INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.802

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(04/95)

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

SECURITY

INFORMATION TECHNOLOGY – LOWER LAYERS SECURITY MODEL

ITU-T Recommendation X.802

(Previously “CCITT Recommendation”)

Foreword

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. Some 179 member countries, 84 telecom operating entities, 145 scientific and industrial organizations and 38 international organizations participate in ITU-T which is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the Members of ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, 1993). In addition, the World Telecommunication Standardization Conference (WTSC), which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of ITU-T Recommendation X.802 was approved on 10th of April 1995. The identical text is also published as ISO/IEC International Standard 13594.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

(February 1994)

ORGANIZATION OF X-SERIES RECOMMENDATIONS

Subject area	Recommendation Series
PUBLIC DATA NETWORKS	
Services and Facilities	X.1-X.19
Interfaces	X.20-X.49
Transmission, Signalling and Switching	X.50-X.89
Network Aspects	X.90-X.149
Maintenance	X.150-X.179
Administrative Arrangements	X.180-X.199
OPEN SYSTEMS INTERCONNECTION	
Model and Notation	X.200-X.209
Service Definitions	X.210-X.219
Connection-mode Protocol Specifications	X.220-X.229
Connectionless-mode Protocol Specifications	X.230-X.239
PICS Proformas	X.240-X.259
Protocol Identification	X.260-X.269
Security Protocols	X.270-X.279
Layer Managed Objects	X.280-X.289
Conformance Testing	X.290-X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300-X.349
Mobile Data Transmission Systems	X.350-X.369
Management	X.370-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600-X.649
Naming, Addressing and Registration	X.650-X.679
Abstract Syntax Notation One (ASN.1)	X.680-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850-X.859
Transaction Processing	X.860-X.879
Remote Operations	X.880-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999

CONTENTS

Page

Summary

This Recommendation | International Standard describes the cross layer aspects of the revision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link, Physical). It describes the architectural concepts common to these layers, the basis for interactions relating to security between layers and the placement of security protocols in the lower layers.

TECHNICAL REPORT

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – LOWER LAYERS SECURITY MODEL

1 Scope

This Recommendation | Technical Report describes the cross layer aspects of the provision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link and Physical layers).

This Recommendation | Technical Report describes:

a) architectural concepts common to the lower layers based on those defined in CCITT Rec. X.800 | ISO 7498-2;

b) the basis for interactions relating to security between protocols in the lower layers;

c) the basis for any interactions relating to security between the lower layers and upper layers of OSI;

d) the placement of security protocols in relation to other lower layer security protocols and the relative role of such placements.

There should be no conflict between the security protocols for the lower layers and the model described in this Recommendation | Technical Report.

CCITT Rec. X.500 | ISO/IEC 9594-1 identifies the security services relevant to each of the lower layers of the OSI Reference Model.

2 References

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | Technical Report. At time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | Technical Report are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.

– ITU-T Recommendation X.233 (1993) | ISO/IEC 8473-1:1994, *Information technology – Protocol for providing the OSI connectionless-mode Network service: Protocol specification*.

– ITU-T Recommendation X.234 (1994) | ISO/IEC 8602:1995, *Information technology – Protocol for providing the OSI connectionless-mode Transport service*.

– ITU-T Recommendation X.273 (1994) | ISO/IEC 11577:1995, *Information technology – Open Systems Interconnection – Network layer security protocol*.

– ITU-T Recommendation X.274 (1994) | ISO/IEC 10736:1995, *Information technology – Open Systems Interconnection – Transport layer security protocol*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

- ITU-T Recommendation X.810[1] | ISO/IEC 10181-1...[1], *Information technology – Open Systems Interconnection – Security frameworks in open systems: Security frameworks overview*.
- ITU-T Recommendation X.812[1] | ISO/IEC 10181-3...[1], *Information technology – Open Systems Interconnection – Security frameworks in open systems: Access control framework*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.
- ITU-T Recommendation X.224 (1993), *Protocol for providing the OSI connection-mode transport service*.

  ISO/IEC 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode Transport service*.
- CCITT Recommendation X.208 (1988), *Specification of Abstract Syntax Notation One (ASN.1)*.

  ISO/IEC 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*.
- CCITT Recommendation X.209 (1988), *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.

  ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.

2.3 Additional references

- ISO/IEC 8208:1995, *Information technology – Data communications – X.25 Packet Layer Protocol For Data Terminal Equipment*.
- ITU-T Recommendation X.25 (1993), *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in packet mode and connected to public data networks by dedicated circuits*.
- ISO 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer*.
- ISO 9542:1988[2], *Information processing systems – Telecommunications and information exchange between systems – End system to intermediate system routeing exchange protocol for use in conjunction with the Protocol routeing for providing the connectionless-mode network service (ISO 8473)*.
- ISO/IEC 10589:1992, *Information technology – Telecommunications and information exchange between systems – Intermediate system to intermediate system intra-domain-routeing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network service (ISO 8473).*
- ISO/IEC 10747:1994, *Information technology – Telecommunications and information exchange between systems – Protocol for exchange of inter-domain routeing information among intermediate systems to support forwarding of ISO 8473 PDUs*.

3 Definitions

3.1 OSI Reference Model definitions

This Recommendation | Technical Report makes use of the following terms as defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- Quality of Service

---

1) Presently at the stage of draft.

2) Currently under revision.

3.2 Open System Security Frameworks definitions

This Recommendation | Technical Report makes use of the following terms as defined in ITU-T Rec. X.810 | ISO/IEC 10181-1:

– security domain

3.3 Internal Organization of the Network Layer definitions

This Recommendation | Technical Report makes use of the following terms as defined in ISO 8648:

a) subnetwork access protocol;

b) end system;

c) intermediate system.

3.4 Additional definitions

For the purposes of this Recommendation | Technical Report, the following definitions apply:

3.4.1 reflection protection: A protection mechanism to detect when a protocol data unit has been sent back to the originator.

3.4.2 security association attributes: The collection of information required to control the security of communications between an entity and its remote peer(s).

3.4.3 security association: The relationship between lower layer communicating entities for which there exists corresponding security association attributes.

3.4.4 security rules: Local information which, given the security services selected specify the underlying security mechanisms to be employed, including all parameters needed for the operation of the mechanism.

NOTE – Security rules are a form of secure interaction rules as defined in the Upper Layers Security Model (ITU-T Rec. X.803 | ISO/IEC 10745).

