的 UN 参数的设置；

c）“可用的”NLSP QOS 置为在 8.5.4.2 规程下发送的 UN-CONNECT Response 中由被叫 NLSPE“选择的”UN QOS，其“目标”和“最低可接收的”未规定。

被叫 NLSPE 应等待 8.5.4.6 中所述的 NLSP-CONNECT Response 或 8.10 中所述的 NLSP-KIDCONNECT Request 或 8.10 中所述的 UN-DISCONNECT Indication 或 8.9 中所述的 UN-RESET Indication。

8.5.4.6 NLSP-CONNECT Response

收到 NLSP-CONNECT Response 时，NLSP 响应地址、NLSP 用户数据参数应放置于 6.4.1.1 中所述的具有数据类型“NLSP-CONNECT res/conf”的 SDT PDU 中。

该 SDT PDU 应被传递给 UN-DATA Request 的 UN 用户数据中的 UN 服务提供者。

现在，被叫 NLSPE 已完成其 NLSP 连接建立规程。

8.5.4.7 在主叫 NLSPE 上包含 SDT PDU 的 UN-DATA

收到包含 SDT PDU 的 UN-DATA Indication 时，应按 6.4.2.1 中所述检验它，应检验数据类型字段是 NLSP-CONNECT res/conf。

应检验 NLSP 响应地址是包含在 SA 属性 Adr _ Served 中的 NLSP 地址。

NLSP-CONNECT Confirm 被发送给 NLSP 用户且参数设置如下：

a）若出现 NLSP 响应地址，NLSP 用户数据，则按接收的 SDT PDU 的内容字段设置；

b）NLSP 接收证实选择和 NLSP 加快数据选择置为在 8.5.4.3 的规程下发送的 UN-CONNECT Confirm 中相同的 UN 参数的设置；

c）NLSP QOS 置为在 8.5.3 的规程下接收的 UN-CONNECT Confirm 中接收的 UN QOS。

现在，主叫 NLSPE 已完成它的 NLSP 连接建立规程。

8.6 NLSP-DATA 功能

8.6.1 NLSP-DATA Request

收到NLSP-DATA Request 时,若 No _ Header 为 TRUE,则应如 6.4.1.2 中所述那样封装 NLSP 用户数据。把它放置于 UN-DATA Request 的 UN 用户数据中且 NLSP 证实请求参数拷贝到相同的 UN-DATA 参数。接着 UN-DATA 应被传递给 UN 服务提供者。

收到NLSP-DATA Request 时,若 No _ Header 为 FALSE,则:

a) 作为本地事情,NLSPE 应对 NLSP 用户数据分段(若 SA 要求);

b) 对每段,如 6.4.1.1 中所述应产生 SDT PDU,且数据类型"NLSP-DATA req/ind"包含:

1) NLSP 用户数据段;

2) 对最后段 Last/Not last 标志置为 0,对所有前面的段置为 1;

3) NLSP 证实请求内容字段,若:

i) 在 NLSP-DATA Request 中出现 NLSP 证实请求指明"请求的接收证实";

ii) 这是最后段;

iii) Param _ Prot 为 TRUE。

c) 对每段,SDT PDU 应放置于 UN-DATA Request 的 UN 用户数据参数中;

d) UN-DATA 的 UN 证实请求参数应出现以指明"请求的接收证实",若:

1) 在 NLSP-DATA Request 中指明 NLSP 证实请求;

2) 这是最后段;

3) Param _ Prot 为 FALSE;

否则,UN 证实请求参数应指明"无请求的接收证实"。

e) 每段的 UN-DATA Request 原语应被传递给 UN 服务提供者。

8.6.2 跟随连接建立的 UN-DATA Indication 中的保护数据

收到 UN-DATA Indication 时,若 No _ Header 为 TRUE 则如 6.4.2.2 中所述那样应封装 UN 用户数据。把它放置于 NLSP-DATA Indication 中的 NLSP 用户数据且 UN 证实请求参数拷贝到等价的 NLSP-DATA Indication 参数。接着 NLSP-DATA Indication 应被传递到 NLSP 服务用户。

收到 UN-DATA Indication 时,若 No _ Header 为 FALSE,则:

a) 应如 6.4.2.1 所述检验 UN 用户数据中的 SDT PDU;

b) 若数据类型字段"与任何 NLSP 服务原语无关",则应如 8.11 中所述而不是下面所述那样处理 SDT PDU;

c) 若数据类型字段是 NLSP-DATA-ACKNOWLEDGE req/ind,则应如 8.9.2 中所述而不是下面所述那样处理 SDT PDU;

d) 若数据类型字段是 NLSP-DISCONNECT req/ind,则应按 8.10.2 中所述而不是下面所述那样处理 SDT PDU;

e) 否则,应检验数据类型字段是 NLSP-DATA 并按下列处理;

f) 若 SDT PDU 中的 Last/Not last 标志置为 1(Not Last),则 SDT PDU 中的 NLSP 用户数据内容字段被添加到任何以前的 NLSP 用户数据,它是同一 NLSP-DATA req/ind 的一部分且由 NLSPE 保留给后来的使用;

g) 若 SDT PDU 中的 Last/Not last 标志置为 0(Last),则:

1) SDT PDU 中的 NLSP 用户数据内容字段添加到任何以前的 NLSP 用户数据,它是同一 NLSP-DATA req/ind 的一部分且放置于 NLSP-DATA Indication 的 NLSP 用户数据参数中;

2) 若 Param _ Prot 为 TRUE,则 NLSP-DATA Indication 中的 NLSP 证实请求应指明"接收的请求证实",若在 SDT PDU 中出现证实请求内容字段;

3) 若 Param _ Prot 为 FALSE,则接收 UN-DATA Indication 中的 UN 证实请求拷贝到 NLSP-

DATA Indication 中的等价的参数；

4) NLSP-DATA Indication 传递给 NLSP 用户。

8.7 NLSP-EXPEDITED-DATA 功能

8.7.1 NLSP-EXPEDITED-DATA Request

收到 NLSP-EXPEDITED-DATA Request 时，若 No _ Header 为 TRUE，则应如 6.4.1.2 中所述那样封装 NLSP 用户数据。把它放置于 UN-EXPEDITED-DATA Request 的 UN 用户数据中。接着该 UN-EXPEDITED-DATA Request 应传递给 UN 服务提供者。

收到 NLSP-EXPEDITED-DATA Request 时，若 No _ Header 为 FALSE，则：

a) 作为本地事情，NLSPE 应对 NLSP 用户数据分段(若 SA 要求)；

b) 对每一段，应如 6.4.1.1 所述产生 SDT PDU，且数据类型“NLSP-EXPEDITED-DATA req/ind”包含：

1) NLSP 用户数据段；

2) 对于最后段 Last/Not last 标志置为 0，对于所有前面的段置为 1；

3) 每一段的 SDT PDU 应放置于 UN-EXPEDITED-DATA 的 UN 用户数据参数中。

c) 每段的 UN-EXPEDITED-DATA Request 原语应传递给 UN 服务提供者。

注：当使用 SDT PDU 时，因为封装功能可能扩展数据大小，因此用户数据字段的限制的大小可能要求保护的加快数据在通过底层网时进一步分段。

8.7.2 UN-EXPEDITED-DATA Indication

收到 UN-EXPEDITED-DATA Indication 时，若 No _ Header 为 TRUE，则应如 6.4.2.2 所述那样解封 UN 用户数据。把它放置于 NLSP-EXPEDITED-DATA Indication 的 NLSP 用户数据中。接着应把 NLSP-EXPEDITED-DATA Indication 传递给 NLSP 服务提供者。

收到 UN-EXPEDITED-DATA Indication 时，若 No _ Header 为 FALSE，则：

注：当使用 SDT PDU 时，因为封装功能可能扩大数据大小，因此，用户数据字段限制的大小可以要求从几个NLSP-EXPEDITED-DATA Request 被全部处理之前重装 SDT PDU。

a) 应如 6.4.2.1 所述检验 UN 用户数据中的 SDT PDU，应检验 SDT PDU 中的数据类型是 NLSP-WXPEDITED-DATA req/ind；

b) 若 SDT PDU 中的 Last/Not last 标志置为 1(Not last)则 SDT PDU 中的 NLSP 用户数据内容字段添加到任何以前的 NLSP 用户数据，它是同一 NLSP-EXPEDITED-DATA req/ind 的一部分，并由 NLSPE 保留给后来的使用；

c) 若 SDT PDU 中的 Last/Not last 标志置为 0(Last)，则：

1) SDT PDU 中的 NLSP 用户数据内容字段添加给任何以前的 NLSP 用户数据，它是同一 NLSP-EXPEDITED-DATA req/ind 的一部分，并放置于 NLSP-EXPEDITED-DATA Indication 的 NLSP 用户数据参数中；

2) 把 NLSP-EXPEDITED-DATA Indication 服务原语传递给 NLSP 用户。

8.8 RESET 功能

下面列出的任何与 NLSP 或 UN-RESET 相关的事件先占任何 CSC PDU 交换、SA-P 交换或正在进行中的 Test 交换。

8.8.1 NLSP-RESET Request

收到 NLSP-RESET Request 时，应发出具有相同的参数值的 UN-RESET Request。

应丢弃在 8.6 或 8.7 中所述的规程下保留的任何分段的 NLSP 用户数据。

NLSPE 应等待 8.8.2 中所述的 UN-RESET Confirm 或 8.10 中所述的 NLSP-DISCONNECT Request 或 UN-DISCONNECT Indication，LSPE 丢弃所有的 UN-DATA 和 UN-DATA-ACKNOWLEDGE 原语直到收到 UN-RESET Confirm 或 DISCONNECT。

8.8.2 跟随着 NLSP-RESET Request 的 UN-RESET Confirm

收到跟随 8.8.1 中所述的 NLSP-RESET Request 的 UN-RESET Confirm 时，应发出具有相同的参数值的 NLSP-RESET Confirm。

注：由于数据可能已丢失，可能需要重新初始化一些安全机制。尤其是完整性序列机制，甚至在数据丢失后必须能防止重演攻击。这可由使用下面所述的 CSC PDU 交换来完成。

若 SA 属性 Inititor 为 TRUE，则 NLSPE 应启动 8.12.1 中所述的 CSC 交换。否则 NLSPE 应等待 8.12.2 中所述包含 CSC-PDU 的 UN-DATA。

8.8.3 UN-RESET Indication

在 8.5 中所述的 NLSP 连接建立规程期间收到 UN-RESET Indication 时，应依照 OSI 网络服务发出 UN-DISCONNECT Request 和 NLSP-DISCONNECT Indication，且夭折连接建立规程。

收到 UN-RESET Indication，下列 NLSP 连接建立完成：

a）应发出具有相同参数值的 NLSP-RESET Indication；

b）应丢弃在 8.6 或 8.7 中所述的规程下保留的任何分段的 NLSP 用户数据；

c）NLSPE 应等待 8.8.4 中所述的 NLSP-RESET Response 或 8.10 中所述的 NLSP-DISCONNECT Request 或 UN-DISCONNECT Indication。NLSPE 丢弃所有的 UN-DATA 和 UN-DATA-ACKNOWLEDGE 原语直到收到 NLSP-RESET Response 或 DISCONNECT。

8.8.4 跟随 UN-RESET Indication 的 NLSP-RESET Response

收到跟随 8.8.3 中所述的 UN-RESET Indication 的 NLSP-RESET Response 时，应发出 UN-RESET Response。

注：由于数据可能已丢失，可能需要重新初始化一些安全机制。尤其是完整性序列机制，甚至在数据丢失后必须能防止重演攻击。这可由使用下面所述的 CSC PDU 交换来完成。

若 SA 属性 Inititor 为 TRUE，则 NLSPE 应启动 8.12.1 中所述的 CSC 交换，否则 NLSP 应等待包含 8.12.2 中所述的 CSC-PDU 的 UN-DATA。

8.8.5 启动 NLSP 复位

由于与 NLSP 协议相关的事件（例如 8.4 中所述的检验失败）启动复位时：

a）应丢弃 8.6 或 8.7 中所述的规程下保留的任何分段的 NLSP 用户数据；

b）NLSP-RESET Indication 应被传递给 NLSP 服务用户且 NLSP 原发者和 NLSP 原因置为本地确定的值；

c）UN-RESET Request 应被传递给 UN 服务提供者且 UN 原因置为本地确定的值；

d）NLSPE 应等待 8.8.6 中所述的 NLSP-RESET Response 和 8.8.7 中所述的 UN-RESET Confirm，也可能收到 8.10 中所述的 NLSP-DISCONNECT Request 或 UN-DISCONNECT Indication；

e）NLSPE 应丢弃所有的 UN-DATA 和 UN-DATA-ACKNOWLEDGE 原语直到收到 UN-RESET Confirm 或任何 DISCONNECT；

f）NLSPE 应丢弃所有的 NLSP-DATA 和 NLSP-DATA-ACKNOWLEDGE 原语直到收到 NLSP-RESET Response 或任何 DISCONNECT。

8.8.6 跟随 NLSP 启动复位的 NLSP-RESET Response

跟随 NLSP 启动复位的 NLSP-RESET 时不要求进一步的动作。

8.8.7 跟随 NLSP 启动复位的 NLSP-RESET Confirm

注：由于数据可能已丢失，可能需要重新初始化一些安全机制。尤其是完整性序列机制，甚至在数据丢失后必须能防止重演攻击。这可由使用下面所述的 CSC PDU 交换来完成。

跟随 NLSP 启动复位的 UN-RESET Confirm 时，若 SA 属性 Initiator 为 TRUE，则 NLSPE 应启动 8.12.1 中所述的 CSC 交换。否则 NLSPE 应等待包含 8.12.2 中所述的 CSC-PDU 的 UN-DATA。

8.9 NLSP-DATA-ACKNOWLEDGE

8.9.1 NLSP-DATA-ACKNOWLEDGE Request

收到 NLSP-DATA-ACKNOWLEDGE Request 时，若 No _ Header 为 TRUE 或 Param _ Prot 为 FALSE，则把 UN-DATA-ACKNOWLEDGE Request 传递给 UN 服务提供者。

收到 NLSP-DATA-ACKNOWLEDGE 时，若 No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则：

a) 如 6.4.1.1 所述产生 SDT PDU 且数据类型"NLSP-DATA-ACKNOWLEDGE req/ind"不包含附加内容字段；

b) 应把 SDT PDU 当作 UN-DATA Request 原语中的 UN 用户数据传递给 UN 服务提供者。

8.9.2 UN-DATA Indication 中保护的 NLSP-DATA-ACKNOWLEDGE

若在 UN-DATA Indication 中收到 SDT PDU，且数据类型置为 NLSP-DATA-ACKNOWLEDGE，如 8.6.2 c)中所述，则：

a) 应检验 SDT PDU，它并不包含与 NLSP 服务参数相关的内容字段；

b) 应把 NLSP-DATA-ACKNOWLEDGE Indication 传递给 NLSP 用户。

8.9.3 UN-DATA-ACKNOWLEDGE Indication

收到 UN-DATA-ACKNOWLEDGE 时：

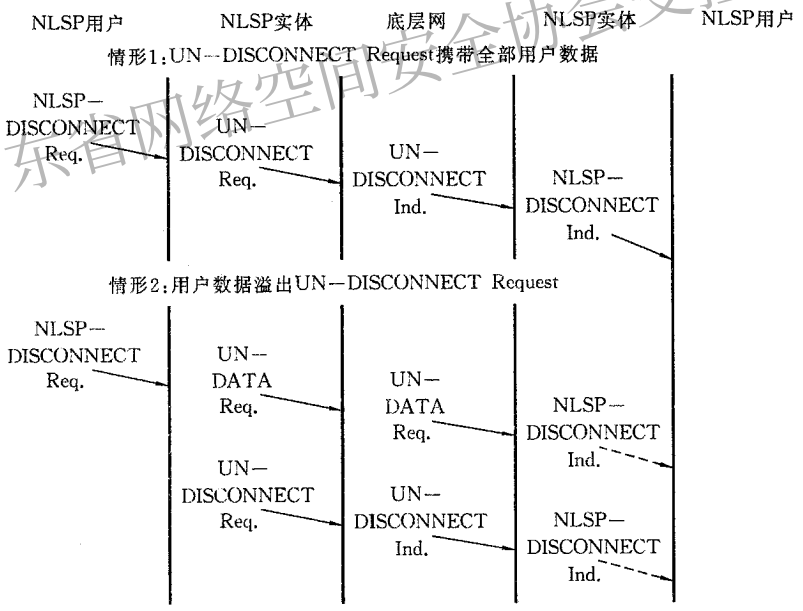
a) NLSPE 应检验 No _ Header 为 TRUE 或 Param _ Prot 为 FALSE；

b) 应把 NLSP-DATA-ACKNOWLEDGE Indication 传递给 NLSP 用户。

8.10 NLSP-DISCONNECT

下面列出的任何与 NLSP 或 UN-DISCONNECT 相关的事件先占任何 CSC-PDU 交换、SA-P 交换或正在进行中的 Test 交换。

图 4 说明了 NLSP 用户启动的断开规程。



注：NLSP DISCONNECT 可能出现在指明的任何点上。

图 4 NLSP-DISCONNECT 的服务原语时序图

8.10.1 NLSP-DISCONNECT Request

8.5 所述的 NLSP 连接建立规程期间收到 NLSP-DISCONNECT Request 时，应依照 OSI 网络服务发出 UN-DISCONNECT Request(即若已开始建立 UN 连接)，且夭折连接建立规程。若 Protect _ Connect _ Param 为 TRUE，应由本地确定任何 UN-DISCONNECT Request 的参数，否则应通过等价的 UN-DISCONNECT Request 参数拷贝 NLSP-DISCONNECT Request 参数。

注：若在连接建立期间出现 NLSP-DISCONNECT Request 且选择了 Protect _ Connect _ Param，则要丢弃 NLSP-DISCONNECT Request 参数。

收到跟随 NLSP 连接建立的 NLSP-DISCONNECT Request 时：

a）若 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 TRUE，则应如 6.4.1.2 中所述那样封装任何 NLSP 用户数据。把它放置于 UN-DISCONNECT Request 的 UN 用户数据中。通过等价的 UN-DISCONNECT Request 参数拷贝其他的 NLSP-DISCONNECT Request 参数；

b）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则产生 SDT PDU，它包含 6.4.1.1 中所述的所有 NLSP-DISCONNECT Request 参数，具有数据类型“NLSP-DISCONNECT req/ind”。把它放置于 UN 用户数据中。其他的 UN-DISCONNECT 参数由本地确定；

c）若出现 NLSP 用户数据，Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 FALSE，则产生 SDT PDU，它包含 6.4.1.1 中所述的 NLSP 用户数据，具有数据类型“NLSP-DISCONNECT req/ind”。把它放置于 UN 用户数据中。通过等价的 UN-DISCONNECT Request 参数拷贝其他的 NLSP-DISCONNECT Request 参数；

d）若 Protect _ Connect _ Param 为 FALSE，则通过等价的 UN-DISCONNECT Request 参数拷贝所有的 NLSP-DISCONNECT 参数；

注：假定 NLSP 用户数据的长度限制与 UN 用户数据的相同。

e）若跟随上面的 b）和 c），得到了 UN 用户数据参数比 UN-DISCONNECT Request 的 UN 用户数据的最大长度更大，则应代替在 UN-DATA Request 的 UN 用户数据参数发送它且传递给 UN 服务提供者。UN-DISCONNECT Request 的 UN 用户数据应为空；

注：一个实现将等待该 UN-DATA 以在进行下段中所述的 UN-DISCONNECT 之前通过底层网。该等待期间由本地确定。

f）应发送 UN-DISCONNECT Request 且如上所述设置参数。

8.10.2 UN-DATA Indication 中保护的 NLSP-DISCONNECT

若在 UN-DATA Indication 中收到 SDT PDU 且数据类型置为 NLSP-DISCONNECT，如 8.6.2 中 d）所述，则：

a）NLSPE 检验 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 FALSE；

b）任何包含 NLSP 服务参数的内容字段拷贝到等价的 NLSP-DISCONNECT 参数，且 NLSP 原发者置为 NS 用户；

c）NLSPE 保留如上设置的 NLSP-DISCONNECT 参数，等待 UN-DISCONNECT Indication 或立即发出 NLSP-DISCONNECT Indication。该选择是一个本地判定。

8.10.3 UN-DISCONNECT Indication

在 8.5 中所述的 NLSP 连接建立规程期间收到 UN-DISCONNECT Indication 时，应依照 OSI 网络服务发出 NLSP-DISCONNECT Indication 且夭折连接建立规程。应通过任何 NLSP-DISCONNECT Indication 的等价参数拷贝 UN-DISCONNECT Indication 参数，或者若 Protect _ Connect _ Param 为 TRUE，它按本地确定来设置。

