UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.802

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(04/95)

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

SÉCURITÉ

TECHNOLOGIES DE L'INFORMATION – MODÈLE DE SÉCURITÉ DES COUCHES INFÉRIEURES

Recommandation UIT-T X.802

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. Le UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution nº 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI. Le texte de la Recommandation X.802 de l'UIT-T a été approuvé le 10 avril 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 13594.

NOTE

Dans la présente Recommandation, l'expression «Administration» est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalisation et commutation	X.50-X.89
Aspects réseau	X.90-X.149
Maintenance	X.150-X.179
Dispositions administratives	X.180-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200-X.209
Définition des services	X.210-X.219
Spécifications des protocoles en mode connexion	X.220-X.229
Spécifications des protocoles en mode sans connexion	X.230-X.239
Formulaires PICS	X.240-X.259
Identification des protocoles	X.260-X.269
Protocoles de sécurité	X.270-X.279
Objets gérés de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Systèmes mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

TABLE DES MATIÈRES

Résumé

La présente Recommandation | Rapport technique décrit les aspects inter-couches de la fourniture des services de sécurité dans les couches inférieures du Modèle de référence OSI (couches transport, réseau, liaison de données et physique). Elle décrit les concepts architecturaux communs à ces couches, la base des interactions entre couches relatives à la sécurité, et le positionnement des protocoles de sécurité dans les couches inférieures.

RAPPORT TECHNIQUE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – MODÈLE DE SÉCURITÉ DES COUCHES INFÉRIEURES

1 Domaine d'application

La présente Recommandation | Rapport technique décrit les aspects inter-couches de la fourniture de services de sécurité dans les couches inférieures du Modèle de référence OSI (couches transport, réseau, liaison de données et physique).

La présente Recommandation | Rapport technique décrit:

a) les concepts architecturaux communs aux couches inférieures sur la base des éléments définis dans la Rec. X.800 du CCITT | ISO 7498-2;

b) les bases des interactions relatives à la sécurité entre les protocoles des couches inférieures;

c) les bases de toute interaction relative à la sécurité entre couches inférieures et couches supérieures de l'OSI;

d) le positionnement des protocoles de sécurité par rapport aux autres protocoles des couches inférieures, et le rôle relatif de tels positionnements.

Il ne doit pas y avoir de conflit entre les protocoles de sécurité des couches inférieures et le modèle décrit dans la présente Recommandation | Rapport technique.

La Rec. X.500 du CCITT | ISO/CEI 9594-1 identifie les services de sécurité qui relèvent de chacune des couches inférieures du Modèle de référence OSI.

2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Rapport technique. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Rapport technique sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

– Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de référence: Le modèle de référence de base.*

– Recommandation UIT-T X.233 (1993) | ISO/CEI 8473-1:1994, *Technologie de l'information – Protocole assurant le service réseau en mode sans connexion de l'interconnexion de systèmes ouverts: Spécification du protocole.*

– Recommandation UIT-T X.234 (1994) | ISO/CEI 8602:1995, *Technologies de l'information – Protocole assurant le service de transport en mode sans connexion de l'interconnexion des systèmes ouverts (OSI).*

– Recommandation UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de sécurité de la couche réseau.*

– Recommandation UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Technologie de l'information – Télécommunication et échange d'informations entre systèmes – Protocole de sécurité de la couche transport.*

- Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de sécurité pour les couches supérieures.*
- Recommandation UIT-T X.810[1)] | ISO/CEI 10181-1...[1)], *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre général de la sécurité dans les systèmes ouverts: Aperçu général.*
- Recommandation UIT-T X.812[1)] | ISO/CEI 10181-3...[1)], *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre général de la sécurité dans les systèmes ouverts: Contrôle d'accès.*

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

  ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base. Partie 2 – Architecture de sécurité.*
- Recommandation UIT-T X.224 (1993), *Protocole pour assurer le service de couche transport en mode connexion pour l'interconnexion de systèmes ouverts.*

  ISO/CEI 8073:1992, *Technologies de l'information – Télécommunications et échanges d'informations entre systèmes – Interconnexion de systèmes ouverts (OSI) – Protocole pour fourniture du service de transport en mode connexion.*
- Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8824:1990, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Spécification de la notation de syntaxe abstraite numéro 1 (ASN.1).*
- Recommandation X.209 du CCITT (1988), *Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8825:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro 1 (ASN.1).*

2.3 Autres références

- ISO/CEI 8208:1995, *Technologies de l'information – Communications de données – Protocole X.25 de couche paquet pour terminal de données.*
- Recommandation UIT-T X.25 (1993), *Interface entre équipement terminal de traitement de données et équipement de terminaison du circuit de données pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données.*
- ISO 8648:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Organisation interne de la couche Réseau.*
- ISO 9542:1988[2)], *Systèmes de traitement de l'information – Téléinformatique – Protocole de routage d'un système d'extrémité à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 8473).*
- ISO/CEI 10589:1992, *Technologies de l'information – Communication de données et échange d'informations entre systèmes – Protocole intra-domaine de routage d'un système intermédiaire à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 8473).*
- ISO/CEI 10747:1994, *Technologies de l'information – Télécommunication et échange d'informations entre systèmes – Protocole pour échange d'informations inter-domaine de routage parmi les systèmes intermédiaires supportant la transmission de PDU de l'ISO 8473.*

---

1) Actuellement à l'état de projet.

2) Actuellement en révision.

3 Définitions

3.1 Définitions du modèle de référence OSI

La présente Recommandation | Rapport technique utilise les termes suivants définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

– qualité de service

3.2 Définitions du cadre général de la sécurité dans les systèmes ouverts

La présente Recommandation | Rapport technique utilise les termes suivants définis dans la Rec. UIT-T X.810 | ISO/CEI 10181-1:

– domaine de sécurité

3.3 Définitions de l'organisation interne de la couche réseau

La présente Recommandation | Rapport technique utilise les termes suivants définis dans ISO 8648:

a) protocole d'accès de sous-réseau;

b) système d'extrémité;

c) système intermédiaire.

3.4 Définitions supplémentaires

Pour les besoins de la présente Recommandation | Rapport technique les définitions suivantes s'appliquent:

3.4.1 protection de réflexion: Mécanisme de protection qui détecte le renvoi d'une unité de donnée protocolaire vers son expéditeur.

3.4.2 attributs d'association de sécurité: Collection des informations requises pour régir la sécurité des communications entre une entité et son entité homologue.

3.4.3 association de sécurité: Relation établie entre des entités communicantes de couches inférieures pour laquelle sont définis les attributs d'association de sécurité correspondants.

3.4.4 règles de sécurité: Information locale qui, pour les services de sécurité choisis, spécifie les mécanismes de sécurité sous-jacents à utiliser, y compris l'ensemble des paramètres nécessaires au fonctionnement de ces mécanismes.

NOTE – Les règles de sécurité sont une forme de règles d'interaction sûres telles que celles-ci sont définies dans le Modèle de sécurité pour les couches supérieures (Rec. UIT-T X.803 | ISO/CEI 10745).