4 Abbreviations

ISN	Integrity Sequence Number
SSAA	Set of SA-Attributes
NLSP	Network Layer Security Protocol
NLSP-CO	NLSP Connection mode
NLSP-CL	NLSP Connectionless mode
QOS	Quality of Service (as defined in CCITT Rec. X.200 | ISO/IEC 7498-1)
SA	Security Association
SA-ID	Security Association Identifier
SNAcP	Subnetwork Access Protocol (as defined in ISO 8648)
SNISP	Subnetwork Independent Security Protocol
TLSP	Transport Layer Security Protocol

5 Security associations

5.1 General overview

5.1.1 Any security protocol makes use of a number of security mechanisms to provide security services to the layer above. The security services required by the higher layer may be indicated to the lower layers through use of local security management functions. The security protocol and each of its security mechanisms require information, in addition to that which is encoded in the PDUs, to enable secure communication. Examples of such additional

information are the specification of the mechanisms to be used by the protocol and, for each mechanism, specific information such as the key required by an encipherment mechanism. Each piece of additional information is known as a Security Association Attribute.

5.1.2 Security Association Attributes may be placed in a protocol entity using a number of mechanisms. Some examples of placement mechanisms are:

a) placement during manufacture of a device;

b) placement during initialisation of a device;

c) placement via a manual interface, e.g. front panel controls;

d) placement by OSI Systems Security Management;

e) placement by OSI Layer Security Management;

f) placement by OSI Operations Security Management.

5.1.3 SA-Attributes may be placed at any time prior to the communication to which they relate. When compatible Sets of SA-Attributes (SSAA) are in place in each protocol entity, a Security Association is said to exist between the protocol entities.

5.1.4 SSAAs (and Security Associations) may exist with different granularity. Sometimes it is useful to be able to refer to SSAAs with different granularity. For instance, the SSAA defined by an Agreed Set of Security Rules (ASSR) could be denoted by SSAA ASSR. Or a pairwise key may be established between two protocol entities for use over a number of instances of common Source-Destination Address Pair. Similarly the SSAA for an instance of communication could be referred to by SSAA-Instance of Communication. Likewise the SSAA for a connection oriented PDU could be referred to by SSAA CO PDU.

5.1.5 In general, SA-Attributes must be placed in the Protocol Entity by secure means in order to maintain security. This implies that the SA-Attributes are either placed using a physically secure means or they may be placed making use of an existing Security Association which has been pre-placed for this purpose.

5.1.6 The SSAA which are part of a security association are often referred to by an identifier which has local significance and is known as an SA-ID. At any instant, some members of the Set of SA-Attributes may be undefined. Typically during the initialisation of a secure communication, the SSAA will not be fully populated and the initial exchanges will be used to completely populate the SSAA before user data is exchanged.

5.1.7 In order to provide Replay Protection, constraints must be applied to the use of SA-IDs, their referenced SSAAs and SA-Attributes.

a) SA-IDs may not be re-used with the same encipherment key.

b) After any SA-Attribute has been populated in a SSAA which is referred to by an SA-ID, that SA-Attribute may never be changed unless the security protocol has a means for signalling the change between the communicating entities. This implies that to enable key roll-over a new SA-ID must be used with copies of the old SA-Attributes and a new key unless the security protocol has an alternative means of signalling the key change (e.g. as supported by NLSP-CO CSC PDU).

5.1.8 Removal of any SA-Attribute from the SSAA effectively closes the Security Association

5.1.9 Some SA-Attributes have significance for an instance of communication (a connectionless PDU or a connection). Other SA-Attributes have significance for a single PDU on a connection. Examples of such SA-Attributes are Integrity Sequence Numbers and Security Labels. It may appear that the changing of these SA-Attributes violates the constraint in b) in 5.1.7 above. However, logically the Security Association, including these SA-Attributes, is only valid for the lifetime of a single PDU. The ISN acts as a logical extension to the SA-ID, hence changing the effective SA-ID. The label is only valid for this instance of the extended SA-ID. Thus, the constraints are maintained. Such SA-Attributes are sometimes termed ‘Dynamic’ SA-Attributes.

5.1.10 Part of a security policy will constrain the operation of the protocol entity. This part of the security policy is termed the Set of Security Rules for the Protocol Entity. The Set of Security Rules for a protocol entity may constrain such things as the security mechanisms to be used and the values and placement mechanisms for the SA-Attributes. The Set of Security Rules will also define the mapping of the security services selected into Security mechanisms used by the Security Protocol. The Set of Security Rules is a form of Secure Interaction Rules.

5.1.11 When used for operation within or between domains, a unique identifier for such Sets of Security Rules needs to be established and is known as an Agreed Set of Security Rules. The ASSR identifier may be exchanged as part of Security Association establishment to define or constrain the SSAA ASSR which are defined in that Set of Security Rules. The remaining SA-Attributes, if any, must be established using other means such as those listed in 5.1.2 above.

5.2 Establishing a security association for the lower layers

5.2.1 In order to protect an instance of communication (a connectionless SDU or a connection) a security association has to be established between the communicating entities.

5.2.2 The information forming an SA is either static information, which may be "negotiated" when the SA is established and then remains fixed for the duration of the association, or dynamic information which may be updated in an instance of communication.

5.2.3 An SA may be established as a OSI layer 1 to 4 protocol through the exchange of security association protocol data units (PDUs), or through mechanisms outside the scope of the lower layers of OSI.

5.2.4 Prior to establishing an SA each entity must have pre-established a common, mutually agreed and uniquely identified, set of security rules as well as the security services that may be selected.

5.2.5 If the SA is to be established through the exchange of security association PDUs, then the following must also be pre-established:

a) An initial selection of security services, and hence the security mechanisms, to be applied in establishing an SA.

b) Basic keying information needed to establish an SA.

5.2.6 On SA establishment, an entity establishes the following shared information with its remote peer which must remain unchanged (i.e. static) for the lifetime of the association:

a) Local and remote SA-IDs.

b) The Security Services Selected for use between the associated entities for instances of communication.

NOTE – The security services to be used may be selected among the pre-established security services.

c) The mechanisms and their properties to be used as implied through the Security Services Selected.

d) Initial shared keys for integrity, encipherment mechanisms and authentication of an instance of communication;

e) The set of security labels and addresses that may be used on this association for access control.

5.2.7 The SA-IDs and shared keys [items a) and d) above] must be established on a per association basis. The other information may be pre-established. In addition, as part of establishing a SA the identity of the remote peer must be authenticated to provide peer entity authentication.

5.2.8 The following information can be dynamically updated for an instance of communication:

a) Integrity sequence number(s) as needed for normal and expedited data in each direction.

b) A security label which is selected dynamically from the static set of security labels.

c) Re-key information for the encipherment/integrity mechanisms in security protocols supporting re-keying within an association (e.g. the connection-mode Network Layer Security Protocol).