否则，在跟随着 NLSP 连接建立且 UN 用户数据非空的 UN-DISCONNECT Indication 上：

a）若 Protect _ Connect _ Param 为 TRUE 且 No _ Header 为 TRUE 则应如 6.4.2.2 所述那样解封 UN 用户数据。把它放置于 NLSP-DISCONNECT Indication 的 NLSP 用户数据中。其他的 NLSP-DISCONNECT Indication 参数应被置为 UN-DISCONNECT Indication 的等价参数；

b）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 TRUE，则如 6.4.2.1 中所述的那样检验 UN 用户数据中的 SDT PDU。应检验数据类型是 NLSP-DISCONNECT req/ind。通过这些参数拷贝与 NLSP-DISCONNECT 参数相关的任何内容字段；

c）若 Protect _ Connect _ Param 为 TRUE，No _ Header 为 FALSE 且 Param _ Prot 为 FALSE，则如 6.4.2.1 中所述检验 UN 用户数据中的 SDT PDU。应检验数据类型是 NLSP-DISCONNECT。应检验用户数据内容字段的出现，接着通过 NLSP-DISCONNECT Indication 的 NLSP 用户数据拷贝用户数据内容字段。通过等价的 NLSP-DISCONNECT Indication 参数拷贝其他的 UN-DISCONNECT Indication 参数；

d）若 Protect _ Connect _ Param 为 FALSE，则通过等价的 NLSP-DISCONNECT Indication 参数拷贝所有的 UN-DISCONNECT 参数；

e）NLSP-DISCONNECT Indication 应传递给 NLSP 用户。

否则，在跟随 NLSP 连接建立且 NLSP 用户数据为空的 UN-DISCONNECT Indication 上：

a）若 NLSPE 在等待跟随 UN-DATA Indication[见 8.10.2 c)]中保护的 NLSP-DISCONNECT 之后的 UN-DISCONNECT Indication，则保护的 NLSP 参数字段应放置于 NLSP-DISCONNECT Indication 中。其他的 NLSP-DISCONNECT Indication 参数应置为 UN-DISCONNECT Indication 的等价参数；

b）否则，应通过等价的 NLSP-DISCONNECT Indication 参数拷贝 UN-DISCONNECT Indication 参数；

c）NLSP-DISCONNECT Indication 应传递给 NLSP 用户，除非已发出了它。

若 Retain _ On _ Disconnect 为 FALSE，可能本地删除跟随任何 UN-DISCONNECT 的 SA 属性。

8.10.4 启动 NLSP 断开

在 SA-P 或任何其他的检验失败时，NLSP-DISCONNECT Indication 及 UN-DISCONNECT Request 被传递到如 8.4 中所定义的 NLSP 用户和底层网。

图 5 给出了由于不成功的 SA-P 启动的 NLSP 断开例子的说明。

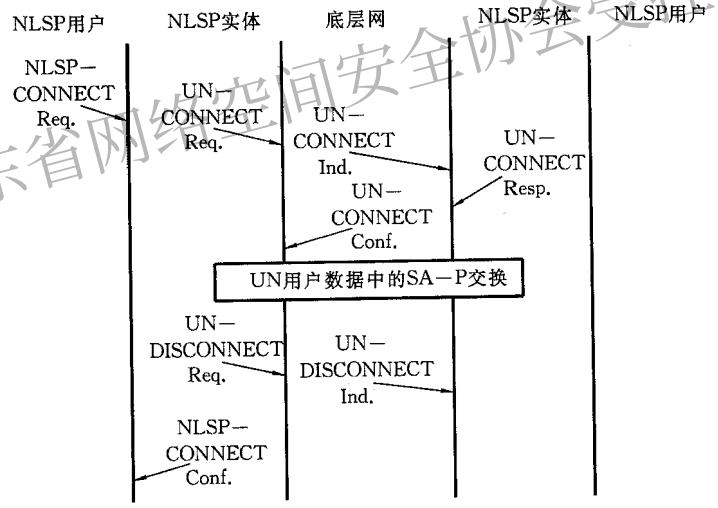


图 5 由于不成功的 SA-P 启动 NLSP 断开

8.11 其他功能

规定时间或外部事件上启动下列规程。

8.11.1 更新动态 SA 属性

NLSPE 可以在连接生命期中的任何时间更新动态 SA 属性(见附录 G)。对动态 SA 属性的任何改变应不更新提供的安全服务。这可通过 CSC PDU 交换或 UN-DATA 用户数据中的 SA-P 交换(使用 SA-PDU 或具有内容数据类型 SA 协议的 SDT PDU)或外部方法完成。该交换对 NLSP 用户是透明的且不定义 NLSP 原语来调用它。

注：例如，为了交换密钥，在连接中有规律地间隔地发生该交换(例如，每小时或每 10 000 安全数据 PSU)。

当执行数据传送且选择了无报头时，应在 8.8.5 中所定义的 CSC PDU 交换之前发送 UN-

RESET。

CSC-PDU 交换的规程应如 8.12 中描述的。附录 C 中给出了包含 SA 属性更新规程的 SA-P 的例子。

8.11.2 安全测试交换

这些规程应使用于测试 SA 的密码方面的操作。

在 NLSP-DATA 原语被发送到 UN-DATA 中的状态下，这些规程才可被调用(即在 NLSP 连接建立完成后，在任何断开规程前，不在复位规程期间)。

任何 DISCONNECT、RESET、CSC-PDU 交换或 SA-P 交换应先占测试交换。

注：这些功能的使用要被本地控制。使用的可能方式有：

a) 不用；

b) 跟随密钥的交换；

c) 定期地在本地确定的时间上。

8.11.2.1 测试交换的调用

在调用测试交换时：

a) 应创建测试数据字段且方向标志清除(置为 0)，测试数据置为随机数据；

b) 应如 6.4.1.1 中所述的产生 SDT PDU，且数据类型“与任何 NLSP 服务原语无关”，包含测试数据字段；

c) PDU 应发送至 UN-DATA 的 UN 用户数据且 UN 接收证实指明“不要求接收证实”。

8.11.2.2 具有 SDT PDU 的 UN-DATA 包含测试数据

收到 UN-DATA 包含其数据类型置为 0(与任何 NLSP 服务原语无关)的 SDT PDU 时，如 8.6.2 中 b)所述，若 SDT PDU 包含测试数据，则应按下列处理它：

a) 若测试数据字段的方向标志被清除，应如 6.4.1.1 所述产生一个新的 SDT PDU，且数据类型“与任何服务原语无关”，并包含测试数据字段，它的方向标志和数据置为收到的随机数据。这应返回到 UN-DATA 的 UN 用户数据且 UN 接收证实指明“不要求接收证实”；

b) 若设置测试数据中的方向标志，则接收到的测试数据应被检验以识别先前发送的测试数据。若不，NLSPE 应执行 8.4 中定义的差错功能。

8.11.3 通信量填充

附加 UN-DATA 原语包含安全数据传送 PDU，且仅通信量填充可被发送来隐藏用户数据的处理。

所有的 NLSP 实体必须能够接收具有该通信量填充的安全数据传送 PDU。该功能的使用是由本地 NLSP 实体自行处理且对 NLSP 服务用户是透明的。

8.11.3.1 通信量填充的调用

通信量填充调用时：

a) 如 6.4.1.1 中所述应产生 SDT PDU，且数据类型“与任何服务原语无关”并不包含附加内容字段而不是 6.4.1.1 要求的那些；

b) 该 PDU 应被发送至 UN-DATA 的 UN 用户数据且 UN 接收证实指明“不要求证实接收”。

8.11.3.2 具有 SDT PDU 的 UN-DATA 并不包含附加内容字段

收到 UN-DATA 包含其数据类型置为 0(与任何 NLSP 服务原语无关的)的 SDT PDU 时，如8.6.2 中 b)所述，若 SDT PDU 并不包含内容字段而不是第 6 章中一般要求的那些，应忽略该 SDT PDU。

8.12 对等实体鉴别

8.12.1 和 8.12.2 中定义的规程能被调用：

a) 跟随如 8.8 中所述的 UN-RESET 或 NLSP-RESET；

b) 在本地确定的时间间隔。

为了执行对等实体鉴别或更新动态 SA 属性。

连接建立期间的CSC-PDU 交换在8.5中描述。

NLSP-DATA 或NLSP-EXPEDITED-DATA Request 应不进行服务直到CSC 交换完成。

任何RESET 或DISCONNECT 原语应先占CSC 交换。

8.12.1 CSC 交换的调用

调用CSC 交换时,应创建CSC 且:

a) UNC-UND 和SA-P 标志清除;

b) SA-ID 置为Your _SA-ID;

c) 按机制特定规程要求的内容置为CSC 第一交换,如10.3中所述的那样。

该CSC-PDU 应被发送至UN-DATA 的UN 用户数据且"不要求证实请求"。

调用CSC 交换的NLSPE 应等待包含CSC PDU 的UN-DATA。任选地,可由8.8中所述的UN-RESET 或NLSP-RESET,或8.10中所述的UN-DISCONNECT 或NLSP-DISCONNECT 先占CSC 交换。

8.12.2 包含CSC-PDU 的UN-DATA

收到包含CSC PDU 的UN-DATA 时(在启动者或CSC 交换的响应者),则按10.3中所述的机制特定规程的要求检验内容。

取决于机制特定规程,NLSPE 可以:

a) 返回CSC-PDU 内容并要求指明进一步的CSC 交换;

在这种情况下CSC PDU UNC-UND 和SA-P 标志应清除,SA-ID 置为Your _SA-ID 且内容按机制特定规程的要求设置。CSC PDU 应被发送至UN-DATA 用户数据。NLSPE 应等待另一个包含CSC PDU 的UN-DATA。任选地,由8.8中所述的UN-RESET 或NLSP-RESET,或8.10中所述的UN-DISCONNECT 或NLSP-DISCONNECT 先占CSC 交换;

b) 返回CSC-PDU 内容并指明要求的SDT PDU 以完成交换;

在这种情况下,CSC UNC-UND 和SA-P 标志应清除,SA-ID 置为Your _SA-ID 且内容按机制特定规程的要求设置。CSC PDU 应被发送至UN-DATA 用户数据。NLSPE 应等待另一个包含SDT PDU 的UN-DATA,如8.6中所述被处理。任选地,由8.8中所述的UN-RESET 或NLSP-RESET,或8.10中所述的UN-DISCONNECT 或NLSP-DISCONNECT 先占CSC 交换。

注1:鉴别不认为完成,因此在该NLSPE 应不处理NLSP-DATA Request (或NLSP EXPEDITED),直到收到SDT PDU。该SDT PDU 可包含从远程NLSP 用户来的NLSP-DATA 或可与任何NLSP 服务原语无关。

注2:若No _Header 为TRUE,则不支持该选项。

c) 返回CSC-PDU 内容并指明交换完成;

在这种情况下,CSC UNC-UND 和SA-P 标志应清除,SA-ID 置为Your _SA-ID 且内容按机制特定规程的要求设置。CSC PDU 应被发送至UN-DATA 用户数据。

d) 指明要求SDT PDU 发送以完成CSC 交换;

在这种情况下,若NLSP-DATA Request(或NLSP-EXPEDITED-DATA)正等待被发送且No _Header 为FALSE,则应按8.6或8.7中所述的处理。否则,应如6.4.1.1中所述创建SDT PDU,且数据类型"与任何NLSP 服务原语无关",并不包含内容字段,而不是第6章中一般要求的那些,并发送至UN-DATA 原语的UN 用户数据。

e) 指明CSC 交换完成。

在这种情况下不要求进一步的动作。

注3:没有定义通用规程来解决同时启动的两个CSC 交换间的冲突。

注4:按照第10章中定义的鉴别机制,若使用封装/解封功能,如第11章中定义的,不提供不包含ISN 全对等实体鉴别。此外,若使用如第12章中所述的No _Header 封装机制,则不提供全对等实体鉴别。

9 使用机制概述

第9章至第12章定义了第1章至第8章中定义的通用协议使用的特定机制。这些机制不是用于通用NLSP中提供安全的仅有的机制。其他机制在将来也可能被标准化，并且NLSP使用专用机制是可能的。

9.1 安全服务和机制

若作出选择，NLSP-CL支持下列安全服务及所述机制：

a）数据原发鉴别——用于提供该服务机制是与密钥管理相结合的ICV；

b）访问控制——用于提供该服务的机制是安全标号，密钥的控制，鉴别地址的使用；

c）无连接保密性——用于提供该服务的机制是加密。该保护任选地包括所有NLSP服务参数，这取决于所选择的安全服务；

d）通信流量保密性——用于提供该服务的机制是通信量填充和/或隐藏NLSP地址；

e）无连接完整性——用于提供该服务的机制是ICV。该保护任选地包括所有NLSP服务参数，这取决于所选择的安全服务。

若作出选择，NLSP-CO支持下列安全服务及所述机制：

a）对等实体鉴别——用于提供该服务的机制是与密钥管理相结合的加密完整性顺序号的交换；

b）访问控制——用于提供该服务的机制是安全标号，通过密钥控制，鉴别的地址；

c）连接保密性——用于提供该服务的机制是加密。该保护任选地包括所有NLSP连接参数，这取决于所选择的安全服务；

d）通信流量保密性——用于提供该服务的机制是通信量填充和/或地址隐藏；

e）无恢复的连接完整性——用于提供该服务的机制是完整性检验值和完整性顺序号。该保护任选地包括所有NLSP连接参数，这取决于所选择的安全服务。

9.2 支持的功能

NLSP支持机制的基本特征是：

a）连接鉴别功能支持对等实体鉴别并建立支持安全数据传送的“动态”SA属性的初始值。仅NLSP-CO使用该功能；

b）通过使用下列机制，基于SDT PDU的封装功能支持安全数据传送：

1）完整性顺序号；

2）为通信流量保密性而进行填充、块完整性算法和块加密算法；

3）完整性检验值；

4）加密；

c）基于无报头保护形式的封装功能使用不改变数据长度的加密机制。

按上面给出的顺序实现各种机制。

10 连接安全控制（仅NLSP-CO）

10.1 导引

“连接安全控制”规程使用连接安全控制（CSC）PDU的交换于：

a）任选地，规定新的加密/完整性密钥；

b）执行对等实体鉴别；

c）建立完整性顺序号。

通过顺序号交换对鉴别机制的支持由本标准规定。当完成双向交换时，对于启动的实体，完成使用该机制的鉴别。对于响应实体，若选择了顺序完整性来保护重演攻击（即ISN为TRUE），则仅当收到来自启动的实体的第一个SDT PDU时，完成鉴别。

10.2 SA 属性

下列安全属性用于支持连接安全控制规程：

a）为 SA 选择的机制：

鉴别：布尔类型

是否要用到使用加密 ISN 的对等实体鉴别。

这些属性的值由给定选择的安全服务的 ASSR 定义。

b）密钥分配机制属性：

kdm：要用到该 SA 的方式

该属性的值由给定选择的安全服务的 ASSR 定义。

它可有下列值：

kdm _ mutual：按对称密钥分配。

kdm _ asymmetric _ single：使用接收者公开密钥的分配。

kdm _ asymmetric _ double：使用远程公开和本地专用密钥的分配。

kdm _ distributed：参考预分配密钥或其他方法分配的密钥的分配。

kdm _ other：使用专用定义的分配机制。

c）鉴别机制属性：

Auth _ Alg：在 ISO/IEC 9979 下分配的客体标识符。

该属性的值由给定选择的安全服务的 ASSR 定义。

Enc _ Auth _ Len：CSC PDU 中加密 auth-data 字段的长度。

该属性的值由给定选择的安全服务的 ASSR 定义。

Auth _ Gen _ Key：由 ASSR 约束的形式。

该属性的初值在 SA 建立时设置并且在联系的生命期内可被改变。

Auth _ Check _ Key：由 ASSR 约束的形式。

该属性的初值在 SA 建立时设置并在联系的生命期内可被改变。

安全数据传送机制使用的下列属性可由连接鉴别机制来建立：

a）ISN 机制属性：

Data _ My _ ISN

Data _ Your _ ISN

Exp _ My _ ISN

Exp _ Your _ ISN

b）加密机制属性：

Data _ Enc _ Key

Data _ Dec _ Key

Exp _ Enc _ Key

Exp _ Dec _ Key

c）ICV 机制属性：

Data _ ICV _ Gen _ Key

Data _ ICV _ Check _ Key

Exp _ ICV _ Gen _ Key

Exp _ ICV _ Check _ Key

注：附加机制特定属性可能在本标准的将来版本中标识，对专用机制也一样。

10.3 规程

NLSP 实体在每个连接建立时或跟随复位或其他的外部定时事件时，交换连接安全控制(CSC)

PDU 以：

a）任选地，规定加密或完整性密钥；

b）执行对等实体鉴别；

c）建立完整性顺序号。

可按下面定义来提供对等实体鉴别。若要求连接完整性时，任何可供选择的方法必须产生完整性顺序号。

加密/完整性密钥由下列任一项来规定：

a）要使用存在的密钥的指示；

b）传递一个采用加密密钥相互密钥进行加密的新密钥；

c）传递一个采用接收者的公开密钥进行加密的新密钥；

d）参考先前分配的密钥。

注 1：加密密钥的派生提供少量的完整性检验，其中用以防止用不同密钥保护的密码文本的重演。将在每个加密算法上规定密钥派生算法以防止弱密钥的意外派生。

NLSP 使用基于交换初始完整顺序号的对等实体鉴别方法，该顺序号用鉴别密钥加密。即使顺序号不用于完整性服务，也可使用该方法。

连接安全控制规程是基于交换两个 CSC PDU 和安全数据传送 PDU，如下所述。

CSC PDU 由安全交换的启动者准备：

a）加密的 Auth-Data 置为本地选择的 My-Initial-ISN 值，Your-Initial-ISN 置为 0，两者都用 Auth _ Gen _ Key 加密，选择的 ISN 对鉴别和完整性密钥必须是唯一的；

b）按照密钥分配机制的要求设置密钥信息。

当并非 CSC PDU 交换的启动者的 NLSP 实体收到 CSC PDU 时：

a）加密的 Auth-Data 用 Auth _ Check _ Key 解密；

b）检验 Your-Initial 字段为 0；

c）本地 SA 属性 Data _ Your _ ISN 和 Exp _ Your _ ISN 被置为收到的 My-Initial-ISN 字段；

d）按密钥分配机制的要求处理密钥信息。

接着准备 CSC PDU 且：

a）加密的 Auth-Data 置为本地选择的 My-Initial-ISN 值，Your-Initial-ISN 具有收到的 My-Initial-ISN 的值，两者都用 Auth _ Gen _ Key 加密。对于鉴别和完整性密钥，选择的 ISN 必须是唯一的；

b）按密钥分配机制的要求设置密钥信息。

在 CSC 交换的启动者收到 CSC PDU 时：

a）加密的 Auth-Data 用 Auth _ Check _ Key 解密；

b）对照先前发送的 My-Initial-ISN 检验 Your-Initial 字段；

c）本地 SA 属性 Data _ Your _ ISN 和 Exp _ Your _ ISN 被置为收到的 My-Initial-ISN 字段；

d）按密钥分配机制的要求处理密钥信息。

跟随着响应成功检验，若 NLSP 实体没有数据在等待且为 SDT PDU 的封装选择 ISN 机制（见第 11 章），则不包含数据但包括 ISN 的安全数据传送 PDU 应被发送以完成鉴别。

注 2：即使有数据正在等待，也可能发送 SDT PDU 以完成鉴别规程而无需要实现正常数据传送规程。

若鉴别失败，则取决于本地判定，可能要采用带内或带外方式重建安全联系，并执行 8.4 中所述的差错恢复规程。

10.4 使用的 CSC-PDU 字段

本章中的规程使用 13.5.6 中定义的下列机制特定 CSC 内容字段：

a）加密的 Auth-Data；

b）密钥信息。

11 基于SDT PDU的封装功能

11.1 导引

NLSP-CL和任选的NLSP-CO使用基于SDT PDU的封装功能来保护用户数据和相关的协议控制信息，本章定义了这样的封装功能，该封装功能基于四个功能：

——ISN；

——填充；

——ICV；

——加密。

使用特定功能的判定应基于SA的属性。

若选择了顺序号，应加上ISN字段。

注1：不期望该保护机制用于NLSP-CL。

若选择了通信量填充，可加上通信量填充字段。

若使用了块完整性算法，可加上完整性填充字段。

若选择了完整性检验，可计算出ICV并加到上面的字段。

注2：ICV也可用来提供数据原发鉴别。

若使用块加密算法，可加上加密填充字段。

若选择了加密，对安全联系使用加密密钥来加密上面的字段。

用上面所述的规程封装用户数据和其他NLSP协议参数来为网上的传送提供保护。在远端，安全数据传送PDU的接收者用相反的规程顺序来移去和检验保护部分。

11.2 SA属性

a）为SA选择的机制：

ISN：布尔类型

在每个封装八位位组串中包括的完整性顺序号。

Padd：布尔类型

在封装的八位位组串中进行填充以支持通信量填充机制。

ICV：布尔类型

使用完整性检验值的封装八位位组串内容的完整性和/或数据原发鉴别。

Encipher：布尔类型

加密封装八位位组串以提供保密性。

这些属性的值由给定选择目标安全服务的ASSR定义。

b）ISN机制属性：

ISN _ Len：整数

该属性的值应由给定选择的安全服务的ASSR定义。

Data _ My _ ISN：发送的最后正常数据的ISN。

Data _ Your _ ISN：收到的最后正常数据的ISN。

Exp _ My _ ISN：发送的最后加快数据的ISN。

Exp _ Your _ ISN：收到的最后加快数据的ISN。

这些“关键”属性的初值应在SA建立时设置，并能在联系的生命期内改变。

注1：加快数据ISN属性仅适用于NLSP-CO。

c）填充机制属性：

Traff _ Padd：受ASSR约束的形式。

通信量填充需求。

d）ICV 机制属性：

ICV _ Alg：客体标识符

该属性的值应受给定选择的安全服务 ASSR 约束。该属性暗指完整性机制的某些属性，如单独生成和检验算法、初始化向量等。

ICV _ Blk：整数

ICV 算法操作的基本块大小。

该属性的值应受给定选择的安全服务的 ASSR 约束。

ICV _ Len：整数

ICV 机制的输出长度。

该属性的值应受给定选择的安全服务的 ASSR 定义。

ICV _ Len 不必等于 ICV _ Blk。

Data _ ICV _ Gen _ Key：受 ASSR 约束的形式。

正常数据的 ICV 生成密钥参考。

Data _ ICV _ Check _ Key：受 ASSR 约束的形式。

正常数据的 ICV 检验密钥参考。

Exp _ ICV _ Gen _ Key：受 ASSR 约束的形式。

加快数据的 ICV 生成密钥参考。

Exp _ ICV _ Check _ Key：受 ASSR 约束的形式。

加快数据的 ICV 检验密钥参考。

这些“关键”属性的初值应在 SA 建立时设置，并能在联系生命期内改变。

注 2：加快数据密钥属性仅适用于 NLSP-CO。

e）加密机制属性：

Enc _ Alg：在 ISO/IEC 9979 下分配的客体标识符。

该属性的值应受给定选择的安全服务的 ASSR 约束。该属性暗指加密机制的某些属性，如任何同步字段的形式和长度、单独的加密和解密算法、初始化向量等。

Enc _ Blk：整数

加密算法的块大小。

该属性的值应受给定选择的安全服务的 ASSR 约束。

Data _ Enc _ Key：受 ASSR 约束的形式。

正常数据的加密密钥参考。

Data _ Dec _ Key：受 ASSR 约束的形式。

正常数据的解密密钥参考。

Exp _ Enc _ Key：受 ASSR 约束的形式。

加快数据的加密密钥参考。

注 3：仅由 NLSP-CO 使用。

Exp _ Dec _ Key：受 ASSR 约束的形式。

加快数据的解密密钥参考。

注 4：仅由 NLSP-CO 使用。

这些“关键”属性的初值应在 SA 建立时设置，并能在联系的生命期内改变。

注 5：附加机制特定属性将在本标准的将来版本中被标识，专用机制也一样。

11.3 规程

在进行封装中，通过添加或前置的一些字段来形成 PDU。这些字段是任选的。部分形成的 PDU 下面称作“现存的字段”。在解封时，应通过移走一些字段来分解 PDU。部分分解的 PDU 下面称作“保留的