4 Abréviations

ISN	Numéro de séquence d'intégrité (*integrity sequence number*)
SSAA	Ensemble d'attributs d'association de sécurité (*set of SA-attributes*)
NLSP	Protocole de sécurité de couche réseau (*network layer security protocol*)
NLSP-CO	Protocole NLSP en mode connexion (*NLSP connection mode*)
NLSP-CL	Protocole NLSP en mode sans connexion (*NLSP connectionless mode*)
QOS	Qualité de service (quality of service) (conformément à la définition de la Rec. X.200 du CCITT | ISO/CEI 7498-1)
SA	Association de sécurité (*security association*)
SA-ID	Identificateur d'association de sécurité (*security association identifier*)
SNAcP	Protocole d'accès de sous-réseau (*subnetwork access protocol*) (conformément à la définition de ISO 8648)
SNISP	Protocole indépendant de sécurité de sous-réseau (*subnetwork independent security protocol*)
TLSP	Protocole de sécurité de couche transport (*transport layer security protocol*)

5 Associations de sécurité

5.1 Vue d'ensemble

5.1.1 Chaque protocole de sécurité utilise un certain nombre de mécanismes de sécurité pour fournir des services de sécurité à la couche immédiatement supérieure. Les services de sécurité nécessaires aux couches supérieures peuvent être indiqués aux couches inférieures au moyen de fonctions locales de supervision de la sécurité. Pour établir des communications sécurisées, le protocole de sécurité et tous les mécanismes de sécurité nécessitent un supplément d'information par rapport à ce qui est codé dans les PDU. Il s'agira par exemple de la spécification des mécanismes à utiliser par le protocole et, pour chaque mécanisme, d'informations spécifiques comme les clés nécessaires au mécanisme de chiffrement. Chaque élément d'information additionnelle est connu sous le nom d'attribut d'association de sécurité.

5.1.2 Les attributs d'association de sécurité peuvent être placés dans une entité de protocole au moyen d'un certain nombre de mécanismes de positionnement. Il s'agira par exemple des mécanismes suivants:

a) positionnement pendant la fabrication d'un dispositif;

b) positionnement pendant l'initialisation d'un dispositif;

c) positionnement via une interface manuelle, par exemple par les commandes des panneaux de face avant;

d) positionnement par la gestion de sécurité des systèmes OSI;

e) positionnement par la gestion de sécurité de couche OSI;

f) positionnement par la gestion de sécurité des opérations OSI.

5.1.3 Les attributs d'association de sécurité (SA) peuvent être positionnés à n'importe quel moment avant la communication à laquelle ils se rapportent. Quand des ensembles compatibles d'attributs d'associations de sécurité (SSAA) sont positionnés dans chaque entité de protocole, on dit qu'une association de sécurité existe entre ces entités.

5.1.4 Des ensembles SSAA (et des associations de sécurité) peuvent exister avec différents niveaux de granularité. Parfois il est utile de pouvoir se référer à des ensembles SSAA de granularité différente. Par exemple, l'ensemble SSAA défini par un ensemble convenu de règles de sécurité (ASSR) pourrait être appelé SSAA ASSR. Ou une clef appariée pourrait être établie entre deux entités de protocole pour être employée sur un certain nombre d'instances de couples d'adresses ayant des sources et destinations communes. De façon similaire le SSAA pour une instance de communication pourrait être dénommé instance de communication SSAA. De même l'ensemble SSAA pour une PDU orientée connexion pourrait être appelée SSAA CO PDU.

5.1.5 En règle générale, les attributs d'associations SA doivent être placés dans l'entité de protocole par un moyen sécurisé afin d'en préserver la sécurité. Ceci implique que les attributs d'associations de sécurité soient positionnés par un moyen physique sécurisé ou à l'aide d'une association de sécurité existante qui aura préalablement été positionnée à cette fin.

5.1.6 Les ensembles d'attributs SSAA qui font partie d'une association de sécurité sont souvent désignés par un identificateur dénommé SA-ID ayant une signification locale. A un instant donné, certains éléments de l'ensemble d'attributs d'association de sécurité peuvent être indéfinis. Au moment de l'initialisation d'une communication sécurisée, l'ensemble des attributs SSAA ne sera généralement pas complètement valué, et les échanges initiaux seront utilisés pour compléter la valuation des attributs SSAA avant l'échange des données utilisateur.

5.1.7 Afin de fournir une protection de répétition, il faut appliquer des contraintes à l'usage d'identificateurs SA-ID, leurs ensembles SSAA de référence et les attributs d'association SA.

a) Les identificateurs SA-ID ne peuvent pas être réutilisés avec la même clé de chiffrement.

b) Après qu'un quelconque attribut SA a été valué dans un ensemble SSAA identifié par un identificateur SA-ID, cet attribut ne pourra jamais être changé, à moins que le protocole de sécurité ne possède un moyen de signaler le changement aux entités en communication. Ceci implique que, pour autoriser un basculement de clé, un nouvel identificateur de SA-ID doit être utilisé avec des copies des anciens attributs SA et une nouvelle clé, à moins que le protocole de sécurité ne dispose d'un autre moyen de signaler le changement de clé (fonction assurée par exemple par l'unité de données protocolaires NLSP-CO CSC).

5.1.8 Le retrait de l'un quelconque des attributs de sécurité SSAA a pour effet de clôturer l'association de sécurité.

5.1.9 Certains attributs d'association de sécurité ont une signification pour une instance de communication (une PDU sans connexion ou une connexion). D'autres attributs d'association de sécurité ont une signification pour une seule PDU sur une connexion. Comme exemple de tels attributs, on citera les numéros de séquence d'intégrité (ISN) et les étiquettes de sécurité. Il peut sembler que la modification de ces attributs viole les contraintes citées au point b) du 5.1.7. Cependant, l'association de sécurité comprenant ces attributs SA n'est logiquement valide que pour la durée de vie d'une

seule PDU. Le numéro ISN joue le rôle d'une extension logique de l'identificateur SA-ID, et modifie par conséquent l'identificateur SA-ID en vigueur. L'étiquette de sécurité n'est alors valide que pour cette instance d'identificateur SA-ID étendu. Ainsi les contraintes sont-elles respectées. De tels attributs sont parfois qualifiés de «dynamiques».

5.1.10 Une part de la politique de sécurité va imposer des contraintes aux opérations de l'entité protocolaire. Cette partie de la politique de sécurité est appelée «ensemble de règles de sécurité pour l'entité protocolaire». Cet ensemble de règles peut imposer des contraintes à des composants tels que le mécanisme de sécurité à utiliser ainsi que les valeurs et le mécanisme de positionnement des attributs d'association de sécurité. L'ensemble des règles de sécurité définira aussi le mappage des services de sécurité sélectionnés sur les mécanisme utilisés par le protocole de sécurité. L'ensemble de règles de sécurité est une forme de règles d'interaction sécurisée.

5.1.11 Lorsqu'un tel ensemble est utilisé en exploitation intra ou inter domaines, il recevra un identificateur unique, et cet ensemble est alors appelé «ensemble mutuellement convenu de règles de sécurité (ASSR) (*agreed set of security rules*)». L'identificateur de l'ensemble ASSR peut être modifié lors de l'établissement de l'association de sécurité pour déterminer ou contraindre l'ensemble des règles de sécurité s'appliquant à l'ensemble des attributs et qui est défini pour l'association de sécurité. Les attributs d'association de sécurité, s'il y en a, doivent être établis en utilisant d'autres moyens, par exemple ceux qui sont énumérés au 5.1.2.