5.2.9 To achieve peer entity or data origin authentication, authentication mechanisms need to be applied to each instance of communication.

5.2.10 The different SA-Attributes that may be established at the different stages of a security association are shown diagrammatically as in Figure 1. The terms pre-established, static and dynamic are used in relation to a security association as described in the preceding subclauses. The terms used and the form of authentication are as described in the preceding subclauses.

Pre-established	Static	Dynamic
Agreed Set of Security Rules Possible Security Services Initial Security Services Basic key information	SA-IDs Initial Keys Authentication	ISN Security Label Re-key information Authentication
Selected level of Protection QOS Selected mechanism Security label / Address set		

Figure 1 – Illustration of Attributes of a Security Association

5.2.11 An entity should identify necessary SA-Attributes using the SA-ID.

5.2.12 The SA shall be established prior to protecting an instance of communication.

5.3 Security association close

An SA indicated by an SA-ID is closed when the SA is no longer valid.

A security association can be closed by the following methods:

a) as a OSI layer 1 to 4 protocol through the exchange of security association protocol data units (PDUs);

b) using external mechanisms outside the scope of the lower layers of OSI;

c) implicitly by closing a connection (this is applicable only to connection mode);

d) implicitly when a key within the SA expires.

NOTE – Care should be taken in using this approach d) with the lifetime of a key defined by the number of packets sent/received between peer entities since significantly different values may result in each peer.

Before using method c) above, an attribute of the security association must indicate that the association is to be closed on closing a connection using that association.

5.4 Modification of attributes in a connection

For each instance of communication (a connectionless PDU or a connection), only one SA can be established.

During the existence of a connection the security services and mechanisms used on that connection cannot be modified (note this does not preclude changing keys).

Indication of use of new keys shall be described by the security protocol.

6 Influence on existing protocols

6.1 General principle

In principle the influence of security protocols on existing protocols should be minimal.

6.2 Connectionless SDU size

During data transfer, depending on the security mechanisms selected, security has the following impact on the (N)-layer protocol:

a) the (N)-user-data, and in some cases parts of the (N)-protocol-control-information, is operated on by cryptographic transformations before and after transmission. This may change the length of the (N)-user-data.

b) protocol control information related to (N)-user-data (e.g. security association identifier, cryptographic check code) may need to be carried by the (N)-protocol.

NOTE – This will have impact on the maximum User Data size as defined in CCITT Rec. X.213 | ISO/IEC 8348, subclause 15.2.3 and CCITT Rec. X.214 | ISO/IEC 8072.

6.3 Concatenation of PDUs

Only PDUs which are to be protected under the same security association may be concatenated.

6.4 Algorithm and mechanism independence

Lower layer security protocols are specified to be independent of the algorithm. Furthermore, NLSP has taken the approach of separating mechanism dependent and mechanism independent parts of the security protocol. It is anticipated that future lower layer security protocols may achieve this using generic abstract services for security common to the upper and lower layers of OSI.

7 Common security PDU structure

7.1 A common general PDU structure is to be used for protected data PDUs in the lower layer security protocols. Although the general PDU structure is the same for all lower layer security protocols they are not, of course, identical for a variety of reasons, the most obvious of which is the format restrictions imposed by a particular protocol layer.

7.2 Common aspects of the PDU structures in the lower layer security protocols may be:

a) an Integrity Check Value (ICV) at the end of the PDU (except for any encipherment padding, see below);

b) padding for traffic flow confidentiality, integrity and encipherment mechanisms may be placed in separate fields;

c) a variable length number used for sequence integrity;

d) a flexible approach to the encoding of fields using type/length/value to allow easy extendibility and place minimal restrictions on the ordering of fields;

e) reflection protection provided by a protected SA initiator to responder direction flag.

8 Determination of security services and mechanisms

The security services to be applied by a security protocol are determined as described in clause 9. The security mechanisms to be applied are determined, given Security Services Selected, through use of security rules as described in clause 10.

9 Protection QOS

Protection QOS is the degree to which a service provider attempts to counter security threats using security services applied in the lower layers.

The handling of protection QOS service parameters is a local matter controlled according to the security policy in force. Protection QOS is not negotiated between the service users. For an instance of communication a service user may indicate its protection QOS requirements to the service provider. A service provider may indicate the protection QOS provided on an instance of communication to the service user. The protection QOS provided by the service provider need not be the same as that requested by the service user.

Any lower layer protocol exchanges between open systems (referred to as “in band” protocol exchanges) to convey information on the security services to be selected are carried in a security association protocol which is independent of an instance of communication. This may be carried implicitly by a security label or explicitly by other means.

10 Security rules

Security rules, given the security services selected, specify the security mechanisms to be used including all parameters needed for the operation of the mechanisms. An illustrative example of security rules which may be registered as agreed for use by a community is given in Annex A.

In the case of the security services selected being implied by a security label, the security rules also specify the mapping from a security label to the implied protection requirements.

NOTE – Currently, ITU-T | ISO/IEC are not standardising security rules.

11 Placement of security in the lower layers

Security Protocols are currently defined for use in the transport layer and the network layer [Transport Layer Security Protocol (TLSP) and Network Layer Security Protocol (NLSP)].

For connection mode communications TLSP operates in conjunction with ITU-T Rec. X.224 | ISO/IEC 8073 (see Figure 2). For connectionless mode communications TLSP operates in conjunction with ITU-T Rec. X.234 | ISO/IEC 8602 (see Figure 3).