数据”。

注

1 对添加和前置的字段的描述并不意味着约束 NLSP 的实现，而是明确地规定协议。

2 封装功能不处理无报头选项。它由第 12 章中定义的规程来处理。

11.3.1 封装功能

SA-ID 应用于引用一个安全联系。若安全联系不存在，则差错 SA-not-available 应被返回而封装的八位位组串的值不定。

若(ISN 为 TRUE)则：

a) 若(data-unit-type＝normal)，则应增进 Data _ Your _ ISN 并放置于顺序号内容字段内，添加到封装前八位位组串中的现存字段；

b) 若(data-unit-type＝expedited)，则应增进 Exp _ Your _ ISN 并放置于顺序号内容字段内，添加到封装前八位位组串中的现存字段。

注

1 ISN 可通过增加顺序号或从非重复的序列中选取下一个号码来增进。时间戳也能被认为是非重复的序列。

2 不期望 ISN 机制会用于 NLSP-CL。

3 Exp _ My _ ISN 仅适用于 NLSP-CO。

若(Padd 为 TRUE)，则按照 Traff _ Padd 中涉及的 ASSR 规则由本地确定的一定数量和形式的填充应被放置于通信量填充内容字段并添加到封装前八位位组串中的现存字段。若要求填充单个八位位组，则应使用单个八位位组填充内容字段。

若(ICV 为 TRUE)且(ICV _ Blk＞1)，则在必须时，完整性填充字段应被添加到现存字段，以使具有完整性填充字段(包括被保护的内容字段)的现存字段的长度是 ICV 块大小(即 ICV _ Blk)的整数倍。若出现这种字段，则由本地确定的一定数量和形式的填充应被放置于完整性填充内容字段。若要求填充单个八位位组，则应使用单个八位位组填充内容字段。内容长度值应增加所加的填充数量。

应在现存字段之前放置于内容长度。所有现存字段的长度应被确定并放置于内容长度。

若(ICV 为 TRUE)则长度 ICV _ Len 的 ICV 应被计算出来，并添加到现存字段。应采用 ICV _ Alg 来标识使用的算法，所用的密钥应是：

a) Data _ ICV _ Gen _ Key，若 data-unit-type＝normal；或

b) Exp _ ICV _ Gen _ Key，若 data-unit-type＝expedited。

若(Encipher 为 TRUE)，则具有由 Enc _ Alg 确定的形式和长度的密码同步字段应被产生并前置于现存字段。

若(Encipher 为 TRUE)，则加密填充应被添加到现存字段，以使现存字段的长度(即被保护数据长度，封装前八位位组串，ISN，完整性填充和 ICV 字段)加上加密填充的长度是加密块大小(即 Enc _ Blk)的整数倍。若出现这种加密填充，则由本地确定的一定数量和形式的填充应放置于加密填充内容字段内。若要求填充单个八位位组，则应使用单个八位位组填充内容字段。

若(Encipher 为 TRUE)，则加密现存字段。Enc _ Alg 应标识使用的算法，使用的密钥应是：

a) Data _ Enc _ Key，若 data-unit-type＝normal；或

b) Exp _ Enc _ Key，若 data-unit-type＝expedited。

所构成的 PDU 应作为封装的八位位组串中的结果返回。

11.3.2 解封功能

若下列检验中的任何一项失败，除了警告、审计和/或帐户信息外，所有的安全相关状态信息都应被置为接收该信息前的安全状态信息。

应使用 SA-ID 自变量来引用安全联系。若安全联系不存在，则应返回差错 SA-not-available 而封装前八位位组串的值不定。

若(Encipher 为 TRUE),则执行下列步骤:

a) 封装的八位位组串应被解密。Enc _ Alg 应标识使用的解密算法。使用的密钥应是:

1) Data _ Dec _ Key,若 data-unit-type=normal;或

2) Exp _ Dec _ Key,或 data-unit-type=expedited。

b) 由 Enc _ Alg 确定,从加密数据的前部,丢弃若干八位位组来移走密码同步字段;

c) 通过将内容长度和 ICV _ Len 相加,然后丢弃任何超出计算长度的保留加密数据的八位位组来移走加密填充或单个八位位组填充内容字段。

若(ICV 为 TRUE),则执行下列步骤:

a) 通过检验保留数据的最后 ICV _ Len 八位位组来验证 ICV 字段。用 ICV _ Alg 来标识使用的算法,若基于密码时,用于计算 ICV 的密钥应是:

1) Data _ ICV _ Check _ Key,若 data-unit-type=normal;或

2) Exp _ ICV _ Check _ Key,若 data-unit-type=expedited。

b) 若 ICV 验证失败,则应返回差错 data-unit-integrity-failure,而封装前八位位组串的值不定。

通过丢弃在内容长度字段之后的超出内容长度中指明长度的保留数据中的任何八位位组来移走 ICV。

通过丢弃保留数据的头两个八位位组来移走内容长度字段。

通过移走在封装前八位位组串之外的数据,应从保留数据中移走任何通信量填充、完整性填充或单个八位位组填充内容字段。

注 1:用对封装前八位位组串的内容进行解码来定位内容字段,它是后接若干 TLV 字段的一个八位位组类型字段。

若(ISN 为 TRUE)则应检验保留数据以确保有且只有一个 ISN 内容字段出现;或者,通过检验保留数据来确保没有 ISN 内容字段存出现。若出现 ISV 内容且:

a) 若(data-unit-type=normal)则应增进 Data _ My _ ISN 并且对照 Data _ My _ ISN 确定的期望值窗口来检验其值;

b) 若(data-unit-type=expedited)则应增进 Exp _ My _ ISN 并且对照 Exp _ My _ ISN 确定的期望值窗口来检验其值。

在 a)和 b)中,在检验前先增进 ISN。

注 2:可通过增加顺序号或从一个伪随机、非重复序列中选取下一个数来完成增进。

封装前八位位组串的值应作为封装前八位位组串中的结果返回。

11.4 使用的 PDU 字段

这些规程使用 13.3 中定义的 SDT PDU 的下列字段:

a) 封装的八位位组串;

b) 密码同步;

c) ICV;

d) 内容字段:

1) 加密填充;

2) 顺序号;

3) 单个八位位组填充;

4) 通信量填充;

5) 完整性填充。

12 无报头封装功能(仅 NLSP-CO)

12.1 导引

NLSP-CO 仅能通过使用无报头选项提供用户数据保密性。无报头选项使用如本章中描述的封装

功能。该封装功能应基于封装机制。

使用无报头选项暗指加密机制是在一个八位位组的块长度上操作，且算法不改变加密数据的大小。

12.2 SA 属性

a）为 SA 选择的机制：

Encipher：布尔类型

封装的八位位组串的加密以提供保密性。

该属性的值应由给定选择的安全服务的 ASSR 定义。

b）加密机制属性：

Enc _ Alg：在 ISO/IEC 9979 下分配的客体标识符。

该属性的值由给定选择的安全服务的 ASSR 定义。该属性暗指加密机制的某些属性，如任何同步字段的形式和长度、独立的加密和解密算法、初始化向量等。

Data _ Enc _ Key：受 ASSR 约束的形式

正常数据的加密密钥参考。

Data _ Dec _ Key：受 ASSR 约束的形式

正常数据的解密密钥参考。

Exp _ Enc _ Key：受 ASSR 约束的形式

加快数据的加密密钥参考。

Exp _ Dec _ Key：受 ASSR 约束的形式

加快数据的解密密钥参考。

这些“关键”属性的初值应在 SA 建立时设置，且在联系生命期内可改变。

注：附加的机制特定属性将在本标准的将来版本中标识，专用机制也一样。

12.3 规程

12.3.1 封装功能

SA-ID 用于引用安全联系。若安全联系不存在，应返回差错 SA-not-available 而封装的八位位组串的值不定。

若(Encipher 为 TRUE)，则应加密封装前八位位组串，Enc _ Alg 应标识使用的算法且使用的密钥应是：

a）Data _ Enc _ Key，若 data-unit-type＝normal；或

b）Exp _ Enc _ Key，若 data-unit-type＝expedited。

加密数据应作为封装的八位位组串中的结果而返回。

12.3.2 解封功能

若下列检验任何一项失败，除了警告、审计和/或帐户信息外，所有的安全相关状态信息都将被置为接收该信息前的安全状态信息。

SA-ID 自变量应用于引用安全联系。若安全联系不存在，则应返回差错 SA-not-available 且封装前八位位组串的值应不定。

若(Encipher 为 TRUE)，则应解密封装的八位位组串，Enc _ Alg 应标识使用的解密算法，且使用的密钥应是：

a）Data _ Dec _ Key，若 data-unit-type＝normal；或

b）Exp _ Dec _ Key，若 data-unit-type＝expedited。

解密数据的值应作为封装前八位位组串的结果而返回。

13 PDU 的结构和编码

13.1 导引

NLSP 协议使用 3 种 PDU 类型：

a）安全数据传送 PDU；

b）安全联系 PDU；

c）连接安全控制 PDU。

无 PCI 的非结构化数据格式与保护数据的 No _ Header 选项一起使用。

所有的 PDU 应包含整数个八位位组。PDU 中八位位组从 1 开始编号，并按序增加，按照这个顺序把它们放入合适的“底层网”请求。当相邻的八位位组用于表示二进制数时，低八位位组数有最有意义的值。八位位组中的位从 1 到 8 编号，这里 1 是低序位。

当在本章中用图解表示 PDU 的编码时，

a）用最低编号的八位位组在左或在上来显示八位位组；

b）在八位位组中，用第八位在左及第 1 位在右来显示位。

方框下的记法显示八位位组中每个字段的长度；“可变”指明该字段长度是可变的。

安全联系中包含的属性应规定“任选的”字段出现或不出现。

注：任选字段之所以是任选的，在于给出的安全联系应要求某些字段出现，其他字段不出现。一旦决定了安全联系，每个字段的出现或不出现由 SA 属性来确定。

13.2 内容字段格式

内容字段是把数据值放置于本章定义的 PDU 中的一般字段格式(见图 6)。

类型	长度	值
1	1～3	可变

图 6 内容字段

内容字段类型应置为下列值之一：

值	内容字段类型
00～5F	为专用保留
60～9F	为将来使用保留
A0～BF	为 SA-P 使用保留(见附录 C)
C0～CF	为独立于机制使用保留(见 13.3.4.3)
D0～FF	为依赖于机制使用保留(见 13.3.5)

内容字段长度应包含八位位组中内容字段值的长度。内容字段长度应是 1 个、2 个或 3 个八位位组长：

a）若 1 个八位位组长，则第 8 位为 0，余下的 7 位定义长度值，可达 127 个八位位组；

b）若 2 个八位位组长，则第一个八位位组按 10000001 编码，余下的 1 个八位位组定义的字段长度达 255 个八位位组；

c）若 3 个八位位组长，则第一个八位位组按 10000010 编码，余下的两个八位位组定义字段长度达 65535 个八位位组。

第一个八位位组的其他值保留给将来使用。

内容字段值应包含 PDU 字段的数据。

13.3 保护的数据

本条描述传送保护数据用的 PDU。它包括 PDU 的两个方面：那些独立于使用的机制(标上通用)和那些特定于第 11 章中定义的封装规程所支持的机制的(标上机制特定)。那些包括通用和机制特定方面的标上混合。

13.3.1 基本 PDU 结构(通用)

为传送安全数据定义了两种数据结构。第一种对 NLSP-CL 是强制的，NLSP-CO 必须支持两者之一。

a) 格式化的安全数据传送 PDU 如图 7 所示。

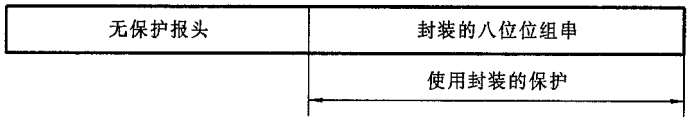


图 7 通用安全数据传送 PDU 结构

在 13.3.2 定义了无保护报头的结构。封装的八位位组串字段应包含来自封装功能的输出(例如,在第 11 章所述的使用 13.3.3 中定义的结构),该封装功能在按 13.3.4 中所述结构化的封装前八位位组串上操作。

支持形成该 PDU 的字段的条件(强制/任选的等)在 D5.3、D5.4(机制特定字段)、D6.4(仅 NLSP-CL)和 D7.6(仅 NLSP-CO)中定义。

b) 无报头保密性选项格式的非结构位串如图 8 所示。不加上 PCI。

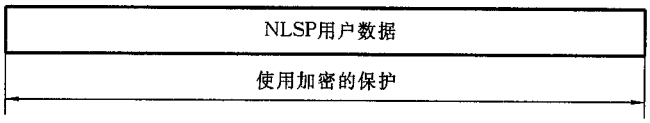


图 8 仅使用无报头选项的保密性

当下列所有条件满足时,仅使用无报头选项:

a) No _ Header 为 TRUE;

b) Lable 为 FALSE;

c) ICV 为 FALSE;

d) ISN 为 FALSE;

e) Encipher 为 TRUE;

f) Enc _ Sync _ Len=0;

g) Enc _ Blk=1;

h) Pad 为 FALSE。

13.3.2 无保护报头(通用)

无保护报头的格式如图 9 所示。

协议 Id	LI	PDU 类型	SA-ID
1	1	1	可变

图 9 无保护报头

13.3.2.1 协议 Id(通用)

该字段包含 NLSP 协议标识符,值为 10001011。

13.3.2.2 LI(通用)

该字段包含 PDU 类型字段加上 SA-ID 的长度。

对于 NLSP-CO,不要求 SA-ID 字段。因此,应如象 SA-ID 字段不出现那样设置该字段(即值为 00000001)。

13.3.2.3 PDU 类型(通用)

该字段包含值为 01001000 的 PDU 类型以指明安全数据传送 PDU。

13.3.2.4 SA-ID(通用)

SA-ID 字段应包含远程实体的安全联系标识符(即 SA 属性 Your _ SA-ID)。NLSP-CO 不要求该字段。

13.3.3 封装的八位位组(机制特定)

第 13 章中定义的使用机制特定规程的 SDT PDU 的结构如图 10 所示。

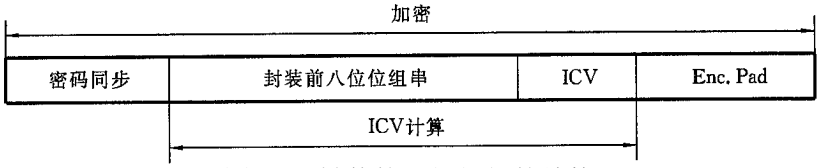


图 10　封装的八位位组的结构

13.3.3.1　密码同步(机制特定)

这是任选的字段,它可包含特定的加密算法的同步数据。它的出现、形式、长度由 **Enc _ Alg** 暗指。

13.3.3.2　完整性检验值(机制特定)

该字段包含完整性检验值(**ICV**)。安全联系属性中包含的 **ICV** 算法标识符定义该字段的长度。

13.3.3.3　加密填充(机制特定)

该字段包含加密填充(**Enc. Pad**),用来支持保密性的块加密算法。填充值的选择是本地事性。所有的 **NLSPE** 必须能丢弃该字段。该字段的格式应按 13.2 中定义的编码或按加密算法定义。**TLV** 字段的类型码如 13.3.5 中定义的。若要求 2 个八位位组的填充,长度应为 0 且无值。若要求单个八位位组的填充,应使用单个八位位组填充字段而不是加密 **PAD** 字段。

该字段的使用取决于加密算法是否要求独立的加密填充。

13.3.4　封装前八位位组串(混合)

图 11 显示了封装前八位位组串的格式,它包含任意数目的通用和机制特定内容字段。

应至少出现内容长度和数据类型。

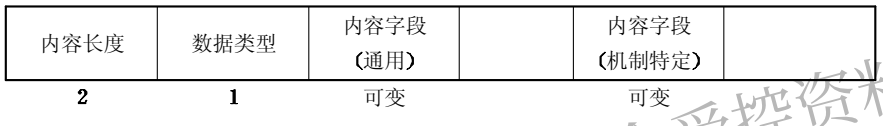


图 11　封装前八位位组串

13.3.4.1　内容长度(通用)

该字段应包含所有内容字段和数据类型的联合长度。

注:它不包括 **ICV** 或加密填充字段。

13.3.4.2　数据类型(通用)

该字段的第 8 位是“启动者到响应者”标志。值 1 指明启动者到响应者,值 0 指明从响应者到启动者。

该字段的第 7 位是“**Last/Not Last**”标志。当 **SDT PDU** 包含序列的最后一段时,该位取 0 值。否则为 1。对于 **NLSP-CL**,它一直为 0。

该字段的第 1 至第 6 位被编码来标识如下的 **NLSP** 服务原语:

值	服务原语
000000	与任何 **NLSP** 服务原语无关(例如,测试数据)
000001	**NLSP-UNITDATA req/ind**
000010	**NLSP-CONNECT req/ind**
000011	**NLSP-CONNECT resp/conf**
000100	**NLSP-DATA req/ind**
000101	**NLSP-DATA-ACKNOWLEDGE req/ind**
000110	**NLSP-EXPEDITED DATA req/ind**
000111	**NLSP-DISCONNECT req/ind**
001000	**SA** 协议
001001～011111	为将来使用保留
100000～111111	为专用使用保留

13.3.4.3 内容字段(通用)

内容字段类型按13.2中定义的编码。第6章、第7章和第8章的规程使用机制独立内容字段(即CO-CF)在下面给出:

值	内容字段类型
OO～BF	保留
CO	用户数据
C1	测试数据
C2	主叫/源NLSP地址
C3	被叫/目的NLSP地址
C4	证实的NLSP地址
C5	不用
C6	标号
C7	标号参考
C8	证实请求
C9	断开原因
CA～CF	为将来使用保留
DO～FF	保留

13.3.4.3.1 NLSP用户数据

该字段包含从服务原语中来的NLSP用户数据。

13.3.4.3.2 测试数据

测试数据的结构如图12所示。

测试控制	测试数据
1	可变

图12 测试数据

测试控制包含下列分配的一系列位:

a) 第1位——方向标志。0表示源,1表示转向的测试数据;

b) 第2位至第4位——为将来使用保留;

c) 第5位至第8位——为专用使用保留。

13.3.4.3.3 主叫/源NLSP地址

该字段包含以GB/T 15126/AD2中所述的形式之一编码的网络层地址。

13.3.4.3.4 被叫/目标NLSP地址

该字段包含以GB/T 15126/AD2中所述的形式之一编码的网络层地址。

13.3.4.3.5 响应NLSP地址

该字段包含以GB/T 15126/AD2中所述的形式之一编码的网络层地址。

13.3.4.3.6 标号

该字段用来携带PDU的安全标号。若出现标号参考内容字段,则不出现该字段(见图13)。

权限长度	定义权限	标号的内容
1～3	可变	可变

图13 标号的值

定义的权限应作为客体标识符值的内容被编码,使用GB/T 16263的第22章中定义的客体标识符的基本编码规则。

各种定义权限定义了标号内容的结构和说明。

注：期望在国家标准定义的规程下登记这些标号。定义权限将作为客体标识符登记，使用 ISO/IEC 9834 中定义的规程。

13.3.4.3.7 标号参考

该字段标识 SA 属性 Label-Set 中定义的一系列安全标号之一。当出现时该字段总是应编码，这样字段的值部分为 2 个八位位组，若标号内容字段出现，则不出现该字段。

13.3.4.3.8 证实请求

当出现时，该字段指明请求接收的证实。该字段应作为一个八位位组类型码被编码(无长度或值)。

13.3.4.3.9 断开原因

该字段应携带 NLSP-DISCONNECT 原因服务参数，按底层网中携带的编码。

注：在底层网是 GB/T 16974 网络的情况下，第一个八位位组是原因的值，若出现，第二个八位位组是从 NLSP-DISCONNECT 原因映射的诊断码，如 GB/T 16976 中定义的。