5.2 Etablissement d'associations de sécurité pour les couches inférieures

5.2.1 Afin de protéger une instance de communication (une SDU sans connexion ou une connexion) une association de sécurité doit être établie entre les entités en communication.

5.2.2 L'information constitutive d'une association de sécurité est soit une information statique qui peut être «négociée» lorsque l'association est établie et qui demeure ensuite fixe pour toute la durée de l'association, soit une information dynamique qui peut être mise à jour au cours d'une instance de communication.

5.2.3 Une association SA peut être établie par un protocole des couches OSI 1 à 4 par l'échange d'unités de données protocolaires (PDU) d'association de sécurité, ou par des mécanismes ne relevant pas des couches inférieures de l'OSI.

5.2.4 Avant d'établir une association de sécurité, chaque entité aura préétabli un ensemble de règles de sécurité commun, mutuellement accepté et uniquement défini, ainsi que les services de sécurité qui peuvent être sélectionnés.

5.2.5 Si l'association de sécurité doit être établie par l'échange de PDU d'association de sécurité, alors les éléments suivants doivent aussi être préétablis:

a) une sélection initiale des services de sécurité et, par conséquent, les mécanismes de sécurité à appliquer pendant l'établissement de l'association de sécurité;

b) les informations élémentaires d'encodage nécessaires pour établir l'association de sécurité.

5.2.6 A l'établissement d'une association SA, une entité détermine avec son homologue distant les informations partagées suivantes qui doivent rester inchangées (c'est-à-dire statiques) pour la durée de l'association:

a) les identificateurs SA-ID local et distant;

b) les services de sécurité sélectionnés pour être utilisés par les entités associées pour les instances de communication qu'elles établissent entre elles.

NOTE – Les services de sécurité à utiliser peuvent être sélectionnés parmi les services de sécurité préétablis.

c) les mécanismes et leurs propriétés à utiliser en conséquence des services de sécurité sélectionnés;

d) les clés partagées initialement pour l'intégrité, les mécanismes de chiffrement et l'authentification d'une instance de communication;

e) l'ensemble des étiquettes de sécurité et des adresses qui peuvent être utilisées dans cette association pour le contrôle d'accès.

5.2.7 Les identificateurs SA-ID et les clés partagées [points a) et b) ci-dessus] doivent être établis sur la base de chaque association. Les autres informations peuvent être préétablies. En plus, dans l'établissement d'une association de sécurité, l'identité du correspondant distant doit être validée pour assurer la fonction d'authentification de l'entité homologue.

5.2.8 Les informations suivantes peuvent être mises à jour dynamiquement lors d'une communication donnée:

a) numéro(s) de séquences d'intégrité selon les besoins de transmission des données normales et express dans chaque direction;

b) étiquette de sécurité, sélectionnée dynamiquement à partir de l'ensemble statique des étiquettes de sécurité;

c) information de changement de clé pour les mécanismes de chiffrement/intégrité dans des protocoles de sécurité acceptant le renouvellement de clé au sein d'une association (par exemple, le protocole de sécurité de la couche réseau en mode connecté).

5.2.9 Pour assurer l'authentification de l'entité correspondante ou de l'origine des données, les mécanismes de validation d'identité doivent être appliqués à chaque instance de communication.

5.2.10 Les différents attributs d'association de sécurité qui peuvent être définis aux différentes étapes de l'établissement d'une association de sécurité sont présentés schématiquement sur la Figure 1. Les termes préétabli, satique et dynamique, sont utilisés en référence à une association de sécurité selon ce qui est décrit dans les paragraphes précédents. Les termes utilisés et la forme de l'authentification correspondent à ce qui est décrit dans les paragraphes précédents.

<table>
<tr><th>Pré-établi</th><th>Statique</th><th>Dynamique</th></tr>
<tr><td>Ensemble convenu de règles de sécurité
Services de sécurité possibles
Services de sécurité initiaux
Clé de base</td><td>Identificateurs SA-ID
Clés initiales
Authentification</td><td>Numéro ISN
Etiquette de sécurité
Information de renouvellement de clé
Authentification</td></tr>
<tr><td colspan="2">Choix du niveau de la qualité de protection
Mécanismes sélectionnés
Ensemble d'étiquettes de sécurité et d'adresses</td><td></td></tr>
</table>

Figure 1 – Illustration des attributs d'une association de sécurité

5.2.11 Une entité identifiera les attributs d'association de sécurité nécessaires au moyen de l'identificateur SA-ID.

5.2.12 L'association de sécurité sera établie avant de protéger l'instance de communication.

5.3 Clôture d'association de sécurité

Une association de sécurité identifiée par un identificateur SA-ID est clôturée quand l'association SA n'est plus valide.

Une association de sécurité peut être clôturée par les méthodes suivantes:

a) comme un protocole OSI des couches 1 à 4, par l'échange d'unités de données protocolaires (PDU) d'association de sécurité,

b) en utilisant des mécanismes ne relevant pas des couches inférieures de l'OSI,

c) implicitement par la clôture d'une connexion (ceci n'est applicable qu'au mode connecté),

d) implicitement lorsqu'expire une clé au sein de l'association SA.

NOTE – Des précautions particulières doivent être prises dans l'approche d) lorsque la durée de vie d'une clé est définie par le nombre de paquets envoyés/reçus entre entités en correspondance, l'évaluation de ce nombre par les deux entités pouvant être très différente.

Pour utiliser le mécanisme c) ci-dessus, un attribut de l'association de sécurité doit indiquer que l'association doit être clôturée à la clôture d'une connexion utilisant cette association.

5.4 Modification des attributs dans une connexion

Pour chaque instance de communication (une PDU sans connexion ou une connexion), une seule association de sécurité peut être établie.

Pendant la durée de vie d'une connexion, les services et les mécanismes de sécurité utilisés pour cette connexion ne peuvent pas être modifiés (à noter que cela n'exclue pas la possibilité de changer de clé).

L'indication de changement de clé sera décrit par le protocole de sécurité.

6 Influence sur les protocoles existants

6.1 Principe général

En principe, l'influence de protocoles de sécurité sur les protocoles existants doit être minimale.

6.2 Taille d'une SDU sans connexion

Durant les transferts de données, et selon les mécanismes de sécurité sélectionnés, la sécurité a l'impact suivant sur le protocole de couche (N):

a) les données d'utilisateur (N), et dans certains cas des parties de l'information de contrôle de protocole (N), sont traitées par des transformations cryptographiques avant et après la transmission. Ceci peut changer la longueur des données d'utilisateur (N).

b) les informations de contrôle protocolaire relatives aux données d'utilisateur (N) (par exemple, les identificateurs d'association de sécurité, les modes de vérification cryptographiques) peuvent nécessiter d'être véhiculés par le protocole (N).

NOTE – Ceci aura un impact sur la taille maximale de données d'utilisateur selon la définition du 15.2.3 de la Rec. X.213 du CCITT | ISO/CEI 8348 et de la Rec. X.214 du CCITT | ISO/CEI 8072.

6.3 Concaténation de PDU

Seules peuvent être concaténées des PDU qui doivent être protégées dans le cadre d'une même association de sécurité.