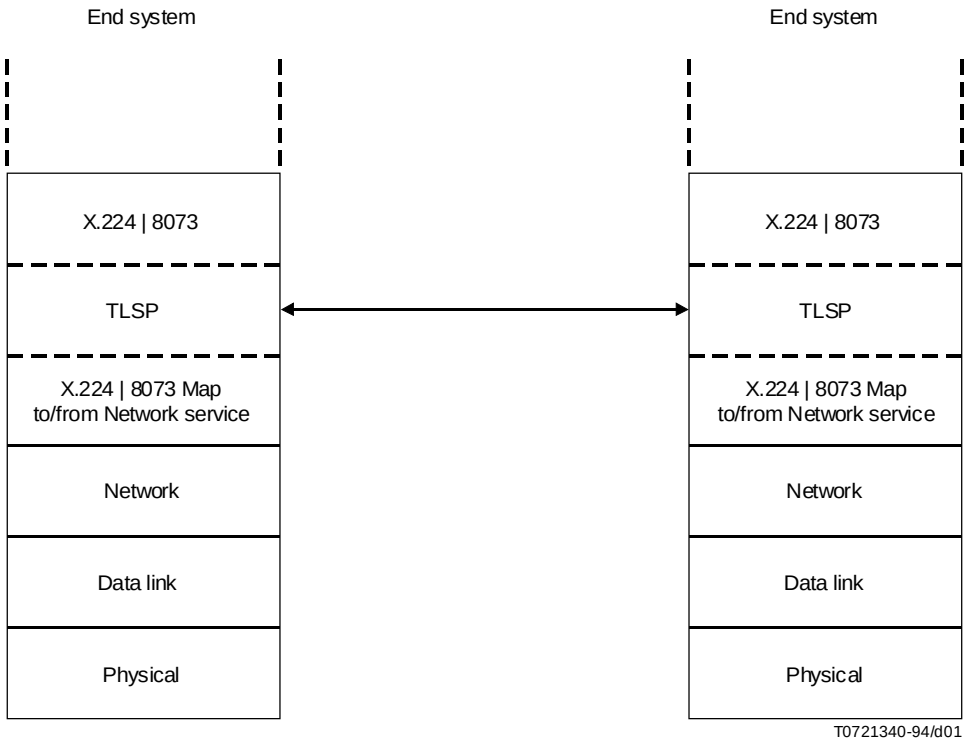


Figure 2 – Illustration of TLSP operating in conjunction with ITU-T Rec. X.224 | ISO/IEC 8073

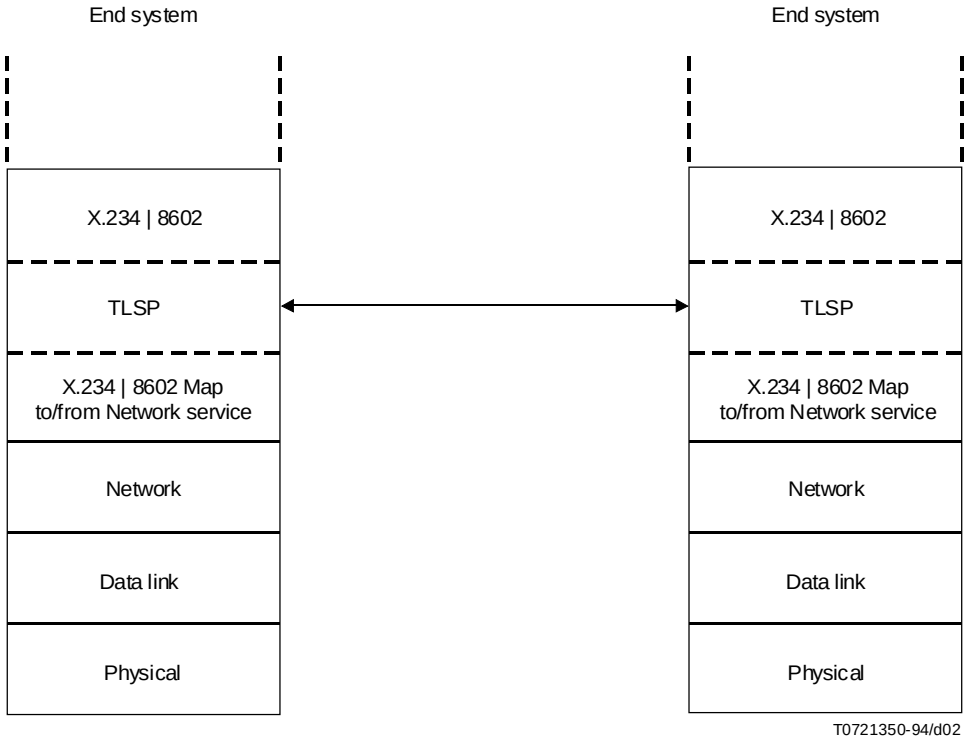


Figure 3 – Illustration of TLSP operating in conjunction with ITU-T Rec. X.234 | ISO/IEC 8602

Security in the network layer may be provided by a Subnetwork Independent Security Protocol (SNISP) which fulfils a subnetwork independent security role in addition to the roles identified in ISO 8648. As described below, a number of options exist for the different relationships between a SNISP such as NLSP and protocols providing the other network layer protocol roles as identified in ISO 8648.

For connectionless mode communication between end systems NLSP can operate over the “normal” network layer protocols. This is illustrated in Figure 4. This protects Network Service Data Units.

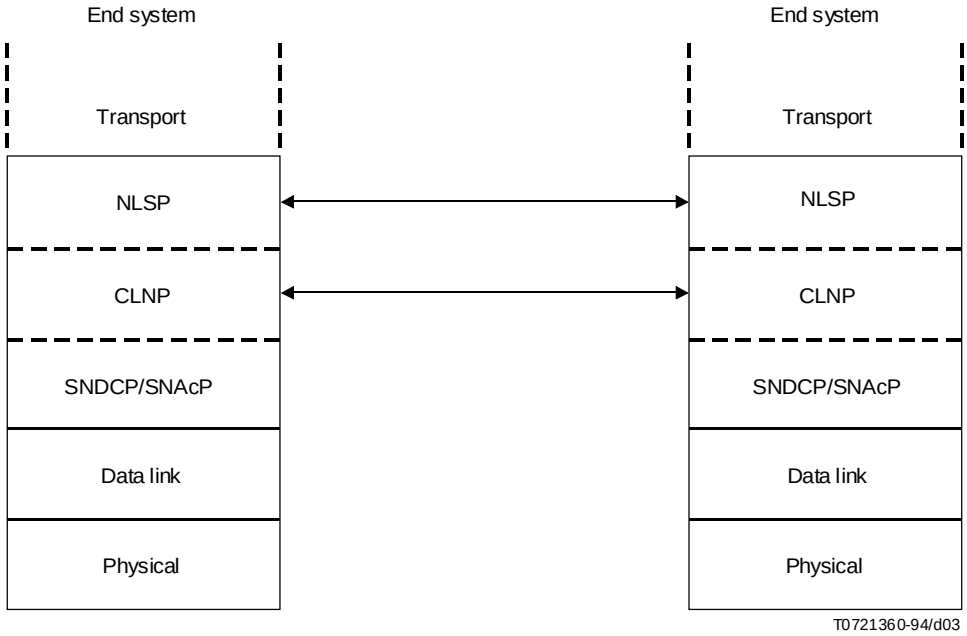


Figure 4 – Illustration of NLSP-CL between end systems

Alternatively, for connectionless mode communications between two end systems, an end system and intermediate system or between two intermediate systems, NLSP operates below the connectionless network protocol (see ITU-T Rec. X.233 | ISO/IEC 8473-1) and above either a subnetwork convergence protocol or ITU-T Rec. X.233 | ISO/IEC 8473-1. This is illustrated in Figures 5 and 6. The representation of two ITU-T Rec. X.233 | ISO/IEC 8473-1 layers and an NLSP layer does not necessarily imply separate protocol machines. This depends on the local implementation policy. This protects Network Protocol Data Units.