13.3.5 内容字段(机制特定)

内容字段编码如 13.2 中定义的。下面给出了机制特定内容字段的内容字段类型编码：

值	内容字段类型
00～CF	保留
D0	顺序号
D1	单个八位位组填充
D2	通信量填充
D3	完整性填充
D4	加密填充
D5～FF	保留给将来使用

13.3.5.1 顺序号

该字段包含 Your _ ISN(即，PDU 完整性顺序号)，它在当前密钥中对数据类型(加快或正常)应是唯一的。

注：在 NLSP CO 中，加快和正常数据流之间的唯一性(因此重演保护)由不同的数据类型字段(见 13.3.4.2)来提供。

13.3.5.2 单个八位位组填充

该字段是通用填充(例如支持完整性填充的单个八位位组)的一个八位位组类型(没有长度和值)字段。该八位位组可以使用一次或多次，代替 TLV 编码完整性、加密或通信量填充字段来提供完整性、加密或通信量填充。所有的 NLSPE 应检测并丢弃该字段。

13.3.5.3 通信量填充

该字段包含用于通信流量保密性的填充。填充值的选择是本地事情。所有的 NLSPE 应检测并丢弃该字段。若要求 2 个八位位组填充，长度应为无值的 0。若要求单个八位位组填充，应使用单个八位位组填充代替通信量填充。

13.3.5.4 完整性填充

该字段包含用于支持块完整性算法的填充。填充值的选择是本地事情。所有的 NLSPE 必须能丢弃该字段。若要求 2 个八位位组，长度为无值的 0，若要求单个八位位组填充，应使用单个八位位组填充代替完整性填充。

该字段也可用来满足加密填充要求。

13.4 安全联系 PDU

安全联系 PDU 格式如图 14 所示。

支持形成该 PDU 字段的条件(强制/任选的等)在 D5.5 和 D5.6(机制特定字段)中定义。

协议 Id	LI	PDU 类型	SA-ID	SA-P 类型	SA-PDU 内容
1	1	1	可变	可变	可变

图 14　安全联系 PDU 结构

13.4.1　协议标识符(PID)

该字段包含 NLSP 协议标识符,值为 10001011。

13.4.2　LI

该字段包含 PDU 类型字段加上 SA-ID 字段的长度。

若 SA-P 需要告知它不知道其对等的 SA-ID(例如建立新的 SA 时),该字段应设置为 00000001,指明 SA-ID 字段不出现。

13.4.3　PDU 类型

该字段包含 PDU 类型,值为 01001001,指明安全联系 PDU。

13.4.4　SA-ID

SA-ID 字段包含远程实体的安全联系标识符(即 SA 属性 Your _SA-ID)。当 SA-P 被用来建立一个新的 SA 时,不要求该字段(即接收方还未分配 SA-ID)。

13.4.5　SA-P 类型

该字段包含客体标识符,指明用于提供 SA 协议的机制。使用 GB/T 16263 中第 22 章定义的基本编码规则把该客体标识符编码为客体标识符值的内容,单个八位位组长度指示符在前。

分配的下列客体标识符用于通用 SA-P,它具有附录 C 中定义的密钥令牌交换规程和附录 H 中描述的指数密钥交换算法:

join-ccitt-iso nlsp (22) sa-p-eke(1)

具有附录 C 中定义的 SA-P 的其他 SA 协议或算法的使用可根据 ISO/IEC 9834-1 分配的更多的客体标识符来指明。

13.4.6　SA-PDU 内容

该字段的内部结构取决于如上面 13.4.5 中规定的提供 SA 协议的机制。附录 C 定义了一个这样的 SA 协议。

13.5　连接安全控制 PDU

连接安全控制 PDU 的格式如图 15 所示。

支持形成该 PDU 字段的条件(强制/任选的等)在 D7.7、D7.8(机制特定字段)中定义。

协议 ID	LI	PDU 类型	SA-ID	内容长度	CSC-PDU 内容
1	1	1	可变	1	可变

图 15　连接安全控制 PDUF

13.5.1　协议标识符

该字段包含 NLSP 协议标识符,值为 10001011。

13.5.2　LI

该字段包含 PDU 类型字段加上 SA-ID 字段的长度。

13.5.3　PDU 类型

该字段包含值为 xx111111 的 PDU 类型,指明连接安全控制 PDU。该字段的位置应如下:

a) 第 1 位至第 6 位——包含值为 111111 的 PDU 类型,指明安全服务控制 PDU;

b) 第 7 位——UNC-UND 标志,若设置它则指明 UN-Data 中携带着 NLSP-CONNECT,否则,若清除它,则指明 UN-CONNECT 中携带着 NLSP-CONNECT;

c) 第 8 位——SA-P 标志,指明该连接中正调用 SA-P,若设置第 8 位,则该 PDU 中不再出现更多的字段。

13.5.4　SA-ID

SA-ID 字段包含远程实体的安全联系标识符(即 SA 属性 Your _SA-ID)。若设置 SA-P 标志,该字

段不出现。

13.5.5 内容长度

它包含八位位组中 CSC-PDU 内容的长度。若设置 SA-P 标志，该字段不出现。

13.5.6 CSC-PDU 内容

该字段的内部结构应取决于支持连接鉴别的机制。若设置 SA-P 标志，则不出现该字段。第 10 章中给出的特定安全控制机制要求的字段如下(见图 16)。

封装权限数据	密钥信息
(注 1)	(注 2)

注

1 封装权限数据的长度取决于使用的加密算法，并由 SA 属性 Enc _ Auth _ Len 定义。

2 密钥信息的长度取决于使用的密钥分配方法。若不改变密钥，则不包括它。

图 16 CSC-PDU 内容

13.5.7 加密的 Auth-Data(机制特定)

见图 17。

该字段包含的编号用于鉴别，若被选择，作为完整性顺序号，它的长度被定义为 SA 属性的一部分。当从主叫方送到被叫 NLSP 实体时，Your-initial ISN 为 0。

My-Initial ISN	Your-Initial ISN
可变	可变

图 17 加密的 Auth-Data

13.5.8 密钥信息(机制特定)

取决于为安全联系选择的密钥分配方法，该参数不出现，指明一个存在着的密钥应被使用，或包含取决于 SA 属性 kdm 的下列之一：

kdm _ mutual- 使用多重 KEK 的加密密钥

kdm _ asymmetric _ single- 具有接收者公开密钥的加密密钥

kdm _ asymmetric _ double- 具有发送者的专用密钥和接收者的公开密钥的加密密钥

kdm _ distributed- 密钥参考

kdm _ other- 专用定义的内容

该字段的出现意味着内容长度与 SA-属性 Enc _ Auth _ Len 的比较。

14 一致性

14.1 静态一致性要求

14.1.1 一致性类

系统应支持一致性的下列类中的一个或两个：

a) NLSP-CL 方式；

b) NLSP-CO 方式。

对这些一致性类的支持按照 14.1.2 和 14.1.3 中定义的性能定义。

使用本标准支持的安全机制，对一致性的每一类的支持是任选的。

本标准支持的安全机制的使用按照 14.1.5 中定义的安全机制的要求定义。

14.1.2 NLSP-CL 方式能力

14.1.2.1 安全服务

与 NLSP-CL 方式一致的系统应支持下列服务；

a) 一个或多个下列服务：

1) 无连接保密性；

2) 无连接完整性；

3) 数据原发鉴别。

b) 任选地，访问控制；

c) 任选地，通信流量保密性。

14.1.2.2 保护的范围

声称与NLSP-CL一致的系统应支持一个或两个：

a) 所有NLSP服务参数的保护；

b) NLSP用户数据的保护；

声称与NLSP-CL一致的系统任选地支持：

c) 无保护。

14.1.2.3 其他能力

当支持NLSP-CL方式时，系统可传送和/或接收SDT PDU。

14.1.3 NLSP-CO方式能力

14.1.3.1 安全服务

与NLSP-CO方式一致的系统应支持下列安全服务：

a) 一个或多个下列服务：

1) 连接保密性；

2) 无恢复的连接完整性；

3) 对等实体鉴别。

b) 任选地，访问控制；

c) 任选地，通信流量保密性。

14.1.3.2 保护的范围

声称与NLSP-CO一致的系统应支持一个或多个：

a) 保护所有NLSP服务参数；

b) 保护NLSP用户数据，包括NLSP-CONNECT和NLSP-DISCONNECT中的NLSP用户数据；

c) 在数据传送中保护NLSP用户数据；

声称与NLSP-CL一致的系统任选地支持：

d) 无保护。

14.1.3.3 其他能力

当支持NLSP-CO方式时，系统应能够：

a) 启动和/或接受连接；

b) 传送并收到CSC PDU；

c) 传送和或收到至少一个：

1) 使用基于无报头的封装机制保护的数据，如6.4.1.2和6.4.2.2中定义的；

2) 基于SDT PDU的封装，如6.4.1.1和6.4.2.1中定义的。

d) 至少在8.5中定义的NLSP连接建立方式之一；

e) 任选地，支持测试交换；

f) 任选地，支持带内SA协议。

14.1.4 对PDU的支持

表3显示给定的PDU的支持对于给定的操作是强制的还是任选的。

14.1.5 机制静态要求

声称支持本标准中定义的安全机制的系统应满足下列要求，就选择的机制而论：

a) 声称支持连接或无连接保密性安全服务的每个系统应通过使用加密机制提供那些服务；

b）声称支持无连接完整性或无恢复的连接完整性安全服务的每个系统应提供使用机制的那些服务，机制使用 13.3.3.2 中定义的 ICV 字段和任选地在 13.3.5.1 中定义的 ISN 字段；

c）声称支持通信流量保密性安全服务的每个系统应提供使用机制的服务，该机制使用 13.3.5.3 中定义的通信量填充字段；

d）声称支持数据原发鉴别安全服务的每个系统应提供使用加密机制或密码机制的服务。该机制使用 13.3.3.2 中定义的 ICV 字段；

e）声称支持对等实体鉴别安全服务的每个系统应支持 13.5.7 中定义的加密的 authdata 字段。

表 3　对 PDU 的 NLSP 支持

PDU	支持条件
SDT PDU	强制的，对 CL 强制的，若支持基于封装的 CO 和 SDT PDU
SA PDU	任选的，若支持 SA-P
CSC PDU	强制的，对 NLSP-CO

14.2　动态一致性要求

14.2.1　一般要求

a）系统应正确地产生、接收和响应所有的有效协议元素，它们支持声称一致性的每个类和操作方式；

b）系统应正确响应 NLSP 协议元素的所有不正确序列。

14.2.2　特定要求

对每个声称一致性的一致性类和实现静态一致性要求的每个选项，系统应展示外部行为与下列正实现的相一致：

a）第 6 章中定义了公共协议功能；

b）对于 NLSP 方式，第 7 章中定义的协议功能；

c）对于 NLSP-CO 方式，第 8 章中定义的协议功能；

d）对于支持机制特定规程的 NLSP-CL 系统，第 11 章中定义的协议功能；

e）对于支持机制特定规程的 NLSP-CO 系统，第 10 章中定义的协议功能，对于连接安全控制和封装协议功能，在第 11 章和第 12 章中定义；

f）对于 PDU 的结构和编码，如第 13 章中所述的 PDU 的结构和编码。

14.3　协议实现一致性声明

实现本标准的一致性的任何声称应完成附录 D 中给出的协议实现一致性声明(PICS)，应根据相关的 PICS 形式表来产生 PICS。

附 录 A
（标准的附录）
映射 UN 原语至 GB/T 15126

表 A1

UN 原语	由下列原语传送	注 释
UN-UNITDATA	N-UNITDATA	从 UN 原语到 GB/T 15126 AD1 N-UNITDATA 原语的简单映射
UN-CONNECT	N-CONNECT	参数映射到等价的 GB/T 15126 参数上，只是： UN 鉴别与 UN 用户数据连在一起被映射到 N-CONNECT 原语的用户数据中
UN-DATA	N-DATA	简单映射：全部参数映射到等价的 GB/T 15126 参数上
UN-EXPEDITED-DATA	N-EXPEDITED-DATA	简单映射
UN-DATA-ACKNOWLEDGE	N-DATA-ACKNOWLEDGE	简单映射
UN-DISCONNECT	N-DISCONNECT	简单映射

附 录 B
（标准的附录）
映射 UN 原语至 GB/T 16974

在 OSI 环境中，在 UN 服务原语与 GB/T 16974 之间的映射如同在 GB/T 16976 为等价的网络层服务原语一样定义，DTE“保护设施”中传送的 UN-CONNECT UN 鉴别参数除外。

表 B1 中间一栏描述了用来传送 UN 原语的 GB/T 16974。在这种情况下，GB/T 16974 可以以本标准允许的任何方式使用。例如，可以调用 Q-bit。这样的GB/T 16974的特定性质通过 NLSP 无改变地传递。

表 B1

UN 原语	由下列原语传送	注 释
UN-UNITDATA	N/A	
UN-CONNECT	CALL	除 DTE“保护设施”中传送的 UN 鉴别参数之外，所有参数映射到等价的 GB/T 16974 CALL包设施中。
UN-DATA	DATA	简单映射
UN-EXPEDITED-DATA	INTERRUPT	简单映射
UN-DATA-ACKNOWLEDGE	RR 或 RNR	简单映射
UN-DISCONNECT	CLEAR	简单映射

附 录 C
（标准的附录）
使用密钥令牌交换和数字签名的安全联系协议

C1 导引

本附录为使用不对称机制执行SA的建立和夭折/释放而定义了一个协议，它允许通信NLSP实体以便：

a）两实体互相鉴别；

b）初始化包括密钥的SA属性；

c）建立初始信息以在提供完整性时使用。

本附录描述了一个SA协议，它逻辑地执行下列明显功能：

a）使用密钥令牌交换建立一个共享秘密。它支持密钥令牌交换，这些令牌的形式是机制特定的。附录H略述了一个机制特定密钥令牌的例子，它支持指数密钥交换，也称为Diffie Hellman交换；

b）证书、数字签名和来自于密钥令牌交换的元素都用来获取鉴别；

c）协议交换用来协商SA属性；

d）协议交换发出SA正被释放的信号。

使用本SA协议建立SA之前每个NLSP实体必须预先建立下列信息：

a）它支持的机制，表达为：

1）支持的ASSR列表；

2）为上面标识的每个ASSR支持的安全服务集。

b）每个被支持的非对称算法的非对称密钥对可被NLSP实体使用以便为了鉴别目的而加标志数据；

c）每个被支持的非对称算法的信任权限的证书，为鉴别目的，它标识了NLSP实体及其公开非对称密钥；

d）任何信任证书权限的公开密钥和暗指的非对称算法，它将给NLSP实体发出证书，该NLSP实体将与之通信。

本SA协议动态地建立了下列安全信息，它需要这些信息以保证它的通信：

a）加密算法的协商，以保护SA协议通信；

b）非对称算法的协商及用来提供SA协议鉴别的数字签名模式；

c）加密算法必需的密钥信息的生成，以保护SA协议通信。

本SA协议在两个NLSP实体间建立下列共享信息：

a）本地和远程SA-ID；

b）用在通信实例的联系实体间的安全服务；

c）机制及其通过选择的安全服务暗指的参数；

d）通信实例的完整性、加密机制及鉴别的初始共享密钥；

e）可在访问控制联系上使用的安全标号集。

一个SA可使用与先前已建立的SA选择相同的安全服务、机制及其参数和安全标号集来建立。在这种情况下，只有SA-ID和密钥被改变，所有其他属性应保持原样。

每当建立一个新SA，就应建立新的密钥值。

在无连接方式NLSP中，一个SA被释放后，SA-ID应放置于冻结状态，在冻结状态，SA-ID不应被重用。SA-ID被冻结的期限应比底层网中PDU的最大生命期更长。

SA 属性 Adr _ Served 用本协议外的方法建立。

SA 属性 Initiator 为 SA 协议交换启动者置为真，为 SA 协议交换响应者置为假。

C2 密钥令牌交换(KTE)

NLSP 实体用密钥令牌交换开始其 SA 协议以在实体间生成一个共享秘密(即一个位串)。NLSP 实体接着用该秘密位串的一个子集与专用密钥算法一起在它们之间加密通信剩余部分。因此就对 SA 协议交换的剩余部分提供了保密性。

KTE 涉及到 Key-Token-1 与 Key-Token-2 两个值的交换。该两值是由机制特定参数连同如附录 H 略述的机制特定算法本地生成的数字一同计算出的，被交换的值然后由两个通信实体使用以产生共享秘密位串。

该位串的子集连同一个专用密钥算法一起用于加密支持 SA 协议鉴别和 SA 属性协商的 SA 协议交换的剩余部分。另外，该位串的子集也被引用来作为正在建立的安全联系的密钥和 ISN 属性，这被下列之一引用：

1) 由 SA 属性 Negotiation 中的交换位置信息；

2) 通过先验的知识。

C3 SA 协议鉴别

一个 NLSP 实体为了在 SA 建立期间鉴别另一个，它需要鉴别证书及公开密钥对。

NLSP 实体交换证书及数字签名(如 GB/T 16264.8 定义的)以核实每一实体的身份。一个证书至少包含一些 NLSPE 标识信息加上该实体的公开密钥。

证书由信任权限证明，并使用 NLSP 协议范围外的规程来提供给 NLSP，证书携带信任权限的鉴别签名，参与该 SA 协议的 NLSP 实体应具有发出证书的信任权限的公开密钥，用于获得此信任权限的公开密钥的方法在本标准范围之外。NLSP 实体要证明它拥有特别证书，它必须证明它知道相应证书中的公开密钥的秘密密钥。

适时证明和防止重演攻击是由加标志数据编址的，该数据由共同确定的特定数值和对该协议的特定操作组成，对两个通信实体 A(SA 的启动者)和 B(响应者)，按下列去做：

a) 创建 SA 内容，包括 A 的证书和 Key-Token-3(用附录 H 中描述的算法计算出)接着签名(例如，使用在 GB/T 16264.8 中定义的鉴别签名)。这个签名不包括交换 ID 和内容长度。然后加密，包括签名和内容长度但不包括交换 ID 的 SA 内容。加密密钥就是 KTE 交换产生的位串的头 n 位，其中 n 为所用算法要求的位数；

b) 创建携带 SA 属性协商(见 C4)或夭折/释放原因(见 C5)的 SA 内容，然后如上面 a)，使用与实体 B 相关的等价信息和 Key-Token-4 而不是 Key-Token-3 来签名和加密。

每个实体通过首先对接收的交换解密来核实对等实体的鉴别签名，然后核实签名及检验密钥令牌以保护不被重演攻击，核实需要使用对等实体公开密钥，以及核实签名的商定过程。

C4 SA 属性协商

C4.1 安全服务选择

作为本地判定，启动的 NLSP 实体发出一个或多个可接受的安全服务选择集，该集中的每一元素包含下列：

a) ASSR _ ID，它为集中的该元素定义了所选择的安全服务的语义；

b) 每一个保密性、鉴别、访问控制、完整性及通信流量保密性的服务选择值(由 ASSR _ ID 定义的语义)。

作为本地判定，接收者 NLSP 实体将给原发者返回下列 PCI：

a）若提出的服务集之一是可接受的，接收者将返回单个所选择的服务元素；

b）若提出的服务集无一个可接受，接收者将拒绝该SA，并返回一个状态指明拒绝SA 的原因。

注：该协商允许两个 NLSP 实体选择与其本地安全策略一致的安全服务。

C4.2 标号集协商

基于它的本地安全策略，启动的NLSP 实体发出一个安全标号和参考的集，该集要在该SA 的保护之下传送，集中的每一元素包含：

a）在SA 的生命期间为了效率的缘故为代替标号而携带的一个参考；

b）标号的全语义。

基于它的本地安全策略，接收者 NLSP 实体将确定要在该SA 保护之下传送哪一个提出的标号集，接收者 NLSP 实体将给原发者返回下列 PCI：

a）若提出的集中的一个或多个标号是可接受的，接收者将返回提出的参考集的一个子集，不允许空集；

b）若提出的集中没有可接受的标号，接收者应拒绝该 SA，通过返回一个状态指明拒绝 SA 的原因。

注：该协商允许 NLSP 实体双方选择一个与其本地安全策略一致的标号集。

C4.3 密钥和 ISN 选择

作为本地判定，启动的 NLSP 实体在向接收者 NLSP 实体通信期间（即 NLSP 通信而非 SA 协议通信）选择由 KTE 导致的位串的那些部分用作密钥和/或 ISN。该密钥/ISN 通过 EKE 结果位串中的起始位位置的通信来标识。该密钥/ISN 长度由与选择服务联系的参数确定，发送到接收者 NLSP 实体的指针集为下列：

a）正常数据加密密钥；

b）加快数据加密密钥；

c）正常数据完整性检验生成密钥；

d）加快数据完整性检验生成密钥；

e）正常数据的 My ISN；

f）加快数据的 My ISN；

g）鉴别生成密钥。

类似地，接收者 NLSP 实体将本地确定它将把 EKE 结果位串的哪一部分用作其密钥/ISN，接收者 NLSP 将给原发者返回下列 PCI：

a）若接收者选择使用与启动的 NLSP 实体提出的相同的位位置，则返回不明确的 PCI；

b）若接收者由于其他协商失败而拒绝 SA，则返回不明确的 PCI；

c）若接收者为其密钥/ISN 选择不同的位位置，它将返回一个指针集。

注

1 通过为多于一个密钥/ISN 提供同一指针，同一密钥值可用于多种目的。

2 若先验地知道选择的密钥和 ISN 的位置，不需使用该规程。

C4.4 杂项 SA 属性协商

作为本地判定，启动的 NLSP 实体为建立 SA 确定下列 SA 属性值：

a）在无连接时保留这些 SA 属性（仅 NLSP-CO）；

b）保护 CO 参数（仅 NLSP-CO）；

c）使用无报头选项（仅 NLSP-CO）。

启动的 NLSP 实体发送接收者 NLSP 实体在杂项标志字段中提出的 SA 属性集。

作为本地判定，接收者 NLSP 实体将对原发者返回下列 PCI：

a）若接收者接受所有提出的 SA 属性，则返回不明确的 PCI，若接收者不拒绝该 SA，则暗指该 SA

属性对接收者 NLSP 实体是可接受的；

b）若任何属性之一不可接受，接收者拒绝 SA 并通过返回一个状态来指明哪一个属性导致拒绝。

C4.5 重定密钥

若为重定密钥一个旧 SA 而建立 SA，则仅执行密钥和 ISN 选择。并把要继承这些属性的旧 SA 的引用放置于 Old-Your-SA-ID 中，而不是服务标号集及杂项 SA 属性协商。