6.4 Indépendance des algorithmes et des mécanismes

Les protocoles de sécurité des couches inférieures sont spécifiés comme étant indépendants de l'algorithme. En outre, le parti pris pour le protocole NLSP a été de séparer les parties du protocole dépendantes du mécanisme des parties indépendantes de celui-ci. On prévoit que les protocoles à venir des couches inférieures pourraient assurer cette indépendance en utilisant des services génériques abstraits de sécurité communs aux couches supérieures et inférieures de l'OSI.

7 Structure commune de sécurité des PDU

7.1 Une structure générale commune de PDU doit être utilisée pour les unités de données protégées dans les protocoles de sécurité des couches inférieures. Bien que la structure générale des PDU soit la même pour tous les protocoles de sécurité des couches inférieures, ceux-ci ne sont bien sûr pas identiques pour différentes raisons, la plus évidente étant les restrictions de format imposées par une couche protocolaire particulière.

7.2 Les PDU des protocoles de sécurité des couches inférieures pourront partager certaines caractéristiques structurelles:

a) ajout d'une valeur de contrôle d'intégrité (ICV) (*integrity check value*) à la fin de la PDU (indépendamment du remplissage de chiffrement, voir ci-dessous);

b) utilisation de champs différents pour les remplissages correspondant aux mécanismes de confidentialité, d'intégrité et de chiffrement du trafic;

c) utilisation d'un nombre de longueur variable pour l'intégrité de séquence;

d) adoption d'une approche flexible pour le codage des champs en utilisant un codage en type/longueur/valeur pour permettre une extension aisée et imposer le minimum de restrictions à l'ordonnancement des champs;

e) protection contre les réflexions assurée par le sémaphore directionnel initiateur vers répondeur de l'association de sécurité.

8 Détermination des services et mécanismes de sécurité

Les services de sécurité que doit assurer un protocole de sécurité sont déterminées conformément à l'article 9. Pour des services de sécurité sélectionnés donnés, les mécanismes de sécurité qui doivent être appliqués sont déterminés par l'application des règles de sécurité selon la description de l'article 10.

9 Qualité de service de protection

La qualité de service de protection est le degré auquel un prestataire de service essaie de contrecarrer les menaces de piratage en utilisant les services de sécurité des couches inférieures.

Le traitement des paramètres de qualité des services de protection est un problème du ressort local, décidé en fonction de la politique de sécurité en vigueur. La qualité de service de la protection n'est pas négociée entre les utilisateurs de service. Pour une instance de communication, un utilisateur peut signifier au prestataire de service ses exigences en matière de qualité de service de protection. Le prestataire peut indiquer à l'utilisateur la qualité de service de protection assurée pour une instance de communication donnée. La qualité de service de protection assurée par le prestataire de service n'a pas besoin d'être la même que celle qui a été demandée par l'utilisateur.

N'importe quel échange protocolaire de couche inférieure entre systèmes ouverts (désigné ici comme un échange protocolaire «dans la bande») destiné à transmettre des informations sur les services de sécurité à choisir sera effectué dans le cadre d'un protocole d'association de sécurité indépendant de l'instance de communication. Ceci peut être assuré implicitement par une étiquette de sécurité ou explicitement par d'autres moyens.

10 Règles de sécurité

Une fois les services de sécurité sélectionnés, les règles de sécurité spécifient les mécanismes de sécurité à utiliser, y compris tous les paramètres nécessaires à la mise en œuvre des mécanismes. L'Annexe A illustre par un exemple les règles de sécurité qui pourraient être considérées comme adoptées par un groupe d'entités.

Lorsque les services de sécurité sélectionnés sont impliqués par une étiquette de sécurité, les règles de sécurité spécifient aussi la correspondance entre l'étiquette de sécurité et les prescriptions de protection implicites.

NOTE – Actuellement l'UIT-T et l'ISO/CEI ne normalisent pas de règles de sécurité.

11 Positionnement des protocoles de sécurité dans les couches inférieures

Des protocoles de sécurité sont actuellement définis pour être utilisés dans la couche transport et la couche réseau [protocole de sécurité de la couche transport (TLSP) (*transport layer security protocol*) et protocole de sécurité de la couche réseau (NLSP) (*network layer security protocol*)].

En mode connecté, le protocole TLSP est mis en œuvre avec le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073 (voir Figure 2). En mode sans connexion, le protocole TLSP est mis en œuvre avec le protocole de la Rec. UIT-T X.234 | ISO/CEI 8602 (voir Figure 3).

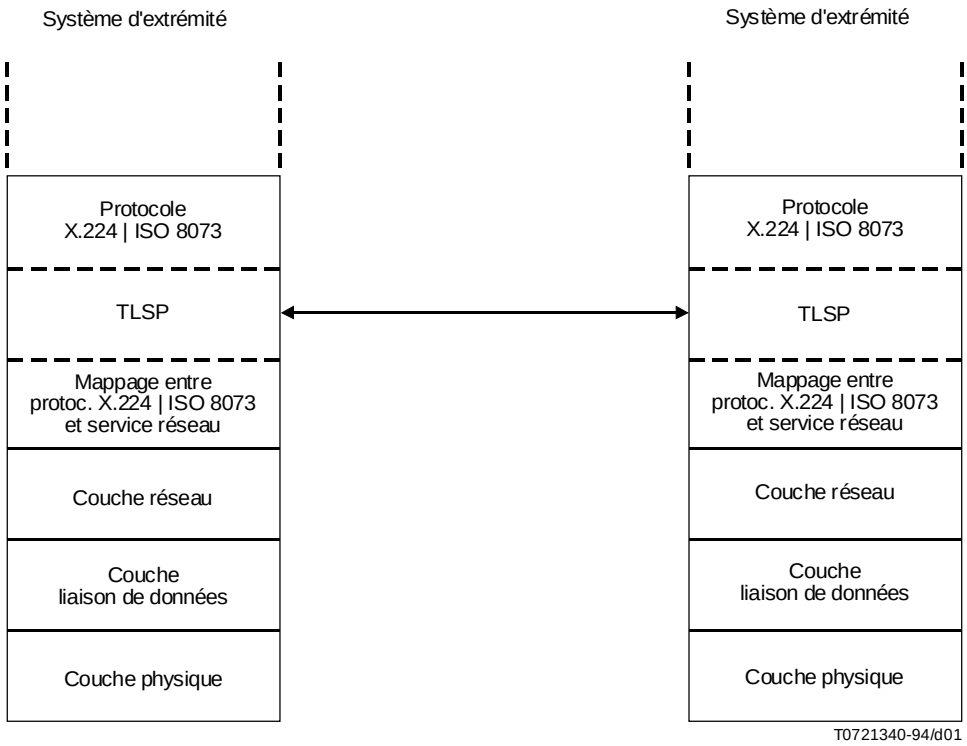


Figure 2 – Illustration du protocole TLSP mis en œuvre avec le protocole UIT-T X.224 | ISO/CEI 8073