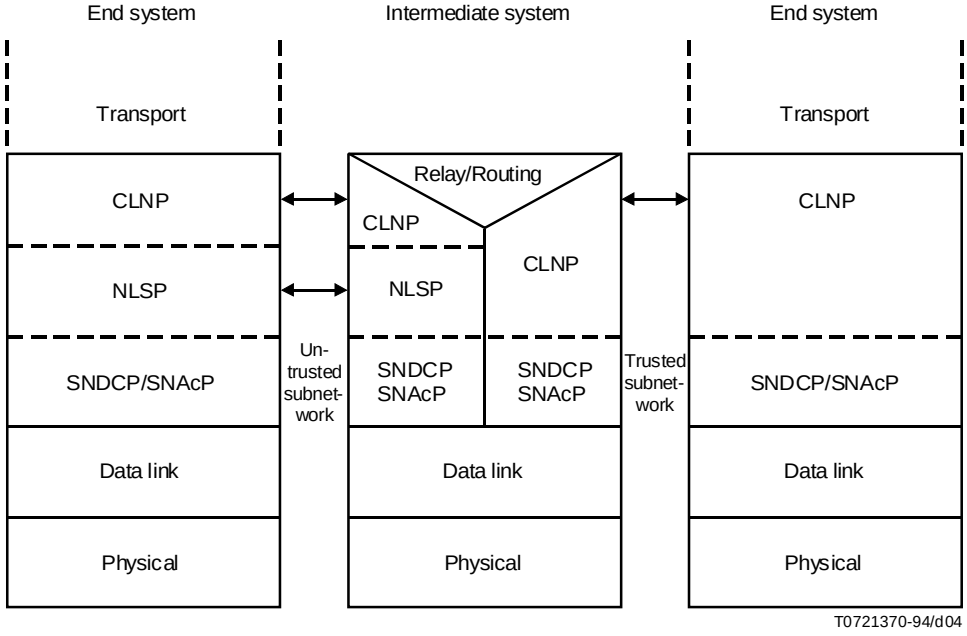


Figure 5 – Illustration of NLSP-CL with untrusted subnetwork

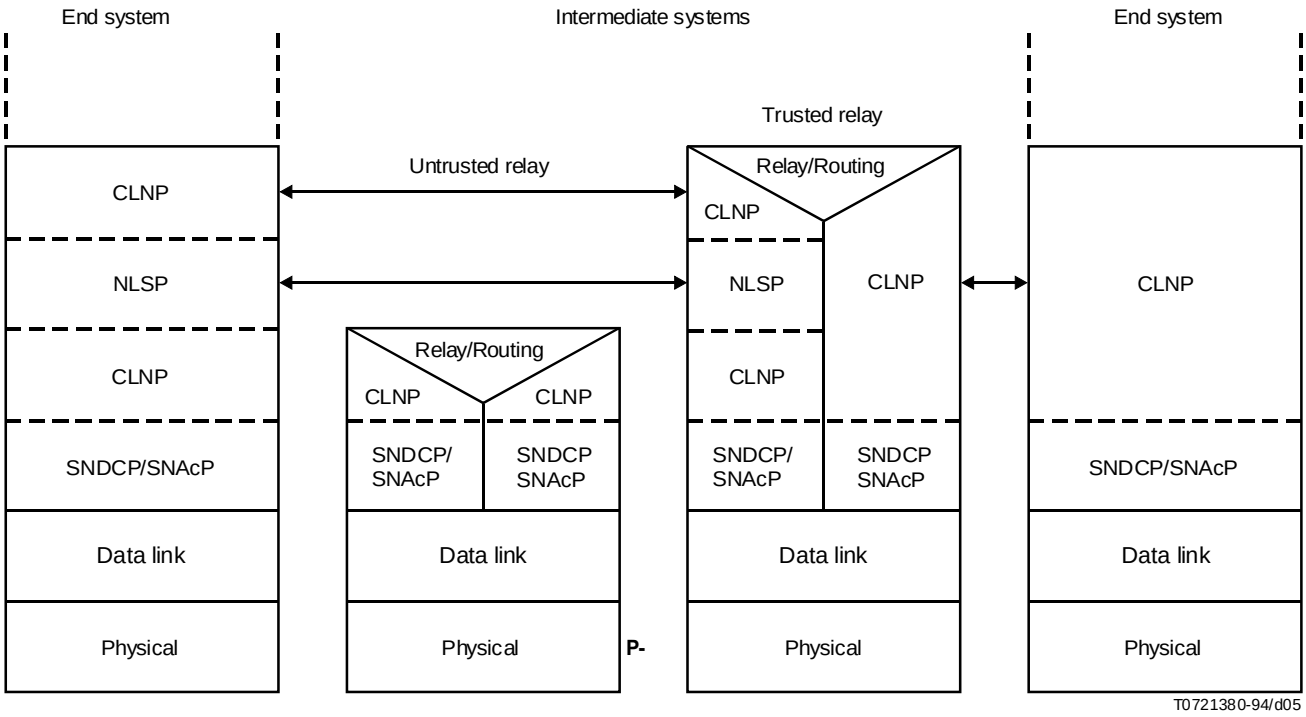


Figure 6 – Illustration of NLSP-CL with untrusted relay system

For connection mode communications NLSP always operates above either over a subnetwork independent protocol or a subnetwork access protocol such as ISO/IEC 8208. This is illustrated in Figures 7, 8 and 9. This protects Network Service Data Units. NLSP need not necessarily be located at the top of the network layer.