C5 SA 夭折/释放

实体可指明，通过 SA PDU 与一个使用 C3 中定义的规程签名和加密原因码的双向交换，它不再使用安全联系。

C6 SA 协议功能到协议交换的映射

本 SA 协议在三个独特的协议交换期间执行前述的三个功能：

a）第一交换，由 EKE 和证书交换组成，且没有应用加密；

b）第二交换，由被保护的安全协商组成以提供 C3 定义的鉴别；

c）分离的交换，当不再要求 SA 时被启动，由被保护的原因码组成，以提供 C3 定义的鉴别。

C6.1 KTE(第一)交换

C6.1.1 请求启动 SA 协议

NLSP 实体或本地安全管理启动 SA 协议。

启动的 NLSP 实体执行下列功能并给接收者发送下列信息：

a）可获得的 SA-ID 作为原发者的 My _ SA-ID 被选择和放置；

b）开始 KTE，并发送 Key-Token-1；

c）提出保密性机制的列表，可用来保护第二 SA 协议交换。该列表被表达为包括下列一个或多个元素的集合：ASSR _ ID 和所选择的保密性安全服务。若机制事先已商定，则不发送该列表；

d）提出完整性机制的列表。其中之一可用于数字签名第二 SA 协议交换。该列表被表达为一个或多个包括下列元素的集合：ASSR _ ID 和所选择的完整性安全服务。若机制事先已商定，则不发送该列表。

注

1 选择的保密性安全服务将只标识一个对称加密算法及其操作方式。选择的完整性安全服务将只标识一个非对称算法及其联系的数字签名模式。

2 项目 c)和 d)可先验地知道。

在 CO 情况下，若超时后不为第一交换返回 PDU，则不建立 SA，并不做进一步尝试。

在 CL 情况下，若超时后不为第一交换返回 PDU，启动的 NLSP 实体再传送其第一交换 PDU，再传送限于本地定义的有限数。

C6.1.2 接收者接收的第一个 SA PDU

接收第一个 SA PDU 时，接收者 NLSP 实体执行下列功能并对启动者发送下列信息：

a）接收的 My _ SA-ID 被放置于 13.4 中描述的通用报头的 Your _ SA-ID 字段中；

b）选择可用的 SA-ID，并作为原发者的 My _ SA-ID 发送；

c）作为本地判定，接收者 NLSP 将给原发者返回下列 PCI：

1）若接收者接受了提出的保密性机制之一，则它返回选择的机制，若启动者提出单个机制，则返回不明确的 PCI；

2）若所有的保密性机制都不可接受，接收者拒绝该 SA 并通过返回一个状态指明拒绝的原因。

d）作为本地判定，接收者 NLSP 实体将对原发者返回下列 PCI：

1) 若接收者接受提出的完整性机制之一，则它返回选择的机制。若启动者提出单个机制，则返回不明确的 PCI；

2) 若所有的完整性机制都不可接受，接收者拒绝该 SA 并通过返回一个状态指明拒绝的原因。

e) 假若保密性和完整性机制都被选择，则开始 KTE 计算并发送 Key-Token-2。

在 CO 情况下，若超时后不返回来自第二交换的 PDU，则不建立 SA 且不做进一步的尝试。

在 CL 情况下，若超时后不返回来自第二交换的 PDU，启动的 NLSP 实体则再传送其第一交换 PDU，再传送限于本地定义的有限数。

在 CL 情况下，若再次收到来自第一交换的 PDU，则重发送返回的 PDU。

C6.2 鉴别和安全协商(第二)交换

C6.2.1 启动者接收的第一个 SA PDU

接收第一个 SA PDU 时，启动的 NLSP 实体执行下列功能：

a) 接收的 My _ SA-ID 被放置于如 13.4 所述的通用报头的 Your _ SA-ID 字段中；

b) 与选择的完整性机制联系的启动者证书被放置于内容字段证书中；

c) 启动者生成 Key-Token-3；

d) 用于保护 NLSP 通信的安全服务而提出的列表被放置于内容字段服务选择中；

e) 在 NLSP 通信期间用于该 SA 保护而提出的标号集被放置于 Label _ Def 中；

f) 密钥/ISN 选择集被放置于密钥选择中；

g) 该 SA 需求的杂项 SA 属性被放置于 SA 标志中；

h) 若 SA 建立要重定密钥一个旧 SA，则为了旧 SA 被重定密钥而 Old Your SA-ID 置为 SA-ID；若执行该处理，则不应执行上述 d)、e)和 g)；

i) 保护如 C3 所述的 SA 内容。

在 CO 情况下，若来自第二交换的 PDU 在超时后无返回，则不建立 SA，且不做进一步尝试。

在 CL 情况下，若来自第二交换的 PDU 在超时后无返回，启动的 NLSP 实体再传送其第二交换 PDU，再传送限于本地定义的有限数。

在 CL 情况下，若再次收到来自第一交换的 PDU，则再发送第二交换 PDU。

C6.2.2 接收者接收的第二交换 PDU

收到第二交换 PDU 时，接收者 NLSP 实体执行下列功能并给启动者发送下列信息：

a) 接收的 My _ SA-ID 被放置于如 13.4 所述的通用报头 Your _ SA-ID 字段中。

b) 检验下列项目，若任何项目检验失败，则拒绝 SA 并返回一个状态字段指明拒收原因：

1) 接收的数字签名检验为有效；

2) 接收的 Key-Token-3 检验为有效；

3) 提出的安全服务集检验为确定是否有可接受的。只选择一种提出的安全服务；

4) 提出的标号集检验为确定是否有可接受的；

5) 杂项 SA 属性检验为确定是否全部可接受。

c) 若接收 PDU 中出现 Old Your SA-ID，则从被引用的 SA-ID 中拷贝合适的 SA，在这种情况下，不能发送下面 c)、d)所述字段的使用。

假若所有检验通过，则发送下列项目：

a) 发送与选择的完整性机制联系的启动者证书；

b) 发送用来保护 NLSP 通信的选择安全服务，若提出的服务集只包括一个元素，则不返回 PCI；

c) 接收者生成 Key-Token-4；

d）发送在NLSP 通信期间使用该SA 保护提出的标号选择子集；

e）发送 Key/ISN 指针集，若启动者为响应者使用而提出的密钥是可接受的，则不发送新值；

f）保护如 C3 所述的 SA 内容。

在 CL 情况下，若再次收到来自第二交换的 PDU，接收者重发送其第二交换 PDU。

C6.3 SA 释放/夭折交换

C6.3.1 启动 SA 释放/夭折请求

NLSP 实体或本地安全管理启动 SA 释放/夭折，SA 夭折/释放的启动者不必是 SA 建立的启动者。

a）若本地实体是 SA 建立的启动者，则生成 Key-Token-3，否则生成 Key-Token-4。在两种情况下生成的令牌都放置于 SA 内容中；

b）合适的原因码被放置于 SA 内容字段夭折/释放原因中；

c）保护如 C3 所述的 SA 内容。

在 CO 情况下，若超时后未返回来自夭折/释放请求的证实 PDU，则不建立该 SA，并且不做进一步尝试。

在 CL 情况下，若超时后未返回来自夭折/释放交换的证实 PDU，则启动的 NLSP 实体再传送其 SA 释放/夭折请求 PDU，再传送限于本地定义的有限数。

C6.3.2 SA 夭折/释放请求的接收

在接收 SA 夭折/释放证实 PDU 时，接收者 NLSP 实体执行下列功能并且给启动者发送下列信息：

a）若本地实体是 SA 建立的启动者，则生成 Key-Token-3，否则生成 Key-Token-4，在两种情况下生成的令牌都放置于 SA 内容中；

b）合适的原因码被放置于 SA 内容字段夭折/释放原因中；

c）保护如 C3 所述的 SA 内容。

在 CL 情况中，若再次收到来自夭折/释放请求的 PDU，则接收者重发送其第二交换 PDU 直至给定的有限次数。

C7 SA PDU-SA 内容

13.4 中为本特定 SA 协议定义的 SA PDU 的 SA 内容字段的格式如图 C1 所示：

交换 Id	内容长度	内容字段	内容字段	···
1	2	可变	可变	可变

图 C1 SA 内容

C7.1 交换 ID

若 PDU 与第一密钥令牌交换联系，该字段包含的值为 00000000，若 PDU 与第二鉴别/协商交换联系，该字段包含的值为 00000001，若 PDU 与 SA 夭折/释放请求联系，该字段包含的值为 10000000，若 PDU 与 SA 夭折/释放证实联系，该字段包含的值为 10000001。

C7.2 内容长度

除了内容长度字段外的所有内容字段按八位位组计的长度。

C7.3 内容字段

内容字段类型编码在 13.2 中定义，由本附录中规程使用的 SA-P 内容字段（即 A0-BF）在下面给出：

值	内容字段类型
A0	My SA-ID
A1	Old Your SA-ID
A2	Key-Token-1
A3	Key-Token-2
A4	鉴别数字签名
A5	鉴别证书
A6	服务选择
A7	SA 拒绝原因
A8	SA 夭折/释放原因
A9	Label-Def
AA	SA 标志
AB	密钥选择
AC	ASSR
AD	Key-Token-3
AE	Key-Token-4
AF-BF	为将来使用保留

注：在本标准的 13.2 中，为专用使用而保留了相应代码。

服务选择、SA 拒绝原因、Label-Def、SA 标志及密钥选择等字段在本特定的 SA 协议内容定义中都是任选的。

C7.3.1 My SA-ID

该必选字段仅用于第一交换，该参数是安全联系的本地标识符。

C7.3.2 Old Your SA-ID

若除了密钥要从旧 SA 继承属性，则在第二交换中使用该字段。

C7.3.3 Key-Token-1、Key-Token-2、Key-Token-3 及 Key-Token-4

这些必选字段用于支持如本附录早先所述的 KTE 及鉴别。

C7.3.4 鉴别数字签名——证书

这些必选字段用于支持如本附录早先所述的鉴别。

C7.3.5 服务选择

该任选字段在第一及第二交换中都使用：

a）若在第一交换期间使用，它用来标识在第二 SA 协议交换期间要使用的保密性和/或完整性机制，在这情况中，仅前两个八位位组出现；

b）若在第二交换期间使用，它用来提出正在建立的 SA 保护的 NLSP 通讯期间要使用的所有机制。

该字段应跟在 ASSR 参数出现之后，可被一次或多次包括在第一或第二交换 PDU 中，以便为协商形成一个安全服务提出集，每个参数与直接的前导 ASSR 参数相关。

该参数包含指明要求选择安全服务级的八位位组序列，级别的语义定义为部分安全策略。每个安全服务八位位组以下面指明的顺序出现。若被截掉的八位位组都与值为 0 的服务相关，八位位组序列可被截短。一个值为 255 的八位位组指明选择的安全服务已被预先建立。

八位位组	含义
1	无连接保密性/连接保密件
2	无连接完整性/无恢复的连接完整性
3	数据原发鉴别/对等实体鉴别
4	访问控制
5	通信流量保密性

C7.3.6 SA 拒绝原因

该任选字段可出现在第一或第二交换 PDU 中。它的出现指明在 SA 建立期间的 SA 拒绝，它包含下列拒绝原因：

值	含义
1	不支持保密性机制
2	不支持完整性机制
3	不支持访问控制机制
4	不支持鉴别机制
5	不支持通信流量保密性机制
6	拒绝保密性机制
7	拒绝完整性机制
8	拒绝访问控制机制
9	拒绝鉴别机制
10	拒绝通信流量保密性
11	无效的鉴别签名
12	无效证书
13	拒绝提出标号集
14	拒绝 Retain _ on _ Disconnect
15	拒绝 Param _ Prot
16	拒绝 No _ Header

C7.3.7 SA 夭折/释放原因

该必选字段出现在 SA 夭折/释放请求和指示中，它用来指明 SA 夭折/释放的原因。

该字段置 0 表示夭折，置 1 表示正常释放，2 到 127 为将来使用保留。其他值可为专用定义的原因码用。

C7.3.8 Label-Def

该任选字段仅用于第二交换中。可一次或多次包括 Label-Def 字段：

a）若原发者使用，提出安全标号集，启动者应一直使用两个子字段；

b）若接收者使用，选择已提出的标号集的子集，接收者应仅使用 Label _ Ref 子字段。

Label-Def 字段被分成两个子字段：

a）两个八位位组的 Label _ Ref 子字段(不使用 FFFF 值，因为该值为 NULL 标号参考保留)；

b）Label 子字段，其内容在 13.3.4.3.7 中定义。

Label _ Ref 是一个与 Label 子字段中定义的安全标号联系的数，Label _ Ref 用于其他 PDU 中作为携带联系的安全标号的替换。

C7.3.9 密钥选择

该任选字段仅用于第二交换 PDU 中，在 SCI-Contents 中它可出现任何次。

该字段分为三个子字段：

a) 用法标志(两个八位位组);

b) 密钥选择信息(两个八位位组);

c) 密钥参考(可变长)。

C7.3.9.1 用法标志

该子字段包含一些标志,它指明要用到前面的子字段中定义的密钥的安全目的。各个位编码为:0表示 FALSE,1 表示 TRUE。可为下列目的任意组合而使用该密钥,允许的组合将取决于本地安全策略。

位编号	服务	数据	数据源
第一个八位位组			
1	保密性	正常	SA 启动者
2	保密性	正常	SA 响应者
3	保密性	加快	SA 启动者
4	保密性	加快	SA 响应者
5	ICV 生成	正常	SA 启动者
6	ICV 生成	正常	SA 响应者
7	ICV 生成	加快	SA 启动者
8	ICV 生成	加快	SA 响应者
位编号	服务	数据	数据源
第二个八位位组			
1	鉴别		SA 启动者
2	鉴别		SA 响应者
3	ISN	正常	SA 启动者
4	ISN	正常	SA 响应者
5	ISN	加快	SA 启动者
6	ISN	加快	SA 响应者

响应者为了自己使用而使选择无效。

C7.3.9.2 密钥选择信息

该字段指明 EKE 结果位串中的位置,其中选择的密钥要取其值。密钥的长度由标识关联算法的关联选择安全服务确定。多密钥可使用相同的位位置(即相同密钥),允许的组合将取决于本地安全策略。

C7.3.9.3 密钥参考

该任选子字段使该密钥以后能够参考,例如它可用于审查目的或为使用连接安全控制 PDU 的连接的新密钥选择,该参考值对安全联系应是唯一的。

C7.3.10 SA 标志

该任选字段仅用于第二交换 PDU,下列位位置用来标记识别的 SA 属性,0 表示 FALSE,1 表示 TRUE。

位	SA 属性
1	Retain-on-Disconnect
2	Param _ Prot
3	No _ Header
4～8	保留给将来使用

4～8 位在传送时置为 0,接收时被忽略。

C7.3.11 ASSR

若服务选择字段出现,则 ASSR 字段必出现。它是客体标识符(如 ISO/IEC 9834-3 所定义),用来标

识安全规则集，它对给定选择服务保护质量定义了要应用的机制。

该字段可多次出现。在这种情况下服务选择参数跟在紧接相关前导 ASSR 参数的每次出现之后。

附 录 D
（标准的附录）
NLSP PICS 形式表[1)]

D1 导引

声称与本标准一致的协议实现的供应者应填写下列协议实现一致性声明(PICS)形式表。

已填写的PICS 形式表是对该实现的PICS。PICS 是对已实现协议的能力和选项的声明。PICS 可有多种用途，包括：

a）对协议实现者，用作检验清单以便通过监督来减少与本标准不一致的风险；

b）对实现的供应者和获得者或潜在获得者，说明了它与标准的 PICS 形式表所提供的公共理解基础的相对关系；

c）对实现的用户或潜在的用户，用作初始检验与另一个实现进行互工作的可能性的基础(注意，尽管互工作从来未能保证，但对互工作的故障往往能从不兼容的 PICS 中预测出来)；

d）对协议测试者，用作选择合适的测试的基础，根据这些测试来对实现一致性声称进行评估。

D2 缩略语和特殊符号

D2.1 状态符号

M　　必选

O　　任选

O.<n>　任选，但要求至少有一组由相同数字<n>标记的选项。

X　　禁止

<item>　条件限制项符号，它取决于对<item>标记的支持(见 D3.4)

D2.2 一般缩略语

N/A　不适用

PICS　协议实现一致性声明

D3 填写 PICS 形式表的说明

D3.1 PICS 形式表的通用结构

PICS 形式表的第一部分——标识和协议概要——要按照指明的充分标识供应者和实现两者所必需的信息来填写。

PICS 形式表的主要部分是分为三个主要条目的固定格式的调查表，覆盖了 NLSP-CL 和 NLSP-CL 的公共特征，后跟这两种操作方式每种的特定特征；它们被分为若干条，每条包含一组项目。对调查表各项目的答案放在最右端一栏，它或者是简单地标出一个答案以指明受限制的选择(常为“是”或“否”)或者是输入一个值或值的集合或数值范围。注意，对某些项目，从一组可能的答案中能适用两个或多个选择；所有相关选择都要作出标记。

每个项目通过引用项目被标识在第一栏；第二栏中包含要答复的问题；第三栏包含本标准的正文中

1）关于 PICS 形式表的版权放弃；

本标准的用户可自由复制本附录中的 PICS 形式表，以便可为特定目的使用和进一步出版已填写的 PICS。

规定该项目的一个或几个引用材料。其余各栏记录了项目的状态——不管该支持是必选的、任选的、禁止还是有条件的——并提供一定的空格以供答复；见下面的D3.4。

供应者可提供或可要求提供进一步的信息，这些信息可分为附加信息或异常信息。若提供时，每种进一步的信息为互相引用而分别标以A<i>或X<i>项目的另一条中提供。其中i是对该项目的明确标识(如简单数字)；其格式或展示没有其他限制。

包括任何附加信息和异常信息的一份已填好的PICS形式表是对该实现的协议实现一致性声明。

注：实现可以用一种以上的方法配置时，按照D5.1的项目，一个单独的PICS可以描述全部这样的配置。然而，若使信息展示更容易和更清楚，提供者有提供多个PICS的选择能力，每一个PICS都涉及该实现的配置能力的某一子集。

D3.2 附加信息

附加信息项允许供应者提供进一步的预期的信息以帮助解释PICS。不打算或不期望它供给大量的信息，在没有任何这种信息的情况下，也可认为PICS是完整的。一些例子可以表达若干方法的一种概括，用这些方法单个实现可能被建立起来，以便在各种环境和配置下操作；或者，这些例子也可以表达也许在特定应用需要时排除若干特征(尽管是任选的特征)的简短理由，而这些特征在网络层安全协议实现中通常仍然是存在的。

对附加信息项目的引用可放入调查表任何答案的下一位置上，也可包括在异常信息项中。

D3.3 异常信息

偶尔发生供应者希望用与指明的要求相冲突的方式(在应用了任何条件后)来答复带有必选或禁止状态的项目。在支持栏里对此找不到预先写出的答案；而是要求供应者在支持栏里写入异常信息项目的引用X<i>，并在异常项一栏里提供合适的理由。

以这种方法要求异常项的实现不一致于本标准。

注：上述情况的一个可能原因是本标准已报告了某种缺陷，期望为此而纠正以改变实现未满足的要求。

D3.4 条件状态

PICS形式表包含了许多条件项。这些是项本身的可适用性及它所适用的状态——必选、任选或禁止——取决于是否或不确定支持其他项。

由状态栏中形式为<item>：<s>的条件符号指明的单独条件项，其中<item>为在其他项目表中第一栏出现的项引用，<s>是一状态符号M、O、O.n或X之一。

若支持涉及条件符号的项，则条件项是可用的，其状态由<s>给出，支持栏以通常方法填写。否则，与条件项无关且要标上不适用(N/A)答案。

在条件符号中使用的每个项目引用都在项目栏中用星号指明。

D4 标识

D4.1 实现标识

供应者	
询问有关PICS的联系点	
实现名称和版本	
对整个标识所需的其他信息——例如机器和或操作系统名称和版本；系统名	

注

1 对所有实现只要求前三项，在满足整个标识的情况下可适当给出其他信息。

2 项目名和版本将作适当解释以符合供应者的术语(例如类型、系列、模型)。

D4.2 协议摘要

协议规范的标识	GB/T 17963
该 PICS 已填写的 PICS 形式表的修正案和勘误表的标识	GB/T 17963 修正案：　勘误表： 修正案：　勘误表： 修正案：　勘误表： 修正案：　勘误表：
要求有任何异常项(见 D3.3)? 注：答案“是”意味着该实现与本标准不一致。	是 □　否 □
声明日期	