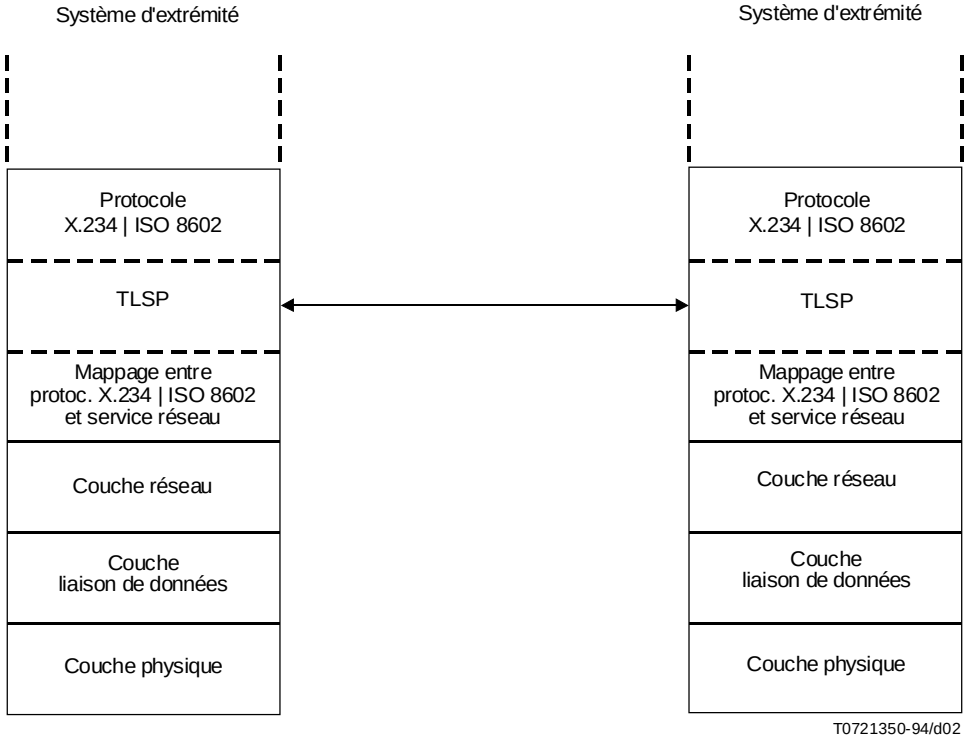


Figure 3 – Illustration du protocole TLSP mis en œuvre avec le protocole UIT-T X.234 | ISO/CEI 8602

La sécurité dans la couche réseau peut être assurée par un protocole de sécurité indépendant du sous-réseau (SNISP) (*subnetwork independent security protocol*) qui, outre les rôles définis par ISO 8648, remplit un rôle de sécurité indépendant du sous-réseau. Comme décrit ci-dessous, un protocole SNISP comme le protocole NLSP peut avoir différentes relations possibles avec les protocoles assurant les autres fonctions protocolaires de la couche réseau identifiés dans ISO 8648.

Pour les communications en mode sans connexion entre systèmes d'extrémité, le protocole NLSP peut agir par dessus des protocoles «normaux» de la couche réseau, comme l'illustre la Figure 4. Cette configuration assure la protection des unités de données de service (SDU) de la couche réseau.

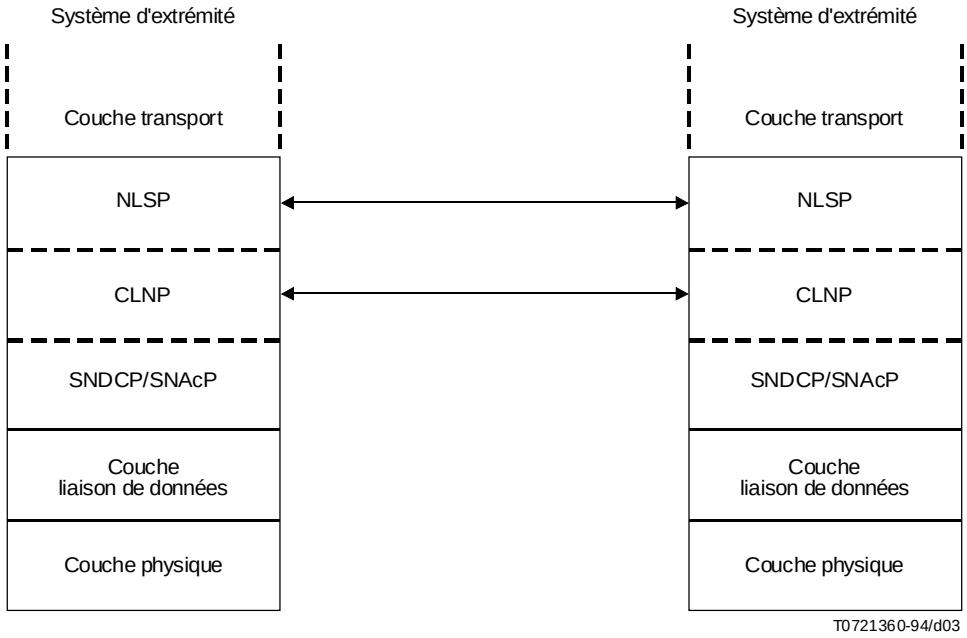


Figure 4 – Illustration du protocole NLSP en mode sans connexion entre systèmes d'extrémité

Pour les communications en mode sans connexion entre deux systèmes d'extrémité, un système d'extrémité et un système intermédiaire, ou entre deux systèmes intermédiaires, il est également possible d'installer le protocole de sécurité NLSP en dessous du protocole réseau en mode sans connexion CLNP (voir Rec. UIT-T X.233 | ISO/CEI 8473-1) et par-dessus un protocole de convergence de sous-réseau SNDCP, ou par-dessus le protocole d'accès au sous-réseau SNAcP de la Rec. UIT-T X.233 | ISO/CEI 8473-1, comme l'illustrent les Figures 5 et 6. Cette représentation de deux couches Rec. UIT-T X.233 | ISO/CEI 8473-1 et d'une couche de protocole NLSP n'implique pas forcément des machines protocolaires distinctes. Ceci dépend de la politique de conception locale. Cette configuration assure la protection des unités de données protocolaires (PDU) de réseau.

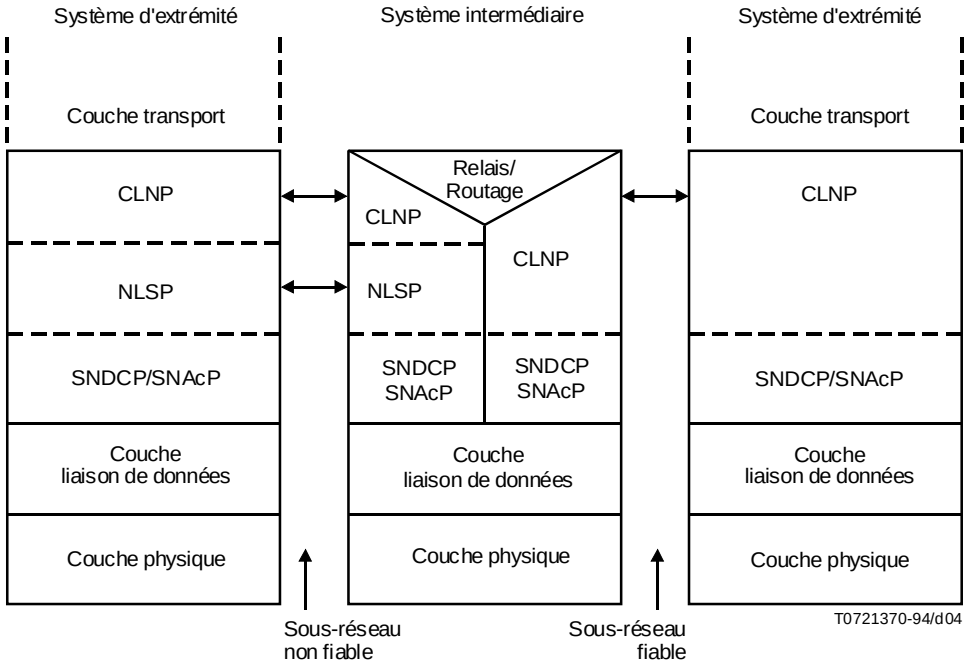


Figure 5 – Illustration du protocole NLSP en mode sans connexion avec un sous-réseau non fiable