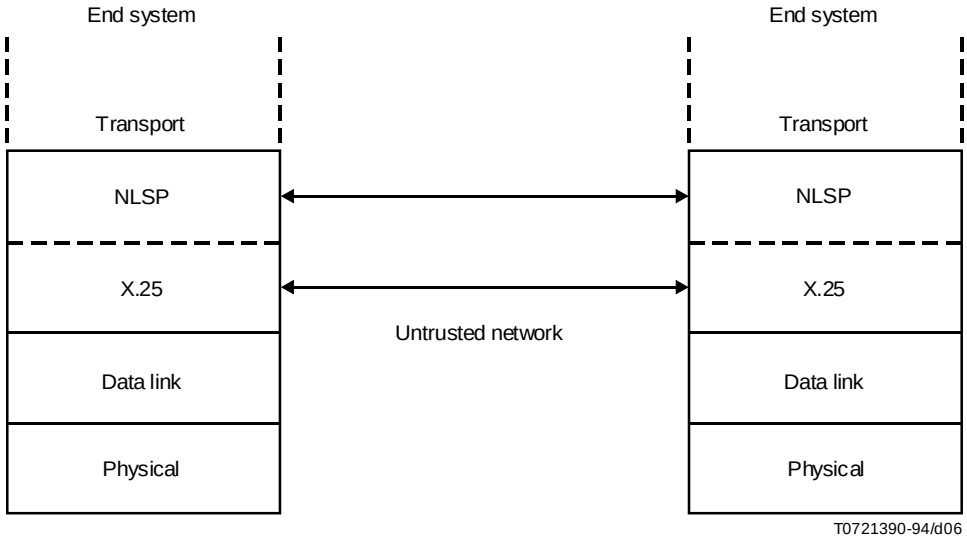


Figure 7 – Illustration of NLSP-CO between end systems

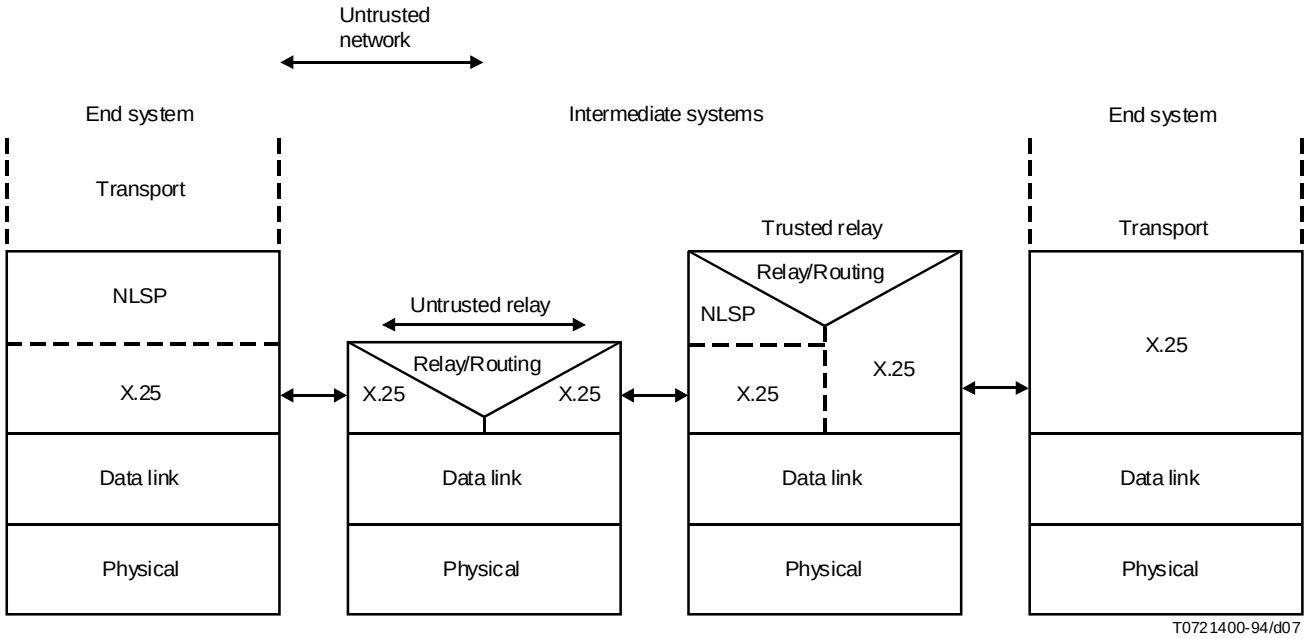
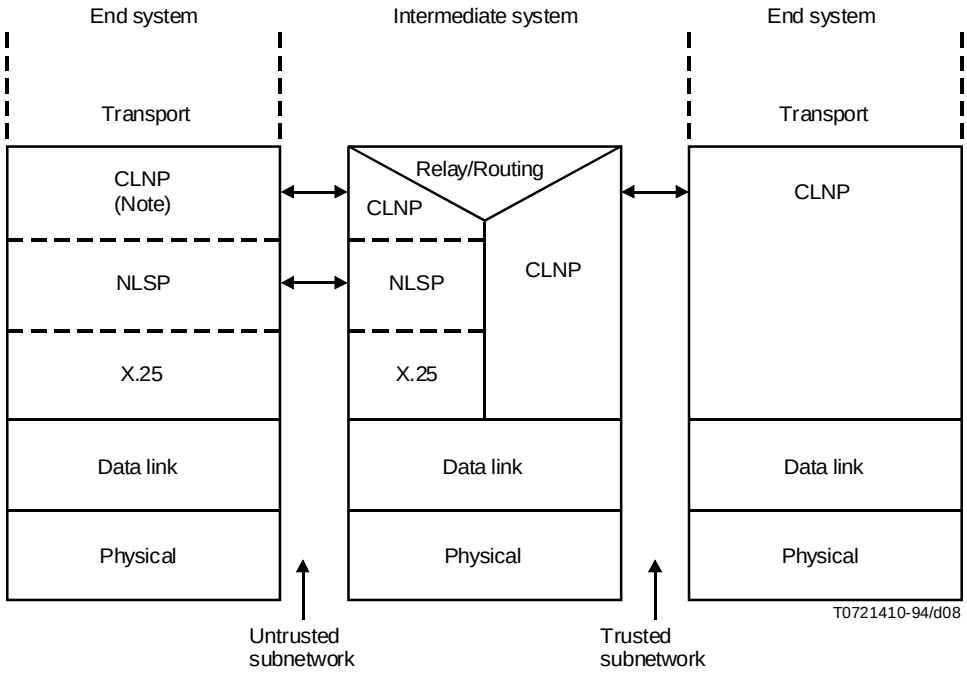


Figure 8 – Illustration of NLSP-CO with untrusted relay system



NOTE – This includes convergence function to CO mode.

Figure 9 – Illustration of NLSP within a multi-network environment

Other placements not included in this model may also be possible.

Interdomain Routeing Protocol (IDRP) (ISO/IEC 10747) exchanges can be protected by use of NLSP operating below IDRP and above ITU-T Rec. X.233 | ISO/IEC 8473-1 (see Figure 10). This protects IDRP Protocol Data Units.