D5　NLSP-CO 和 NLSP-CL 公共特征

D5.1　主要能力(公共)

项目	问题/特征	引用条号	状态	支持
CO*	支持连接方式?	5.1	O.1	是 □ 否 □
CL*	支持无连接方式?	5.1	O.1	是 □ 否 □
AC	支持访问控制?	5.2	O	是 □ 否 □
TFC*	支持通信流量保密性?	5.2	O	是 □ 否 □
ParamProt*	支持所有 NLSP 服务参数的保护?	5.5.1a	O.2	是 □ 否 □
UserDatProt	支持所有 NLSP 用户数据的保护?	5.5.1b	O.2	是 □ 否 □
NoProt*	支持无保护?	5.5.1c	O	是 □ 否 □
SdtBase*	支持基于任何 SDT PDU 的封装功能?	5.5.3	CO:O.3 CL:M ParamProt:M	是 □ 否 □
NoHead	支持任何无报头封装功能?	5.5.3	CO:O.3 CL:X ParamProt:X	是 □ 否 □ N/A □
SA-P*	支持任何带内 SA-P?	5.4.1	O	是 □ 否 □
LabMech*	支持标号机制?	6.2g, 6.4.1.1e 6.4.2.1f	SdtBase:O	是 □ 否 □ N/A □
SDTMech*	支持基于标准化 SDT PDU 的封装功能	11	SdtBase:O	是 □ 否 □ N/A □
NoHeadMech	支持标准化无报头封装功能?	12	NoHead:O	是 □ 否 □ N/A □

D5.2 PDU(公共)

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
SDT *	在发送/接收时支持安全数据传送 PDU?	6.4.1.1 13.3	SdtBase:M	是 □ N/A □	是 □ N/A □
SA *	在发送/接收时支持安全联系 PDU?	5.4.1, 13.4	SA-P:O	是 □ N/A □	是 □ N/A □

D5.3 对 CO 和 CL 公共,对机制通用的 SDT PDU 字段

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
SdtPID	每个 SDT PDU 中 PID 字段值 10001011	13.3.2.1	SDT:O	是 □ N/A □	是 □ N/A □
SdtLI	每个 SDT PDU 中长度指示符字段	13.3.2.2	SDT:M	是 □ N/A □	是 □ N/A □
SdtPDUType	每个 SDT PDU 中其值为 01001000 的 PDU 类型字段	13.3.2.3	SDT:M	是 □ N/A □	是 □ N/A □
SdtContLen	每个 SDT PDU 中内容长度	13.3.4.1	SDT:M	是 □ N/A □	是 □ N/A □
DataType	每个 SDT PDU 中数据类型字段	13.3.4.2	SDT:M	是 □ N/A □	是 □ N/A □
UserData	内容字段类型 CO——用户数据	13.3.4.3	SDT:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
CSAddr	内容字段类型 C2——主叫/源 NLSP 地址	13.3.4.3	ParamProt:M	是 □ N/A □	是 □ N/A □
CDAddr	内容字段类型 C3——主叫/目的 NLSP 地址	13.3.4.3	ParamProt:M	是 □ N/A □	是 □ N/A □
Label	内容字段类型 C6——标号	13.3.4.3	LabMech:O.4	是 □ 否 □ N/A □	是 □ 否 □ N/A □
LabRef	内容字段类型 C7——标号参考	13.3.4.3	LabMech:O.4	是 □ 否 □ N/A □	是 □ 否 □ N/A □
LabelExc	任何强制 SDT PDU 中标号和标号参考相互排斥?	13.3.4.3	LabMech:M	是 □ N/A □	是 □ N/A □

D5.4 具有基于特定SDT的封装机制的CO和CL的公共SDT PDU字段

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
Synch	密码同步	11.3， 13.3.3.1	O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
ICV	ICV字段	11.3， 13.3.3.2	COInteg:M CLInteg:M	是 □ N/A □	是 □ N/A □
EncPad	加密填充	11.3， 13.3.3.3	COConf:O CLConf:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
SeqNo	顺序号内容字段	11.3， 13.3.5.1	COInteg:O CLInteg:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
SinglePad	单个八位位组通用填充字段	11.3， 13.3.5.2	O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
TFCPad	通信量填充	11.3， 13.3.5.3	TFC:M	是 □ N/A □	是 □ N/A □
IntegPad	完整性填充	11.3， 13.3.5.4	COInteg:O CLInteg:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
注：所有上述字段以所选择的SDT Mech为条件。					

D5.5 SA-P通用的SA PDU字段

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
SaPID	每个SA PDU中PID字段的值为10001011	13.4.1	SA:M	是 □ N/A □	是 □ N/A □
SaLI	每个SA PDU中发送长度指示符字段?	13.4.2	SA:M	是 □ N/A □	是 □ N/A □
SaPDUType	每个SA PDU中其值为01001001的PDU类型字段	13.4.3	SA:M	是 □ N/A □	是 □ N/A □
SaSA-ID	SA-ID字段	13.4.4	SA:M	是 □ N/A □	是 □ N/A □
SA-PTtype	SA-P类型字段	13.4.5	SA:M	是 □ N/A □	是 □ N/A □
SAKTE*	支持使用密钥令牌交换的SA协议例子?	附录C	SA:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □

D5.6 密钥令牌交换 SA-P 特定的 SA PDU 内容字段

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
SAExchId	交换 ID	C7.1	SAKTE:M	是 □ N/A □	是 □ N/A □
ContLen	每个 SA PDU 发送长度指示符字段?	C7.2	SAKTE:M	是 □ N/A □	是 □ N/A □
MySA-ID	My SA-ID 内容字段	C7.3.1	SAKTE:M	是 □ N/A □	是 □ N/A □
OldYrSA-ID	Old Your SA-ID 内容字段	C7.3.2	SAKTE:M	是 □ N/A □	是 □ N/A □
KeyTokens	Key-Token-1,Key-Token-2,Key-Token-3,Key-Token-4 内容字段	C7.3.3	SAKTE:M	是 □ N/A □	是 □ N/A □
AuthFields	鉴别数字签名和鉴别证书内容字段	C7.3.4	SAKTE:M	是 □ N/A □	是 □ N/A □
ServSel*	服务选择内容字段	C7.3.5	SAKTE:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
SARejReas	SA 拒绝原因内容字段	C7.3.6	SAKTE:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
SAAbReas	SA 夭折/释放原因内容字段	C7.3.7	SAKTE:M	是 □ 否 □ N/A □	是 □ 否 □ N/A □
LabDef	标号定义内容字段	C7.3.8	SAKTE:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
KeySel*	密钥选择内容字段	C7.3.9	SAKTE:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
KeyUse	标志用法子字段	C7.3.9.1	KeySel:M	是 □ N/A □	是 □ N/A □
KeySelInfo	密钥选择信息子字段	C7.3.9.2	KeySel:M	是 □ N/A □	是 □ N/A □
KeyRefx	密钥参考子字段	C7.3.9.3	KeySel:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □

表（完）

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
SAFlags	SA 标志内容字段	C7.3.10	SAKTE:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
ASSR	ASSR 内容字段	C7.3.11	ServSel:M	是 □ N/A □	是 □ N/A □

D5.7 支持的算法

项目	问题/特征	引用条号	状态	支持
RegKTE	支持登记密钥令牌交换算法列表	—	O	名： 客体标识符：
UnRegKTE	支持未登记指数密钥交换算法列表	—	O	名：
RegICV	支持登记 ICV 算法名列表	—	O	名： 客体标识符：
UnRegICV	支持未登记 ICV 算法列表	—	O	名：
RegConf	支持登记保密性算法名列表	—	O	名： 客体标识符：
UnRegConf	支持未登记保密性算法列表	—	O	名：

D6 NLSP-CL 的特定特征

D6.1 主要能力(NLSP-CL)

项目	问题/特征	引用条号	状态	支持
CLConf*	支持无连接保密性?	5.2	CL:O.5	是 □ 否 □ N/A □
CLInteg*	支持无连接完整性?	5.2	CL:O.5	是 □ 否 □ N/A □
DOA	支持数据原发鉴别?	5.2	CL:O.5	是 □ 否 □ N/A □

D6.2 启动者/响应者(无连接方式)

项目	问题/特征	引用条号	状态	支持
CLXmtProt	该实现能发送保护的无连接数据单元?	7.6	CL:O.6	是 □ 否 □ N/A □

表（完）

项目	问题/特征	引用条号	状态	支持
CLRcvProt	该实现能接受保护的输入无连接数据单元？	7.7	CL：O.6	是 □ 否 □ N/A □
CLXmt	该实现能发送无保护的无连接数据单元？	7.6.1	NoProt：M	是 □ N/A □
CLRcv	该实现能接受无保护的输入无连接数据单元？	7.7.1	NoProt：M	是 □ N/A □

D6.3 环境(无连接方式)

项目	问题/特征	引用条号	状态	支持
CL1	支持 GB/T 15126 ADI 强制性元素？	5.2	CL：M	是 □ N/A □

D6.4 SDT PDU 字段(无连接方式)

项目	问题/特征	引用条号	状态	支持
SdtSA-ID	在每个 SDT PDU 中发送 SAID 字段？	13.3.2.4	CL：M	是 □ N/A □

D7 NLSP-CO 的特定特征

D7.1 主要能力(NLSP-CO)

项目	问题/特征	引用条号	状态	支持
SNAcP	该协议直接映射到 GB/T 16974	5.3， 附录 B	CO：O.7	是 □ 否 □
SNISP*	该协议映射到 GB/T 15126？	5.3， 附录 A	CO：O.7	是 □ 否 □
COConf*	支持连接保密性？	5.2	CO：O.8	是 □ 否 □ N/A □
COInteg*	支持无恢复连接完整性？	5.2	CO：O.8	是 □ 否 □ N/A □
PEA	支持对等实体鉴别？	5.2	CO：O.8	是 □ 否 □ N/A □
ExCSC*	支持 NLSP 中定义的 CSC PDU 规程的例子？	10	CO：0	是 □ 否 □ N/A □

D7.2 PDU(连接方式)

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
CSC*	连接安全控制 PDU	8.5, 13.5	CO:M	是 □ N/A □	是 □ N/A □

D7.3 连接方式的建立/释放

项目	问题/特征	引用条号	状态	主叫实体支持	被叫实体支持
UNConn	UN-CONNECT 中的 NLSP-CONNECT	8.5.1.2	CO:O.9	是 □ 否 □ N/A □	是 □ 否 □ N/A □
UNConnSAP	具有 SA-P 的 UN-CONNECT 中的 NLSP-CONNECT	8.5.1.2	CO:O.9	是 □ 否 □ N/A □	是 □ 否 □ N/A □
UNData	UN-DATA 中的 NLSP-CONNECT	8.5.1.2	CO:O.9	是 □ 否 □ N/A □	是 □ 否 □ N/A □
UNDataSAP	具有 SA-P 的 UN-DATA 中的 NLSP-CONNECT	8.5.1.2	CO:O.9	是 □ 否 □ N/A □	是 □ 否 □ N/A □
DUNDisc	UN-DISCONNECT 中的 NLSP-DISCONNECT	8.10	CO:O.10	是 □ 否 □ N/A □	是 □ 否 □ N/A □
DUNData	UN-DATA 中的 NLSP-DISCONNECT	8.10	CO:O.10	是 □ 否 □ N/A □	是 □ 否 □ N/A □

D7.4 环境(连接方式)

项目	问题/特征	引用条号	状态	支持
CO1	支持 GB/T 15126 的强制性元素?	5.3	SNISP:M	是 □ N/A □
CoNopt1	该实现提供加快数据?	8.7	CO:O	是 □ 否 □ N/A □
CoNopt3	该实现提供接收证实?	8.9	CO:O	是 □ 否 □ N/A □

D7.5 定时器和参数(连接方式)

项目	问题/特征	引用条号	状态	支持
T1	支持在发送 NLSP-DISCONNECT 和发出 UN-DISCONNECT 之间的定时器?	8.10	CO:O	是 □ 否 □ N/A □

D7.6 SDT PDU 字段(连接方式)

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
TestData	内容字段类型 C1——测试数据	13.3.4.3	O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
RAdrr	内容字段类型 C4——响应 NLSP 地址	13.3.4.3	ParamProt:M	是 □ N/A □	是 □ N/A □
ConfReq	内容字段类型 C8——证实请求	13.3.4.3	ParamProt:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
Reason	内容字段类型 C9——断开连接原因	13.3.4.3	ParamProt:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
注:D7.6 中所有项目都以所支持的 SDT 为条件。					

D7.7 CSC PDU 字段——通用(连接方式)

项目	问题/特征	引用条号	状态	发送时支持	接收时支持
CscPID	每个 CSC PDU 中 PID 字段的值为 10001011	13.5.1	CSC:M	是 □ N/A □	是 □ N/A □
CscLI	每个 CSC PDU 中长度指示符字段	13.5.2	CSC:M	是 □ N/A □	是 □ N/A □
CscPTyp	每个 CSC PDU 中 PDU 类型字段具有 xx111111 的值	13.5.3	CSC:M	是 □ N/A □	是 □ N/A □
UNC-UNDFlg	每个 CSC PDU 中发送 PDU 类型字段的 UNC-UND 标志?	13.5.3	CSC:M	是 □ N/A □	是 □ N/A □
SA-PFlg	每个 CSC PDU 中发送 PDU 类型字段的 SA-P 标志?	13.5.3c	CSC:M	是 □ N/A □	是 □ N/A □
CscSA-ID	SA-ID 字段	13.5.4	CSC:O	是 □ 否 □ N/A □	是 □ 否 □ N/A □
ContLen	每个 CSC PDU 中内容长度字段	13.5.5	CSC:M	是 □ N/A □	是 □ N/A □

D7.8 CSC PDU 内容举例(连接方式)

项目	问题/特征	引用条号	状态	支持
CscInit	实现能启动 **CSC PDU** 交换?	10.3	**ExCSC:O.1** 1	是 □ 否 □ **N/A** □
CscResp	实现能对对等实体启动的 **CSC PDU** 交换进行响应?	10.3	**ExCSC:O.1** 1	是 □ 否 □ **N/A** □
EncAuth	加密 **AUTH-DATA** 字段	13.5.7	**ExCSC:M**	是 □ **N/A** □
KeyInfox	密钥信息字段	13.5.8	**ExCSC:O**	是 □ 否 □ **N/A** □

附 录 E
(提示的附录)
NLSP 基本概念指导

E1 保护的基础

NLSP 用户数据的保护基础是安全数据传送 **PDU**(**SDT PDU**)或无报头保护。**SDT PDU** 通过添加完整性检验值(**ICV**)的封装功能来保护数据,然后为了保密性对该数据进行加密。填充字段可与被保护数据一同放置以支持通信流量保密性和块 **ICV** 机制。单独的填充字段为了块加密机制可置于块加密机制的 **ICV** 之后。

SDT PDU 中附加安全控制信息(例如标号,顺序号)受保护之前可与用户数据一起存放,以产生封装前八位位组串。然后使用上面描述的封装功能保护封装前八位位组串。在 **PDU** 的前部置有一个清除头,以标识 **PDU** 类型及"安全属性"集(密钥等等见第 5 章)用来保护数据单元。**SDT PDU** 的建构如图 **E1** 所示。

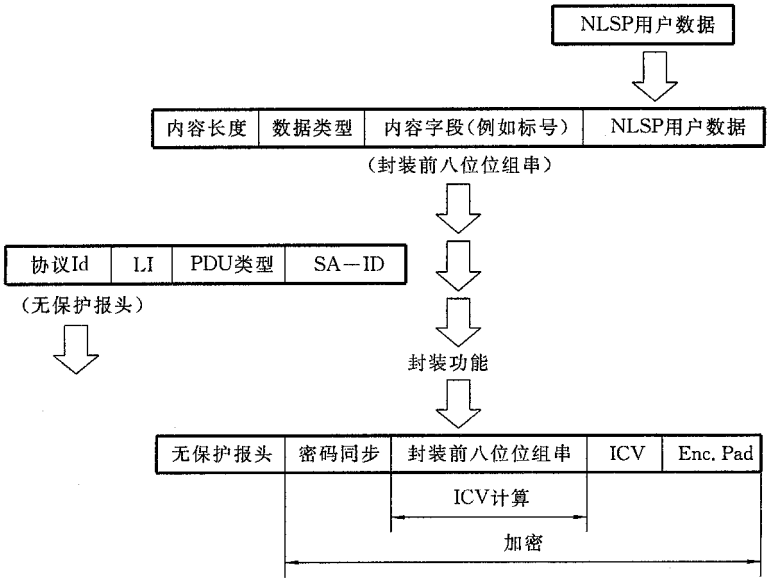


图 **E1** 建构安全数据传送 **PDU**

NLSP-CO 支持第二种任选的方法以保护称为 No _ Header 的 NLSP 用户数据。用这种方法对 NLSP数据可直接加密而不用附加任何安全控制信息或清除头。

E2 底层服务与 NLSP 服务

NLSP 有两个概念的服务接口，一个称为 NLSP 服务，是对“上面”“NLSP”的协议提供的接口(即利用被保护通信的协议)，另一个称为 UN(底层网)服务，是 NLSP 用来调用底层通信协议的。NLSP 可在不影响高于和低于 NLSP 协议的操作而透明地加入，NLSP 接口反映了上述协议期望的服务，而 UN 服务映射到底层协议提供的服务形式上。

NLSP 服务接口处的用户数据，在它下行传递到底层 UN 服务接口之前受到保护(例如将它封装在 SDT PDU 中)

除了在一个主要方面外，NLSP 和 UN 服务接口两者都与 OSI 网络服务相似。受 NLSP 服务的实体并不总是运输实体，并且 UN 服务从不直接与运输实体接口。如后面描述的，在某些情况下(见图 E2) NLSP 服务可接口到中间系统内的中继和路由选择功能或甚至接口到支持网络层协议的实体。使用 UN 服务时，从底层协议的角度看，服务接口可能就好象它是网络服务，但从整个 OSI 栈的观点看，它接口到网络层内的 NLSP 实体上，因此它不是一个纯 OSI 网络服务。

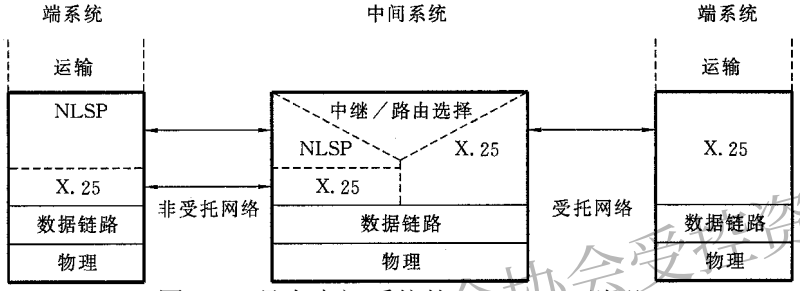
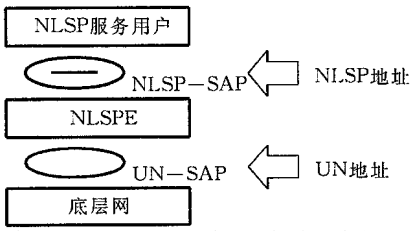


图 E2 具有中间系统的 NLSP-CO 说明

E3 NLSP 寻址

NLSP 实体(NLSPE)被嵌入在 NLSP 服务用户和底层网之间，相应的服务访问点为 NLSP-SAP 及 UN-SAP。在 NLSP 当前支持的配置中(见图 E3-1 及注)，标识连接到 NLSP-SAP 的实体地址(例如 NLSP 服务用户)是 NLSP 地址，标识连接到 UN-SAP 的实体地址(例如 NLSPE)是 UN 地址。对等 NLSPE 在网络层中形成一个子层。其上边界和下边界是交换地址的交互点。下图描绘了服务访问点及相应的地址。



注：在中继 CO 方式 N 服务的配置中，NLSP 地址可能标识端系统中的 NSAP 地址，而不是中间系统中的 NLSP-SAP(见图 E4 和图 E5)。

图 E3-1 高层和低层 SAP 及其地址

NLSP 位于网络层内部，它可置于下边界、上边界或中间任何地方。NLSP 及其较低的 UN 服务边界以不同角色进行动作，这取决于放置。类似地，所用的地址也根据放置而具有不同的语义。图 E3-2 显示了 NLSPE 在网络层中的可能放置。

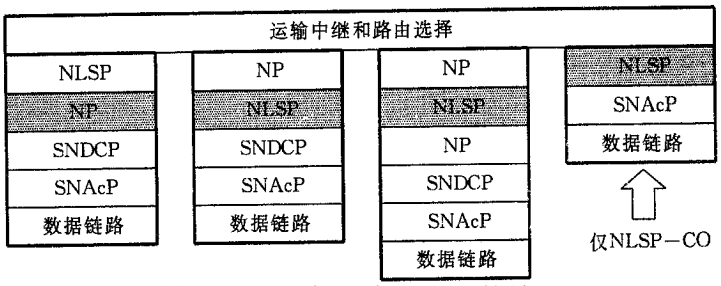


图 E3-2　网络层内 NLSP 的放置

图 E3-3 及图 E3-4 标识了不同放置中包含的 NLSP 子层的网络层内使用的地址形式。

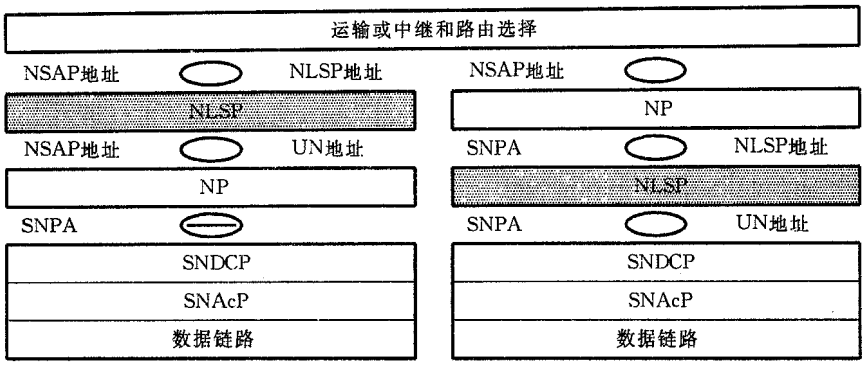


图 E3-3　包含 NLSP 子层的网络层中的地址——带有 NLSP 上面和下面的网络协议(NP)