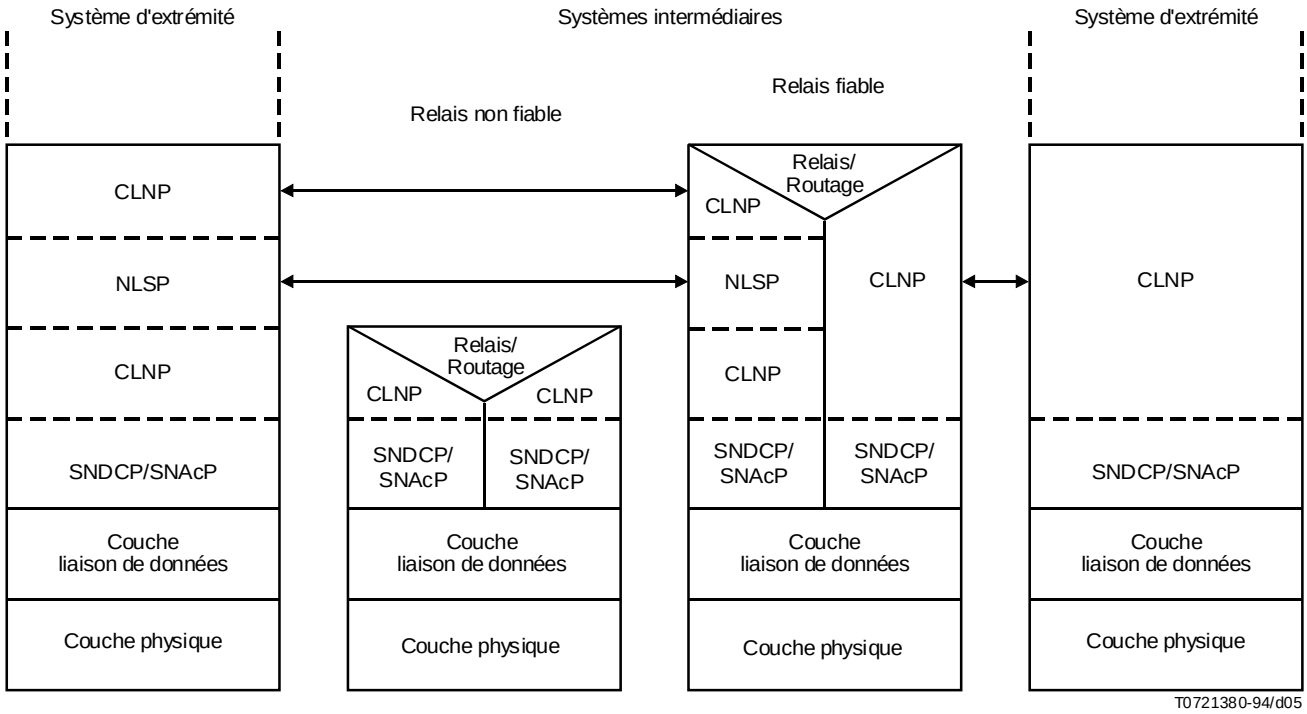


Figure 6 – Illustration du protocole NLSP en mode sans connexion avec un système relais non fiable

Pour les communications en mode connecté, le protocole NLSP agit toujours par-dessus un protocole de sous-réseau indépendant, ou par-dessus un protocole d'accès de sous-réseau comme l'ISO/CEI 8208. Ceci est illustré sur les Figures 7, 8 et 9. Cette configuration assure la protection des unités de données de service (SDU) de réseau. Le protocole NLSP n'a pas forcément besoin de se situer au sommet de la couche réseau.

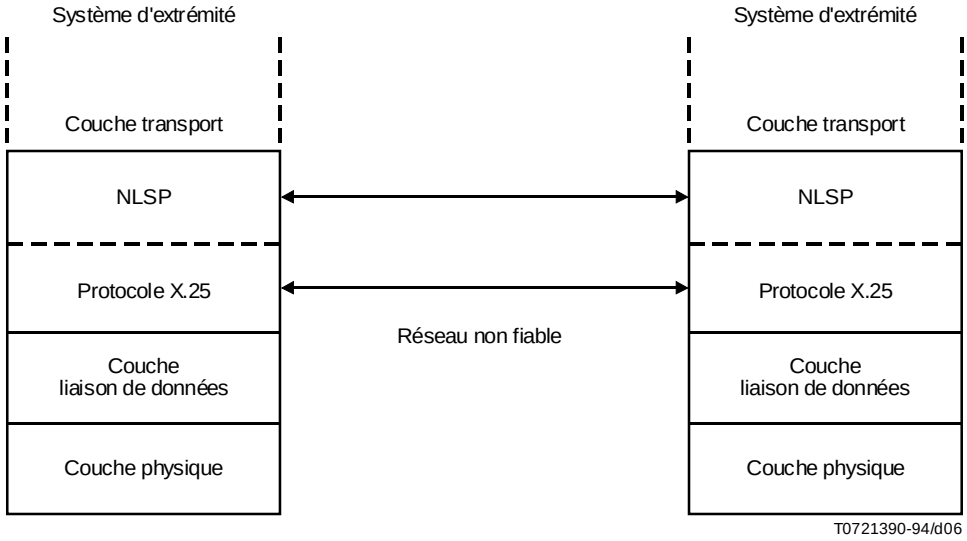


Figure 7 – Illustration du protocole NLSP en mode connecté entre systèmes d'extrémité