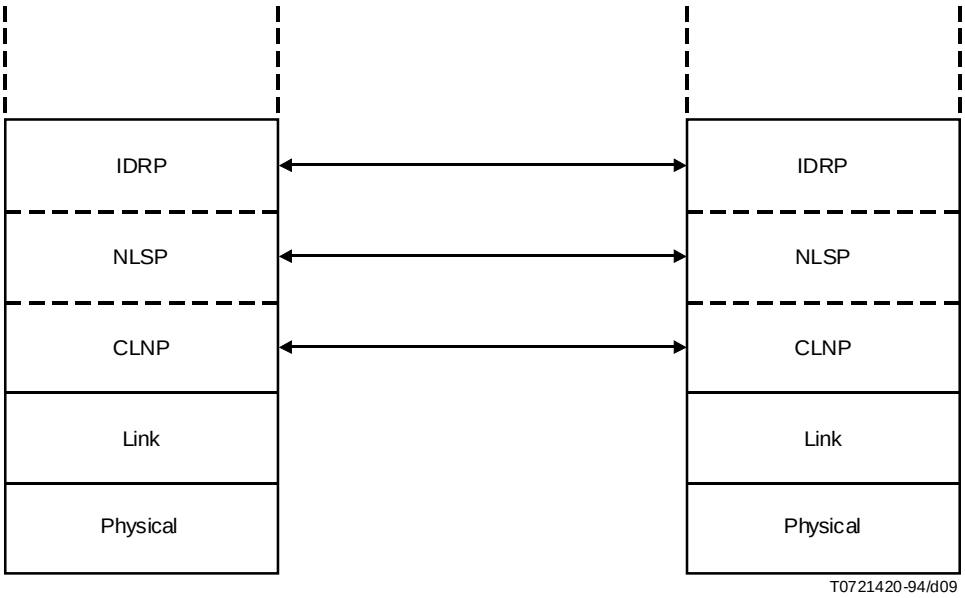


Figure 10 – Illustration of NLSP operating in conjunction with IDRP

A mapping may be defined for the NLSP underlying network service primitives to the data link service for use of a link layer protocol such as a Local Area Network (LAN) protocol as defined in ISO/IEC 8802 (see Figure 11).

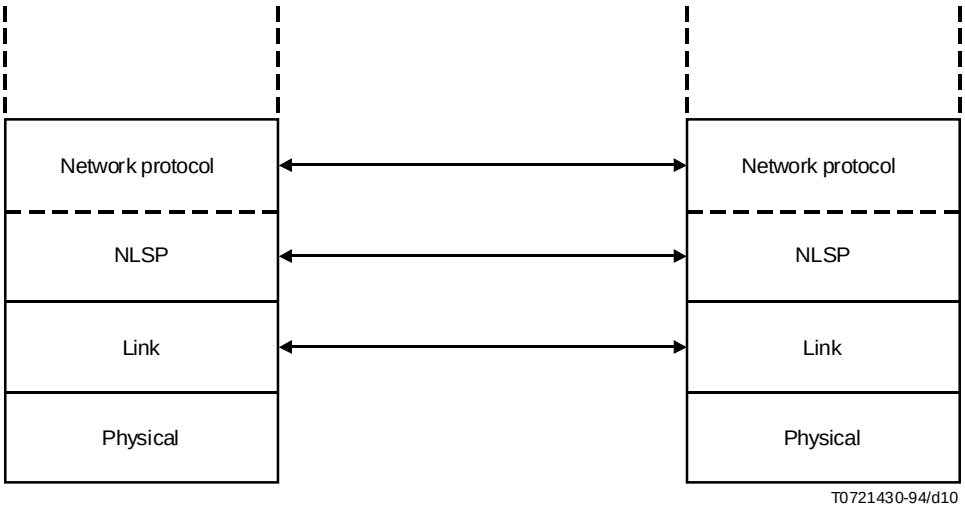


Figure 11 – Illustration of NLSP operating over link layer

CCITT Rec. X.800 | ISO 7498-2 includes a requirement for confidentiality in the data link layer. There is a requirement for a data link security protocol to protect communications between layer 2 bridges in a LAN environment (see Figure 12).

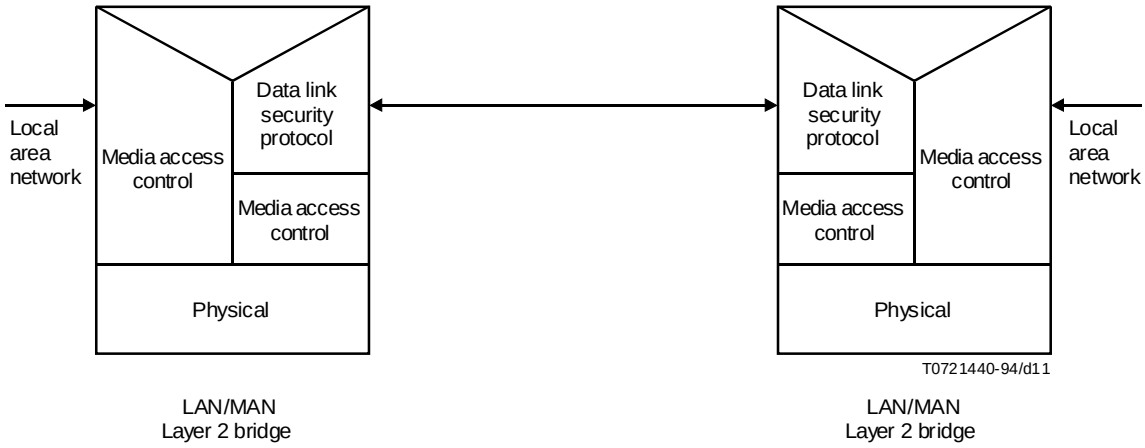


Figure 12 – Illustration of data link layer security protocol used to protect communication between two bridges

12 Use of (N–1)-layer(s) to enhance (N)-layer security

In providing security functions in a given layer, it is possible to make use of the security services provided by the layer(s) below. The total security services provided to the (N)-layer user can be made up from mechanisms in the underlying layers.

13 Security labelling

A security label may be used to indicate Security Services Selected requirements (see clause 9), as well as for access and routeing control.

Under a security association a pair of entities may pre-establish a set of security labels that may be assigned to connections/connectionless protocol data units between them.

The use of security labels is defined as part of a security policy.

The Security Frameworks, Part 3: Access Control describes the application of security labels for access control.

The first field of a security label shall identify the Security Authority which defines the label. This identifier will be an object identifier (as defined in ASN.1 CCITT Rec. X.208 | ISO/IEC 8824), encoded using the basic encoding rules (see CCITT Rec. X.208 | ISO/IEC 8825).

The general structure of security labels should be in line with SC27 work on security information objects.

14 Security domains

Security domains, as defined in ITU-T X.810 | ISO/IEC 10181-1 (Security Frameworks Overview), is not of direct concern to the peer-to-peer protocols. Rather, the use of domains should be considered in the context of the management of security.