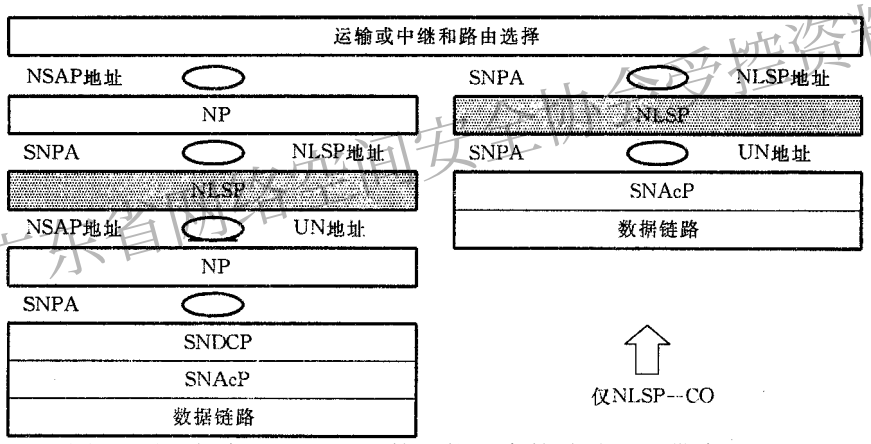


图 E3-4　包含 NLSP 子层的网络层中的地址——带有 NLSP 上面和下面的网络协议(NP)——没有网络协议

在网络协议(连接方式或无连接方式)位于 NLSP 子层之下的情况下,NLSP 使用 NSAP 地址(UN 地址)在底层网中寻址。NSAP 地址形成了由 NLSP 子层包围的被封装的寻址域。NSAP 地址同 NSAP 地址有相同的语法并且用 NSAP 地址登记规程来登记。形成一个受托网络域的 NSAP 地址仅仅用在由 NLSP 子层保护的域中。

SNPA 可能与上层 NP 实体确定的 SNPA 相同。然而,根据对等 NLSPE 的定位,SNPA 地址可能不同。

封装的寻址域可看作是 OSIE 中的虚拟子网,它由 ES 或 IS 中的一组 NLSP 实体定界,这些实体每一个都有相同的依赖于技术子网协议的 N-Layer 栈(SNACP,依赖于子网网络收敛协议),因此这些 NLSPE 在网络层内有相同的放置。

图 E3-5 显示了可能的 OSIE 的方案。该 OSIE 包含了 ES 和 IS 内的 NLSP 实体所包围成的虚拟

UN。

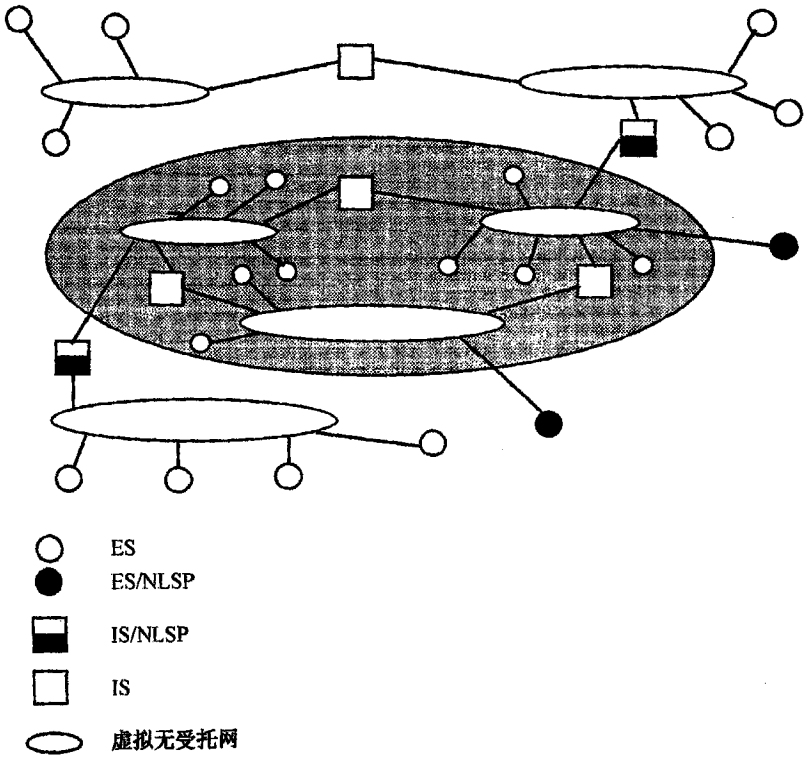


图 E3-5　OSIE 内的虚拟 UN

网络层协议栈和 NLSP 实体的放置取决于子层中使用的协议及其配置。选择处理由定义受托和无受托网络组合静态配置的“权限”完成，这要求在本标准的范围之外附加安全管理和路由选择功能。

取决于网络层内的 NLSPE 放置，NLSP 地址和 UN 地址有不同的语义。概念上，两种放置是不同的(见图 E3-6)。

——放置 A——对应于 OSI NSAP 的 NLSP _ SAP，NLSP 服务的用户是运输实体，标识运输实体的地址被定义为 NSAP 地址且与 NLSP 地址相同。

底层网被看作是无保护的网络域。它实际上是 OSI 网络。因此标识 NLSPE 的地址对应于 OSI NSAP 地址。然而，若 NLSP 服务参数被保护(Param _ Prot 为 True)，经由 NLSP _ SAP 和 UN _ SAP 边界在服务原语中传送的参数可能不同。

——放置 B——NLSPE 放置于两个网络子层之间。顶部的子层描绘了被保护的网络域，而底层子网代表无保护的网络域。

在端系统中，NSAP 地址标识了在端系统中配置的不同网络服务用户。NLSP 地址标识了端系统路由选择实体，该实体对 ES 路由选择功能负责。

在中间系统中，NSAP 地址包含了被保护的网络域中的中继 NPDU 的路由选择信息，NLSP 地址标识了 IS 中的 ES/IS 路由选择实体，UN 地址标识了连接到 UN 上的 NLSPE。

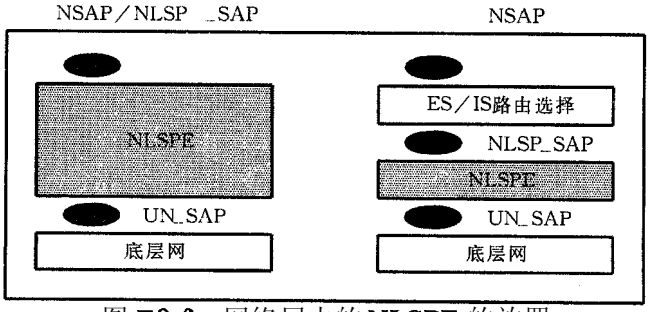


图 E3-6　网络层内的 NLSPE 的放置

由远程NLSPE服务的NLSP地址持有SA属性Adr _ Served。远程NLSPE的UN地址持有SA属性Peer _ Adr。

——若Param _ Prot为FALSE

NLSP功能局限于从NLSP-SAP到UN-SAP的服务原语的映射,NSAP地址直接映射成UN地址,NLSP SA属性Adr _ Served保持和SA属性Peer _ Adr相同的值。

——若Param _ Prot为TRUE

保护方式——地址映射取决于NLSPE放置并通过使用属性Adr _ Served和Peer _ Adr来提供。

表E1包括了取决于它们的不同放置的NLSPE的功能映射地址及Peer _ Adr和Adr _ Served属性之间的对应性。表E1仅覆盖了目的地址。

E4 连接方式NLSP

E4.1 基本操作

NLSP复杂性中的大部分与处理为连接方式通信的连接建立相关。

表E1

放置	Param _ Prot	NLSP地址	UN地址	NLSP地址与UN地址
A	FALSE	NSAP地址	NSAP地址	相同
A	TRUE	NSAP地址	对等UN地址	不同
B:端系统	FALSE	NLSP地址(注)	对等UN地址	相同
B:端系统	TRUE	NLSP地址(注)	对等UN地址	不同
B:中间系统	FALSE	NLSP地址(注)	对等UN地址	相同
B:中间系统	TRUE	NLSP地址(注)	对等UN地址	不同
注:从NLSP地址到NSAP地址或从NSAP地址到NLSP地址的映射是与高于NLSP的协议相关的路由选择功能所关注的。				

支持两种NLSP连接建立基本方式。在一种方式中,NLSP-CONNECT参数携带于UN-CONNECT服务原语中。在另一种方式中,NLSP-CONNECT参数被封装进SDT PDU之后,在建立了UN连接之后,携带于UN-DATA中。两种NLSP连接建立方式有不同的变种,一种变种用于带内SA-P,另一种用于带外建立的SA。

“连接安全控制”(CSC)PDU用来发出连接建立方式的信号。若在UN连接上不携带带内SA-P,CSC PDU交换也用于:

a) 建立机制特定的安全属性,以便用于保护连接(例如:密钥,完整性顺序号);

b) 执行对等实体鉴别。

在带有带内SA-P的UN-CONNECT中要携带NLSP-CONNECT的情况下,建立UN连接用来携带SA-P,然后在执行携带NLSP-CONNECT参数的UN-CONNECT交换之前,将该UN连接释放。第二次UN-CONNECT交换时,CSC PDU用于重新鉴别对等NLSP实体。

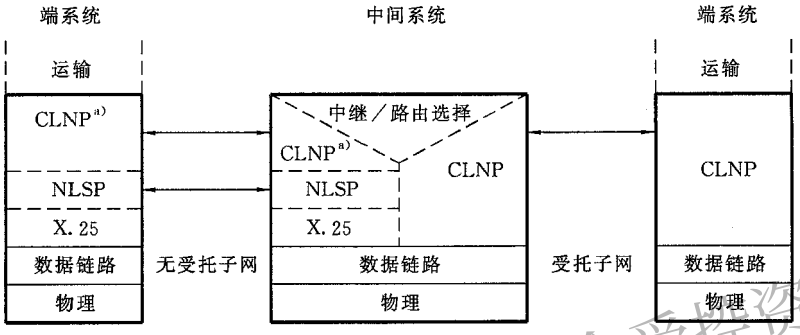
通过携带设置要求的SA属性所必须的信息的SA PDU或SDT PDU的交换来获得SA的建立。附录C为该目的定义了SA协议。

若要求保护 NLSP-CONNECT 参数，这些参数将被封装进 SDT PDU 中或在传送之前予以加密(选择无报头)。

一旦建立了连接，通过把用户数据封装进 SDT PDU 中来保护它，或者若选择了无报头方式，仅通过加密 NLSP 用户数据即可保护它。

E4.2 放置

连接方式 NLSP 可被放置在网络层中的不同位置。它对 NLSP 用户或者提供 OSI 网络服务接口(此时用户对应于运输实体)，或者若用户是附加网络协议实体(例如 GB/T 17179.1CLNP)，该服务对应于子网接口。NLSP 之下的接口实际上与 OSI 网络服务完全相同，除了服务用户是 NLSP 而不是运输服务外，该服务可在端系统操作或在中间系统操作。在 NLSP 之下操作的协议进行操作好象它曾在提供 OSI 网络服务的两个端系统之间进行操作。尽管全面地看，它仅可在中间系统上操作，不能直接与运输服务接口。带有中间系统和端到端的 NLSP-CO 操作在图 E4-1、E4-2、E4-3 和 E4-4 中说明。NLSP 的其他放置也有可能。



a) 这包括 CO 方式收敛功能。

图 E4-1 多网络环境中 NLSP 的说明

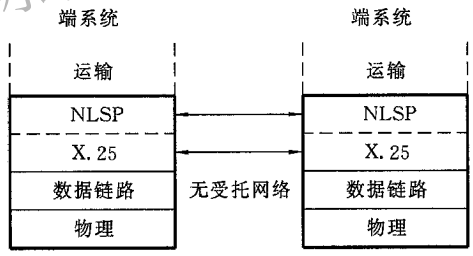


图 E4-2 端系统之间的 NLSP-CO 说明

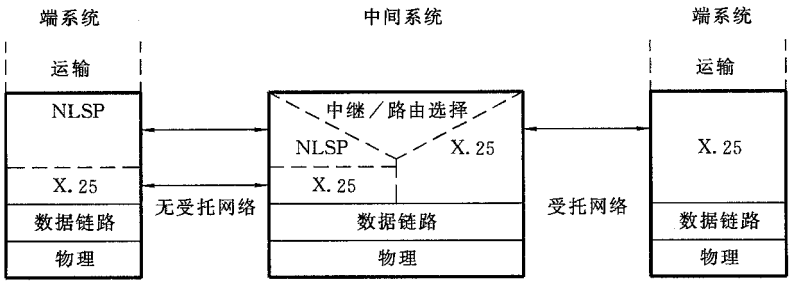


图 E4-3 无受托网络的 NLSP-CO

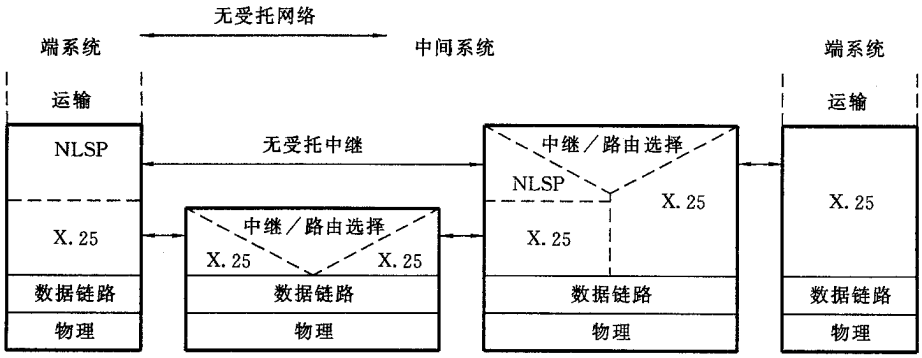


图 E4-4　无受托中继系统的 NLSP-CO 说明

E4.3　NLSP/UN 服务接口映射

在端系统中，NLSP 服务直接映射到 OSI 网络服务上。

支持两种 UN 服务映射，其一，UN 服务接口映射到等价的 OSI 网络服务上，其 CSC PDU 携带在 UN 连接用户数据字段中。其二，直接映射到如 GB/T 16976 定义的建议 X.25 上，除了 CSC PDU 携带在 X.25 保护设施字段外。

E4.4　寻址

若 NLSP 在网络层顶部操作，NLSP 服务接口用的地址是 OSI 网络服务 NSAP 地址；或者若 NLSP 在如 CLNP 的另一个网络层协议下操作，则是 SNAP 地址。若有地址隐藏（即 Param _ Prot 为 FALSE）则在 UN 服务接口的地址与NLSP服务接口上的地址相同。

若提供了地址隐藏（即 Param _ Prot 为 TRUE），则在 UN 服务接口（UN 地址）上用的地址与NLSP地址（例如 NLSP 地址为按照 GB/T 15126 构造的 NSAP 地址）有相同的形式。然而，它们用于标识可能位于中间系统或端系统的 NLSP 实体。这些 UN 地址可与 NSAP 地址相同的方式进行管理。相同的登记模式可用于分配地址，同样的路由选择协议可用于管理路由选择。但是，它们在隔离路由选择域中。从 NSAP 地址到 UN 地址的映射通过使用 Adr _ Served 安全联系属性的 NLSP 来处理，以便标识在 Peer _ Adr 安全联系属性中保持的 UN 地址服务的 NSAP 地址。

E5　无连接方式 NLSP

E5.1　基本操作

通过在 SDT PDU 中封装用户数据来简单地提供 NLSP-CL 的保护。

E5.2　放置

无连接方式的 NLSP 可在下列之一的情况下进行操作：

a）在网络层顶部，在被无连接网络协议（GB/T 17179.1）处理之前将 NSDU 封装在 SDT PDU 中（见图 E5-1）。该栈仅可用于两个端系统之间；

b）在无连接网络协议之下，在无连接协议 PDU 被映射到底层子网之前封装它们（见图 E5-2）。该栈可与“受托”中继中间系统一起使用或用于两通信系统之间没有网络中继的端对端系统；

c）在一个 GB/T 17179.1（CLNP）协议层之下对“受托”/“红”域进行操作以及对“无受托”/“黑”域映射到另一个 CLNP 协议层。该栈是最灵活的，可在任何环境下操作，在移去由 NLSP 提供的安全保护之后，“受托的”中间系统中继上层 CLNP 协议。其他“无受托的”中继系统在低层 CLNP 协议上进行中继，并透明地传递 NLSP 保护数据（见图 E5-3）。

注

1　两个 GB/T 17179.1 层和 NLSP 层的表示并不一定暗指独立的协议机制。这取决于本地实现策略。

2　两个 CLNP 协议层的存在并不一定暗指独立实现的存在。

E5.3　NLSP/UN 服务接口映射

NLSP 在网络层顶部操作的情况下，NLSP 服务接口与 OSI 网络服务相同，除了它与 NLSP 实体接口而不是运输服务之外，UN 服务接口也相同。

第二种情况，NLSP 在 CLNP 之下操作，NLSP 服务接口与 CLNP 之下操作的子网络提供的服务等价，UN 服务与子网络服务相同。

最后一种情况，NLSP 之上的接口在其上的 CLNP 协议看来好像它是一个子网，UN 接口对于其下的 CLNP 协议看来好像该接口是 OSI 网络服务。

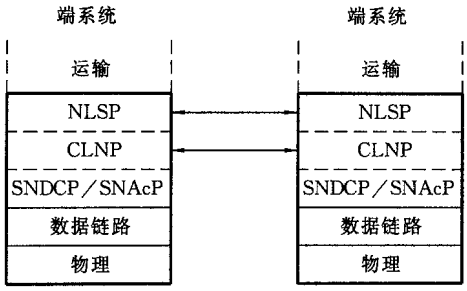


图 E5-1　端系统之间的 NLSP-CL 说明

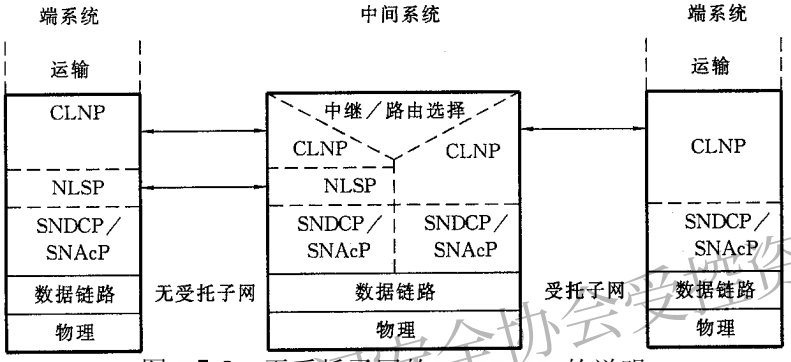


图 E5-2　无受托子网的 NLSP-CL 的说明

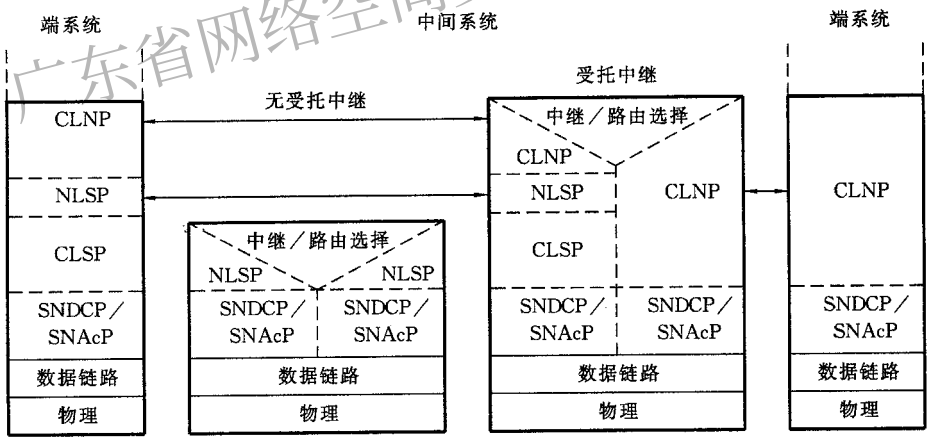


图 E5-3　无受托中继系统的 NLSP-CL 说明

E5.4　寻址

NLSP 在网络层顶部操作情况下，NLSP 使用的地址是 OSI 网络 NSAP 地址，NLSP 在映射到底层子网络之前，在 GB/T 17179.1(CLNP)下面操作情况下，NLSP 上面和下面接口使用的地址是一个子网地址(例如局域网 MAC 地址)，NLSP 在两个 CLNP 层之间操作的情况下，传递到 NLSP 实体的地址是子网地址。