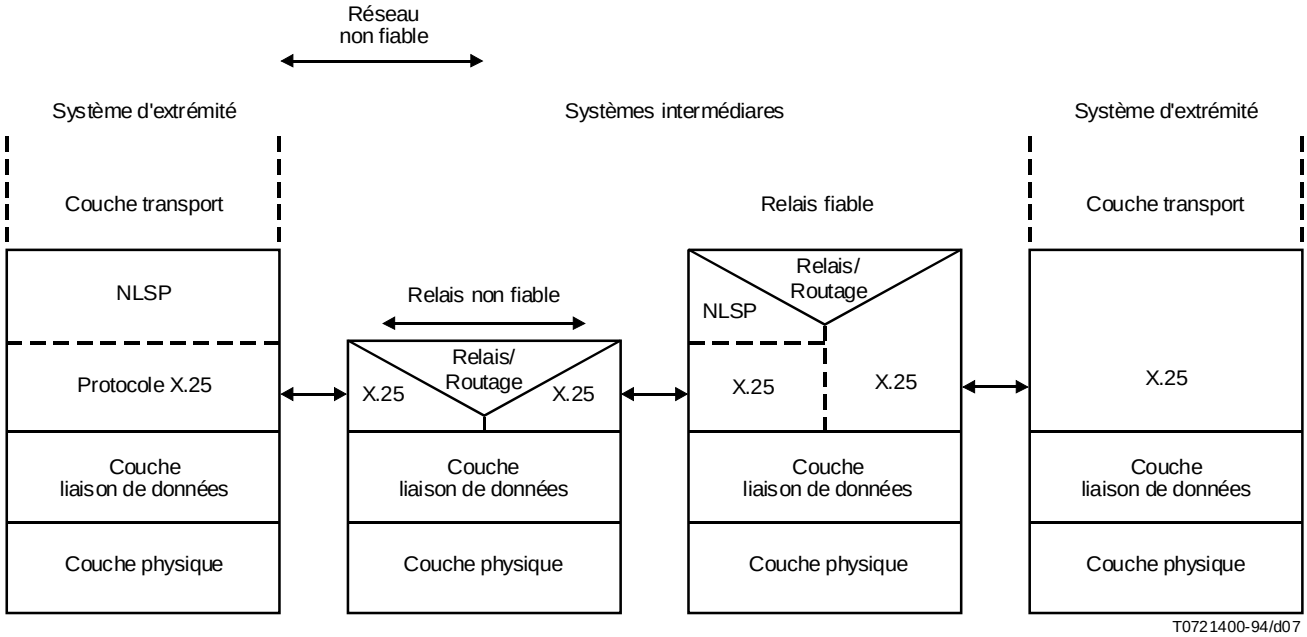
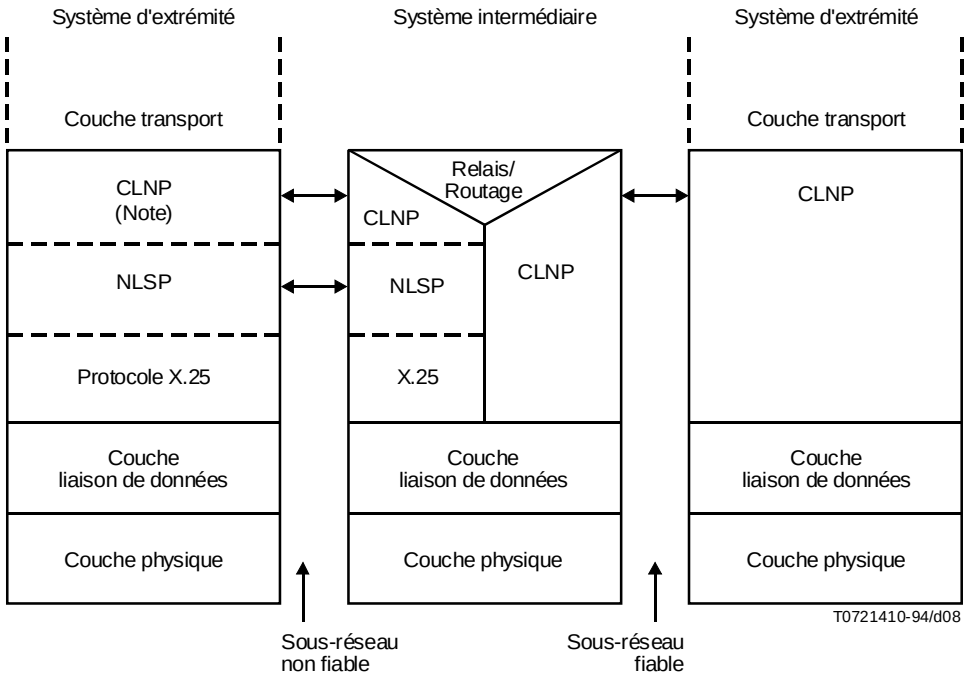


Figure 8 – Illustration du protocole NLSP en mode connecté avec un système relais non fiable



NOTE – Y compris la fonction de convergence avec le mode connecté.

Figure 9 – Illustration du protocole NLSP dans un environnement multi-réseaux

D'autres positionnements non inclus dans ce modèle sont aussi possibles.

Les échanges de protocoles de routage inter-domaines (IDRP) (*interdomain routing protocol*) (ISO/CEI 10747) peuvent être protégés par un protocole NLSP agissant en dessous du protocole IDRP et par-dessus le protocole CLNP de la Rec. UIT-T X.233 | ISO/CEI 8473-1 (voir Figure 10). Cette configuration assure la protection des unités de données protocolaires (PDU) IDRP.

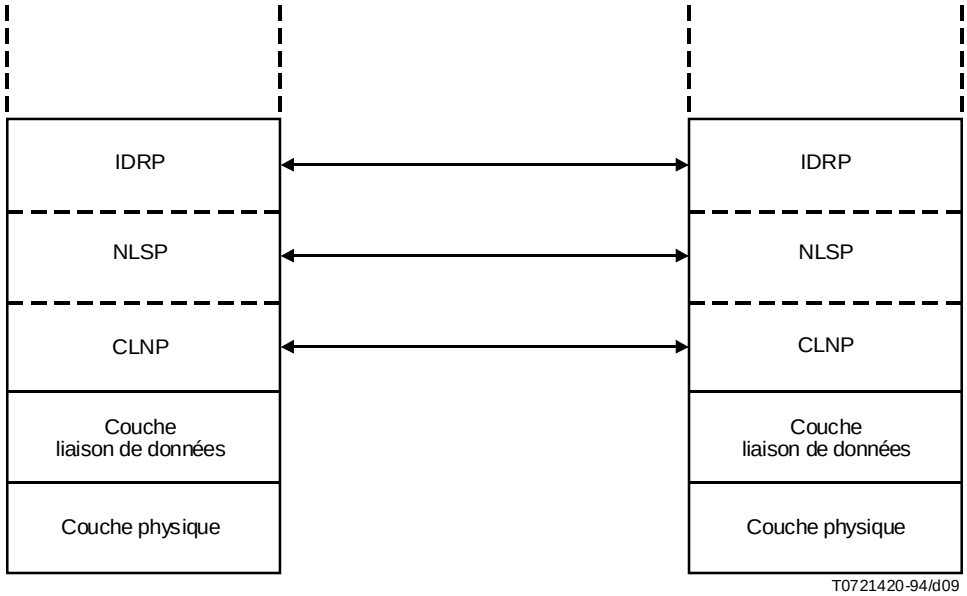


Figure 10 – Illustration du protocole NLSP mis en œuvre avec un protocole IDRP

Une correspondance peut être définie pour les primitives de service du réseau sous-jacent au protocole NLSP vers les services de liaisons de données pour l'utilisation d'un protocole de la couche liaison, tel un protocole de réseau local RZL défini dans l'ISO/CEI 8802 (voir Figure 11).