15 Security of routeing

15.1 The Network Layer Security Protocol (NLSP) (see ITU-T Rec. X.273 | ISO/IEC 11577) can be used to protect the exchanges of interdomain routeing protocol data units (ISO/IEC 10747) (see also clause 11 on placement of IDRP).

15.2 NLSP (as defined CCITT Rec. X.273 | ISO/IEC 11577) cannot be used to support the security of intra-domain routeing exchanges based on ISO/IEC 10589 (Intermediate System to Intermediate System, IS-IS) and ISO/IEC 9542 (End System to Intermediate System, ES-IS) as it does not support multi-peer communications. A standard protocol based on an extension of NLSP for the security of IS-IS intra-domain and ES-IS routeing exchange protocols may be defined. Any such standard protocol for the security of IS-IS intra-domain and ES-IS routeing exchange should be independent of these routeing protocols.

15.3 It should be noted that access controls applied to communications (e.g. ITU-T X.25 | ISO/IEC 8208 closed user groups, ITU-T Rec. X.233 | ISO/IEC 8473-1 security labels, NLSP) may effect the routes available. Information on the security status of routes may be required for routeing information to be of use in secure environments.

15.4 Furthermore, consideration needs to be given on the requirements of routeing to support access control/routeing control.

NOTE – CCITT Rec. X.800 | ISO 7498-2 defines routeing control as "The application of rules during the process of routeing so as to avoid specific networks, links or relays". The routeing control might, for example, be based on addresses, and inhibit the routeing of all data into a subnetwork except from given authorised addresses. Alternatively, routeing control could be based on security labels, for example packets labelled "commercial in confidence" are not to be routed out on to the public network.

16 Security Management

16.1 Security policy

The following information is established as part of the security policy criteria for selecting security service and mechanisms in an (N)-layer for a given (N)-entity:

- criteria for establishing the Security Services Selected for an (N)-layer including maximum and minimum levels acceptable;
- criteria for mapping Security Services Selected to mechanisms and underlying protection requirements (i.e. security rules as described in clause 10).

Where security labels are used information is established as part of the security policy for the use of security labels (see clause 13).

Information is established as part of the security policy for auditing security relevant aspects of the layer protocols and for providing recovery.

16.2 Security association management

The management of security associations is discussed in clause 5.

16.3 Key management

The distribution and selection of keys may be done in one of the following ways *(methods)*:

a) as part of SA establishment;

b) within a security protocol; or

c) through mechanisms outside the scope of the lower layers of OSI.

16.4 Security Audit

The collection and analysis of security audit information is described in the Security Frameworks, Part 7: Security Audit (to be ISO/IEC 10181-7).

17 Traffic flow confidentiality

The handling of traffic padding is not well understood. Associated with traffic flow confidentiality in the CONS environment there may be three types of padding provided:

a) padding existing Secure Data PDUs;

b) generating dummy Secure Data PDUs;

c) generating dummy connections with other NLSP peer entities.

With each type of padding there are potential parameters which must be defined (for example, all PDUs should have length of 1024 octets; there should be a PDU on the connection every 500 milliseconds; when this NLSP entity makes a connection with a particular peer NLSP entity, then these six NLSP entities should also be connected and the same volume of traffic exchanged with them). These parameters are not well understood but in the first two padding cases they should be included as part of the security association. Therefore a boolean attribute is not adequate. Further study is required on the types of parameters needed.

18 Guidelines for the definition of SA-Attributes

An SA-Attribute is an information item required to control the security of communications and its remote peer. Three different classes of SA-Attribute are described in clause 5.

The SA-Attributes required to control a security protocol are defined as part of security protocol. This definition should include:

a) a mnemonic used to refer to the attribute in the security protocol;

b) the data type of the attribute;

c) a description of the attribute semantics;

d) a description of how the value of this attribute is established.

Many of the attributes required for a security protocol will depend on the mechanisms supported.

Examples of SA-Attribute definitions are:

Encipher:	Boolean
	Encipherment is used to provide confidentiality.
	The value of this attribute is defined by an Agreed Set of Security Rules given the Security Services Selected.
Enc_Alg:	Object Identifier allocated under ISO 9979
	Encipherment algorithm
	The value of this attribute is defined by an Agreed Set of Security Rules given the Security Services Selected.
Enc_key	Form defined by Agreed Set of Security Rules
	Encipherment key
	Value established by Security Association Establishment.

19 Error handling

The action to be taken when an error occurs in a security protocol will be determined by the local security policy. Options can include:

– discarding the PDU in error;

– issuing error PDUs;

– carrying out a Reset or Disconnect procedures;

– filing an audit report.

Annex A

Illustrative example of an Agreed Set of Security Rules

(This annex forms an integral part of this Recommendation | International Standard)

An Agreed Set of Security Rules (ASSR) establishes the security mechanisms to be used including all parameters needed to define the operation of the mechanism for given Security Services Selected.

ASSR-ID OBJECT IDENTIFIER

SA-ID_Length 4

Services Selected Definition Module

PE Auth: none, low, high
AC: none, low, high
Confid: none, low, high
Integ: none, low, high

Security Label Mapping

Label_Def_Auth XYZ

Label->Sensitivity = Unclass
implies
PE Auth none, AC none, Confid none, Integ none

Label-Sensitivity = Confidential
implies
PE Auth low, AC low, Confid low, Integ none

Label-Sensitivity = Secret
implies
PE Auth high, AC high, Confid high, Integ high

Protection of All Service Parameters
For Security Services Selected: Integ = high or Conf = high

Mechanism Module – Security labels for Access Control
For Security Services Selected: AC = high or Conf = high

Label_Def_Auth XYZ
Explicit indication Yes

Mechanism Module – Integrity Check Value
For Security Services Selected: Integ > none or PE Auth = High
or Mechanism Security Labels

ICV_Alg_Id XYZ
ICV_Block_size 8 octets
Re-key after 10,000 PDUs
Key distribution mechanism Asymmetric

Mechanism Module – Integrity Sequence Number
For Security Services Selected: Integ = high or Auth = High

ISN_Len 4 octets

Mechanism Module – Encipherment
For Security Services Selected: Conf > low

Enc_Alg_ID XYZ
Mode Chained

Enc_Block_Size 8 octets
Re-key after 1,000 PDUs
Key distribution mechanism Asymmetric

Mechanism Module – No Header

For Security Services Selected: Conf = low and Integ = none and not Label mechanism

Mechanism Module – Connection Authentication

For Security Services Selected: AC > Low or PE Auth > Low

Enc_Alg_ID XYZ

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

PKC_Alg_ID RSA