若有地址隐藏(即 Param _ Prot 为 FALSE)，则在 UN 服务接口上的地址与 NLSP 服务接口上的地址相同。

若提供隐藏地址(即 Param _ Prot 为 TRUE)，UN 服务接口(UN 地址)使用的地址与 NLSP 地址

形式相同。然而它们用于标识可能位于中间或端系统的NLSP 实体。这些UN 地址可用NSAP 地址相同的方式管理。相同的登记模式可用于分配地址,相同的路由选择协议可用于管理路由选择。然而它们在隔离路由选择域中。从NSAP 地址到UN 地址到映射由NLSP 使用Adr _ Served 安全联系属性处理,标识在Peer _ Adr 安全联系属性中保持的UN 地址服务的NSAP 地址。

E5.5 分段

分段和重装由GB/T 17179.1(CLNP)处理。可在NLSP 处理之前或之后进行分段,取决于PDU 越过的底层子网,若分段在NLSP 之前进行,则每个段是所封装的NLSP,转发给NLSP 解封设备解封,然后被CLNP 重装。若分段在NLSP 之后进行,则CLNP 将首先重装各段,完整的PDU 将被NLSP 解封,然后CLNP 通过正常通信协议将解封了的PDU 交付给指明的目的地址。

E6 安全属性和联系

为了进行安全通信,NLSP-CO 和NLSP-CL 两者都需要相应属性集,称为安全联系属性,包括:

a) 与基本"策略"相关的信息,它定义或约束了NLSP 的操作。例如加密算法、加密块大小、完整性顺序号长度、标号定义权限;

b) 控制NLSP 操作所需的初始值,例如主密钥、初始完整性顺序号;

c) 控制NLSP 操作所需的当前值:特定的连接工作密钥、当前完整性顺序号。

相应属性汇集的存在称为安全联系,用于保护连接或无连接PDU 的属性集被安全联系标识符来引用。

第一个与"策略"相关的信息集称为"安全规则商定集"(ASSR),建议通过登记建立它。

第二个集合,初始控制信息集可使用本地管理接口或OSI 管理接口在带外建立,或使用与称为"安全联系建立协议"的NLSP 一起操作的协议在带内建立。

第三个信息集作为基本NLSP 协议的操作部分被更新。例如,工作密钥可通过连接安全控制PDU 的交换在NLSP-CO 中建立;当前完整性顺序号在每个安全数据运输PDU 时更新。

E7 NLSP 和CLNP 之间的动态功能关系

E7.1 导引

E5.2 描述了通信实例的NLSP 和CLNP 的关系,本章的目的是证明NLSP 与CLNP 一起使用以支持独立于通信体系结构的保护和无保护通信的灵活性。

图E7-1 描述了进出于这些组合协议的数据流。下列文本描述该数据流和它所需的通信参数。

E7.2 SU-UNITDATA Indication

a) 在SN-UNITDATA Indication(1)[GB/T 17179.1(CLNP)(见5.5)]上检验第一个八位位组中的协议标识符(PID)(或是否用寻址来识别协议地址)以标识PDU 的第一部分是否包括CLNP 或NLSP 报头(2);

b) 若第一个报头标识了CLNP,则基于CLNP 报头(3)中的目的地址做出判定。若目的地址被认作该系统自身端系统地址之一,则CLNP PDU 被发送到重装进程(4)[CLNP(见6.8)],若它不是端系统地址之一,则CLNP 报头按E6.4 所述的转递处理(8);

c) 若第一个报头标识了NLSP,则子网服务参数和用户数据由NLSP 作为UN-UNITDATA 处理,然后检验结果NLSP-UNITDATA 用户指示,看第一个八位位组是否为CLNP PID(8),若是,NLSP-UNITDATA 如上面b)处理(3),否则,NLSP-UNITDATA Indication 映射到N-UNITDATA Indication(7);

d) 在CLNP 重装之后(若需要)(4),则需要另一个判定(5)。若CLNP PDU 包含NLSP PDU(即第一个八位位组包含NLSP PID)则CLNP 服务参数和用户数据由NLSP 作为UN-UNITDATA Indication 处理(6),否则将它直接映射到N-UNITDATA Indication(7)。然后,检验结果NLSP-

UNITDATA 用户指示，看第一个八位位组是否为 CLNP PID(8)(或是否用寻址来识别检验协议地址)，若是，NLSP-UNITDATA 如上面 b)处理(3)，否则 NLSP-UNITDATA Indication 映射到 N-UNITDATA Indication(7)。

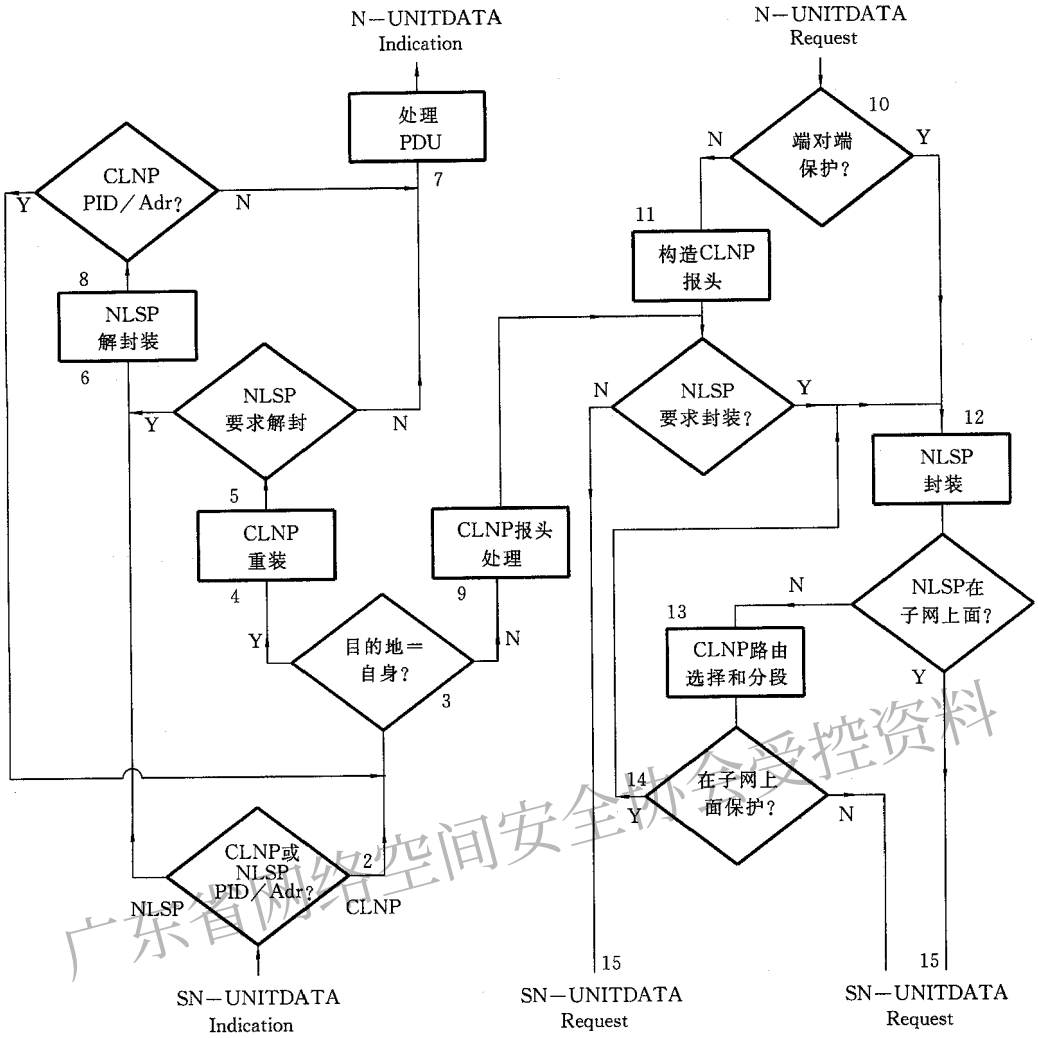


图 E7-1 CLNP 与 NLSP 的流程图

E7.3 N-UNITDATA Request

a) 在 N-UNITDATA Request(10)上，取决于服务参数(例如源和目的地址)及本地安全策略，请求或者直接映射到 CLNP(见 5.4)(11)上或者映射到 NLSP-UNITDATA Request 并进行相应的处理(12)；

b) 若 N-UNITDATA 被 CLNP 处理(11)，结果 CLNP PDU 或者直接映射到 SN-UNITDATA Request 上(15)或者映射到 NLSP-UNITDATA Request(10)以便由 NLSP 处理；

c) 若 N-UNITDATA 或者 CLNP PDU 被 NLSP 处理(12)，结果 UN-UNITDATA Request 或者直接映射到 SN-UNITDATA Request(15)，或者映射到 CLNP，好象它是 N-UNITDATA(13)一样处理，这取决于服务参数和本地安全策略。紧接 CLNP 处理之后，若要求子网之上的附加保护(14)，可能提供进一步的 NLSP 保护。否则 CLNP PDU 被映射到 SN-UNITDATA。

E7.4 CLNP PDU 的转发

保护转发的 CLNP PDU 的判定是基于 CLNP PDU 报头和用户数据中的信息以及本地安全策略。若要求保护，CLNP PDU 被映射到 NLSP-UNITDATA Request 以便由 NLSP 处理(12)，取决于服务参数和本地安全策略要求，结果保护的 UN-UNITDATA 或者直接映射到 SN-UNITDATA Request [CLNP(见 6.5)](15)或者映射到 CLNP，以便好象是 N-UNITDATA 一样处理(13)，这取决于服务参

数和本地安全策略要求。

E7.5 CLNP NLSP-CL 接口摘要说明

前面说明了**NLSP-CL** 和**CLNP** 之间的功能关系。为简单起见，这些协议的操作由服务接口显示为明显的分离，两个协议的操作可以按单层 3 协议组合的**CLNP** 和**NLSP** 协议机制功能性来实现。

E8 与分层模型相关的动态功能性

描述**NLSP** 的分层方法与流程图相关，以图 **E7-2** 给出的配置举例说明。

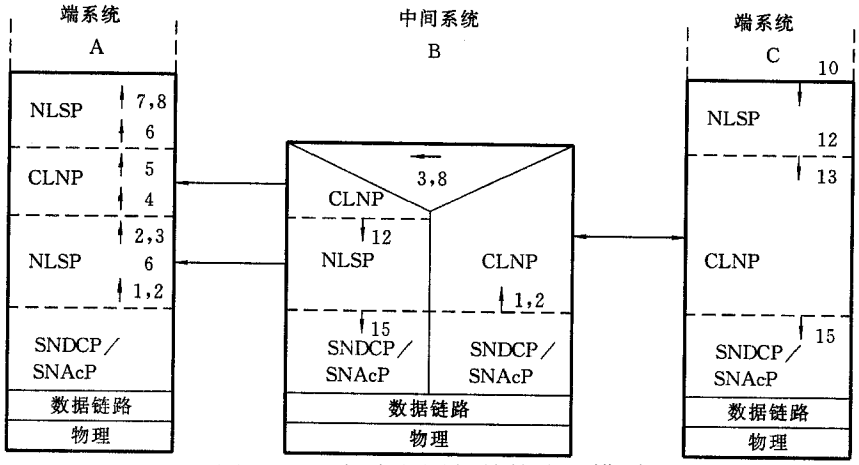


图 **E7-2** 与流程图相关的分层模型

动 作	流程图引用编号
在端系统 **A** 中	
SN-UNITDATA Indication 在端系统 **C** 中	1
若 **CLNP** 或 **NLSP** 检验	2
若目的地是本地检验	3
CLNP 重装	4
若 **NLSP** 检验	5
映射到 **UN-UNITDATA** 和 **NLSP** 解封上	6
映射到 **N-UNITDATA Indication**	7
若 **CLNP** 检验	8
在中间系统 **B** 中	
SN-UNITDATA Indication 在中间系统 **B** 中	1
若 **CLNP** 或 **NLSP** 检验	2
若目的地是本地检验	3
处理 **CLNP** 转发	8
映射到 **NLSP-UNITDATA** 和 **NLSP** 封装上	12
映射 **UN-UNITDATA** 到 **SN-UNITDATA Request** 上	15
在端系统 **C** 中	
N-UNITDATA Request 在端系统 **A** 中	10
映射到 **NLSP-UNITDATA** 和 **NLSP** 封装上	12
映射 **UN-UNITDATA** 到如 **N-UNITDATA** 处理的 **CLNP** 上	13
映射 **CLNP** 到 **SN-UNITDATA Request**	15

附 录 F
（提示的附录）
安全规则商定集的例

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操作所必需的所有参数。本附录的例说明可能由 ASSR 建立的 SA 属性的值是如何按形式表写出的。

ASSR-ID　　XYZ(客体标识符)　　--给出 SA-P 中使用的客体引用
SA-ID _ Length　　4
选择的安全服务定义方式　　-- 指明可能在安全规则下支持的安全服务，并给出使用不同算法、密钥长度等支持的保护级别名。

PE Auth：无，低，高
AC：　　无，低，高
Confid：　无，低，高
Integ：　无，低，高

安全标号映射　　--把服务标号映射到安全服务选择。
Label _ Def _ Auth　　XYZ
Label-Sensitivity＝无级
暗指：
PE Auth 无，AC 无，Confid 无，Integ 无
Label-Sensitivity＝机密的
暗指：
PE Auth 低，AC 低，Confid 低，Integ 无
Label-Sensitivity＝秘密
暗指：
PE Auth 高，AC 高，Confid 高，Integ 高

Param _ Prot　　TRUE　　--选择了要求保护所有服务参数的保护级别。

选择的安全服务：Integ＝高或 Conf＝高
机制模块——访问控制的安全标号
选择的安全服务：AC＝高或 Conf＝高
--指明安全服务选择要求安全标号。

Label _ Def _ Auth　　XYZ
(注意这必须如保护 QOS 标号 Auth 一样)
明确指示　是
机制模块——完整性检验值
选择的安全服务：Integ＞无或 PE Auth＝高或机制安全标号
ICV _ Alg　　XYZ
重密钥后　　10000PDUs
密钥分配机制　　非对称

机制模块——完整性顺序号

选择的安全服务：Integ＝高或 Auth＝高

ISN _ Len　　总计 8 个八位位组

顺序号　　4 个八位位组

增加 1

时间戳　　4 个八位位组

来自同步点的毫秒

收到 ISN 窗口丢弃以前的顺序号

时间戳应在 2 * maximum 内

在网络内变更

若在外边，延迟

然后窗口重演攻击。

机制模块——封装

选择的安全服务：　Conf＞低

Enc _ Alg _ ID　　XYZ

方式　　链式

Enc _ Blk　　8 个八位位组

密钥交换信息　　（例如，素数 P，生成器 a）

重密钥后　　1000 PDU

密钥分配机制　　非对称

机制模块——无报头

选择的安全服务：　Conf＝低和 Integ＝无和非标号机制

机制模块——连接鉴别

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

机制封装或完整性检验值

Enc _ Alg　　RSA

附　录　G
（提示的附录）
安全联系和属性

为了保护通信实例（无连接或连接 SDU），必须在通信实体之间建立信息汇集（控制安全操作所必需的密钥和其他属性）。该信息汇集就是安全联系（SA）。

形成 SA 的信息或者是静态信息，当建立 SA 时，它可被“定做”，然后在联系期间保护固定；或者是动态信息，可在安全联系生命期内更新。

SA 可以在带外建立，或者对 NLSP-CO，由 SA PDU 的交换在带内建立。当使用带内方法时，实现 SA-P 的特定的机制可以是如本标准定义的机制或者可以是专用机制的。

在建立 SA 之前，每个 NLSP 实体须预先建立：

a）公共安全规则集。给定了所选择的安全服务，规定要使用的安全机制，包括定义机制操作所需的所有参数（例如算法、密钥长度、密钥生命期）。这些安全规则通过通信实体相互商定并唯一地被标识，安全规则及其标识符可由第三方登记，安全规则集的例子见附录 F。

b) 安全服务及因此可能使用的安全机制。

若要使用带内方法建立SA，则下列须预先建立：

c)初始选择的安全服务及因此在建立SA 时要使用的安全机制。

d) 建立SA 所需的基本密钥信息。

在SA 建立时，NLSP 实体建立下列与其远程对等实体共享的信息：

e) 本地和远程SA-ID。

f) 通信实例联系的实体之间使用的安全服务。

g) 安全服务选择所暗指的机制及其参数。

h) 通信实例的完整性、加密机制和鉴别用的初始共享密钥。

i) 在该联系上为访问控制而可能使用的地址及安全标号集。

SA 引用及共享密钥[上述e)，h)]必须建立在每个联系基础上，其他信息可预先建立且对几个联系是公共的，另外，作为建立定做SA 的一部分，必须鉴别远程对等实体的识别，附录C 定义了一个机制，可用于密钥分配和鉴别。

通信实例可动态地更新下列信息：

j) 每个方向的正常和加快数据所需要的完整性顺序号。

k) 安全标号。

l) 加密/完整性机制的重密钥信息。

为获得鉴别，需要在每个通信实例上应用鉴别机制。

表G1 说明可在安全联系的不同阶段建立的不同的SA 属性。

表G1　三层安全联系的说明

预先建立	静　态	动　态
安全服务选择的范围 初始选择的安全服务 基本密钥信息 安全规则商定集	初始密钥 SA-ID 鉴别 安全标号	ISN 鉴别 SA-ID 重密钥信息
选择的安全服务 选择的机制 安全标号集/地址集		

附　录　H
（提示的附录）
密钥令牌交换——EKE 算法的例

下面是密钥令牌交换算法的一个例子，它可与附录C 中定义的安全联系协议一同使用。

EKE 要求两个参数。一个是大素数P(如此P－1 有一个大素数因子)，另一个数“a”，其范围是1＜a＜P－1。

设A 和B 是两个通信部分(见图H1)。EKE 开始时，A 选择一个大随机数X，B 选择一个大随机数Y，然后A 计算(a＊＊X mod P)，且将a，P 及(a＊＊X mod P)发送给B，B 计算(a＊＊Y mod P)并将它发送给A，A 和B 都计算(a＊＊XY mod P)。窃听者只看到(a＊＊X mod P)和(a＊＊Y mod P)而不能知道X 和Y，因此无法计算(a＊＊XY mod P)。

A 和B 随后将(a＊＊XY mod P)中位的子集用作密钥并在第二交换上用作防止重演攻击的信息。

际录C 定义的SA 协议中描述的值是：

——共享 KTE 位串为(a * *XY mod P)；

——Key-Token-1 为 a、P、(a * *X mod P)，其中“a”，“P”及(a * *X mod P)编码为并置的八位位组串；

——Key-Token-2 为(a * *X mod P)；

——Key-Token-3 为来自防止重演攻击的共享 KTE 位串(a * *XY mod P)派生的信息；

——Key-Token-4 为来自防止重演攻击的共享 KTE 位串(a * *XY mod P)派生的信息。

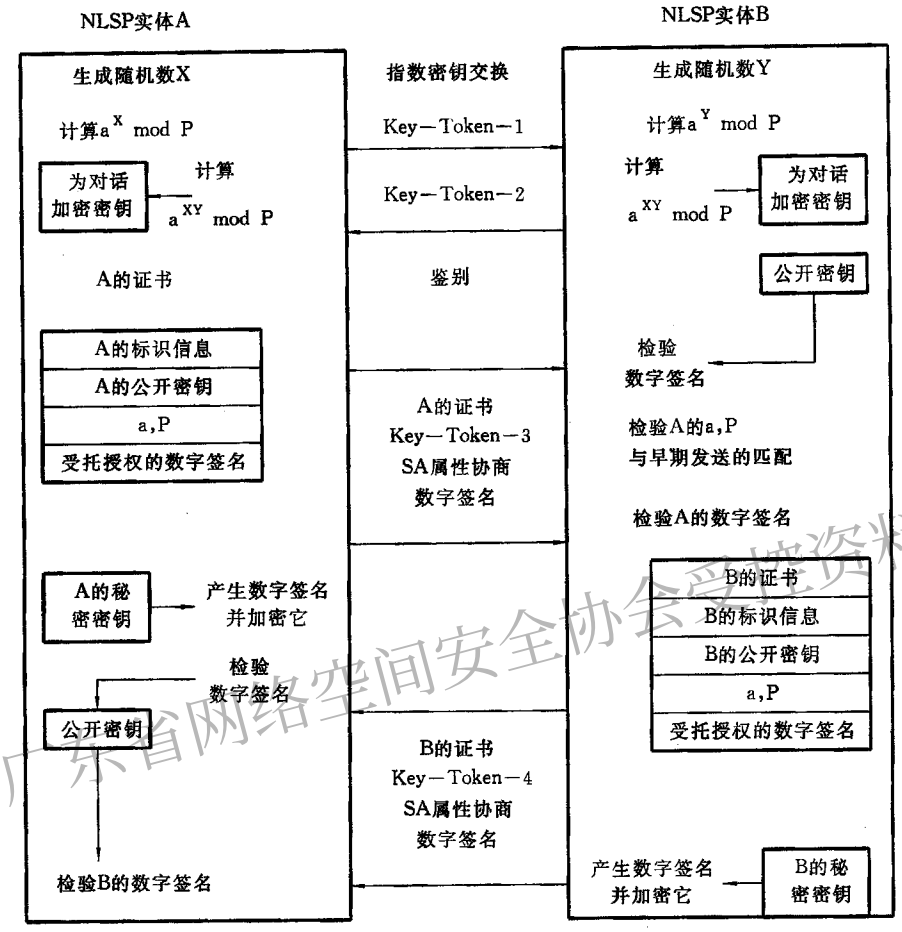


图 H1　联机密钥推导和使用 EKE 推导的说明