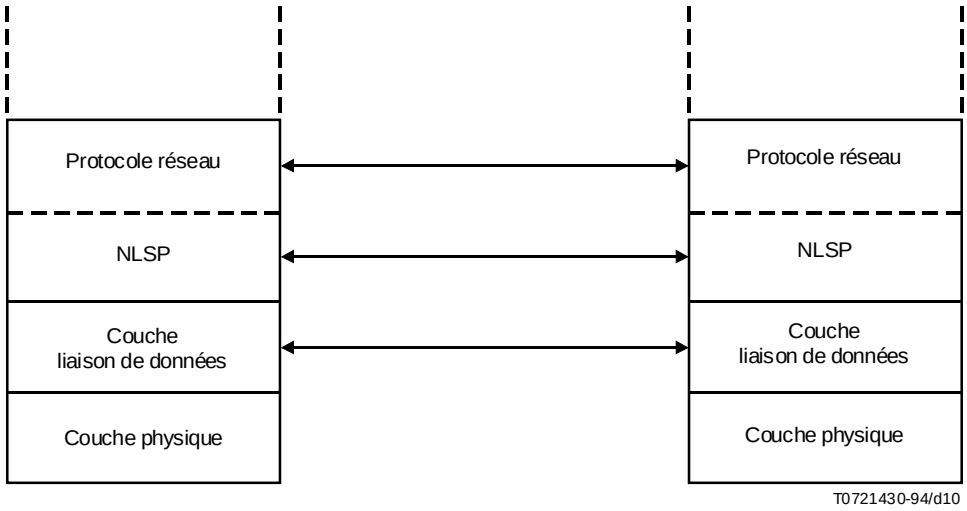


Figure 11 – Illustration du protocole NLSP mis en œuvre par-dessus la couche liaison de données

La Rec. X.800 du CCITT | ISO 7498-2 comporte une prescription de confidentialité dans la couche liaison de données. Il existe un besoin pour un protocole de sécurité de liaison de données pour assurer la protection des communications entre des ponts de couche 2 en environnement de réseau local RZL (voir Figure 12).

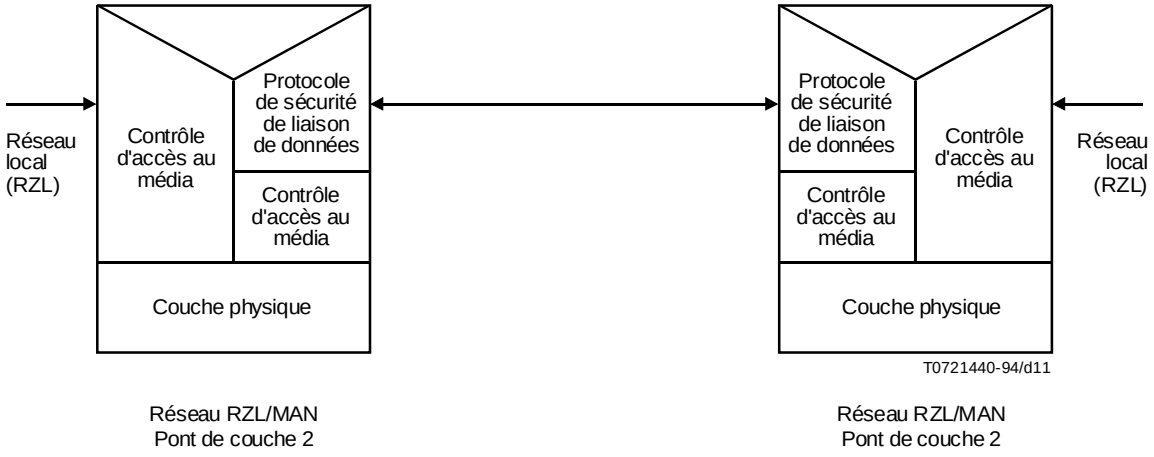


Figure 12 – Illustration du protocole de sécurité de la couche liaison de données utilisé pour protéger les communications entre deux ponts

12 Utilisation des couches (N-1) pour renforcer la sécurité de la couche (N)

Pour assurer des fonctions de sécurité dans une couche donnée, il est possible d'utiliser les services de sécurité fournis par les couches sous-jacentes. Le service de sécurité global fourni à l'utilisateur de la couche (N) peut être construit sur des mécanismes des couches sous-jacentes.

13 Etiquetage de sécurité

Une étiquette de sécurité peut être utilisée pour indiquer les prescriptions choisies des services de sécurité (voir l'article 9), ainsi que pour le contrôle d'accès et de routage.

Au sein d'une association de sécurité, un couple d'entités peut préétablir un ensemble d'étiquettes de sécurité qui pourront être assignées à des unités de données protocolaires en mode connecté ou sans connexion.

L'utilisation des étiquettes de sécurité est défini dans le cadre de la politique de sécurité.

Le cadre général de la sécurité: Partie 3 – Contrôle d'accès décrit l'application des étiquettes de sécurité au contrôle d'accès.

Le premier champ d'une étiquette de sécurité identifiera l'autorité de sécurité qui a défini l'étiquette. L'identificateur sera un identificateur objet (selon la définition ASN.1 de la Rec. X.208 du CCITT | ISO/CEI 8824), codé par les règles de codage de base.

La structure générale des étiquettes de sécurité sera conforme aux travaux du Comité d'études 27 de l'ISO sur les objets informationnels de sécurité.

14 Domaines de sécurité

Les domaines de sécurité, selon la définition de la Rec. UIT-T X.810 | ISO/CEI 10181-1 (cadre général de la sécurité) n'intéressent pas directement les protocoles d'échange entre entités homologues. L'utilisation des domaines devrait plutôt être considérée dans le contexte de gestion de la sécurité.

15 Sécurité du routage

15.1 Le protocole de sécurité de la couche réseau (NLSP) (*network layer security protocol*) (voir Rec. UIT-T X.273 | ISO/CEI 11577) peut être utilisé pour protéger les échanges d'unités de données protocolaires (PDU) de routage inter-domaines (ISO/CEI 10747) (voir aussi l'article 11 concernant le positionnement du protocole IDRP).

15.2 Le protocole NLSP (selon la définition de la Rec X.273 du CCITT | ISO/CEI 11577) ne peut pas être utilisé pour prendre en charge la sécurité des échanges de routage intra-domaines basés sur la ISO/CEI 10589 (système intermédiaire à système intermédiaire IS-IS) et sur ISO/CEI 9542 (système de terminaison à système intermédiaire ES-EI), et ne prend pas en charge les communications à interlocuteurs multiples. On peut définir un protocole normalisé basé sur une extension du protocole NLSP pour assurer la sécurité des protocoles d'échange intra-domaines IS-IS et d'acheminement ES-IS. Tout protocole de ce type devra être indépendant de ces protocoles de routage.

15.3 Il est à noter que le contrôle d'accès appliqué aux communications (par exemple les groupes fermés d'utilisateurs selon la Rec. UIT-T X.25 | ISO/CEI 8208, les étiquettes de sécurité de la Rec. UIT-T X.233 | ISO/CEI 8473-1, le protocole NLSP) peut affecter les routes disponibles. Des informations sur l'état de sécurité des itinéraires peuvent être exigées pour que les informations de routages soient utilisables dans les environnements sécurisés.

15.4 De plus, on doit prendre en considération les prescriptions de routage pour assurer le support du contrôle d'accès et du contrôle de routage.

NOTE – La Rec. X.800 du CCITT | ISO 7498-2 définit le contrôle de routage comme «l'application de règles au cours du processus de routage afin de choisir ou d'éviter des réseaux, liaisons ou relais particuliers». Le contrôle de routage peut, par exemple, être basé sur les adresses et inhiber le routage de toutes les données dans un sous-réseau à l'exception des données originaires d'adresses autorisées. Le contrôle de routage peut aussi être basé sur les étiquettes de sécurité, des paquets étiquetés «confidentiel entreprise» ne devant pas être routés, par exemple, par l'intermédiaire du réseau public.

16 Gestion de la sécurité

16.1 Politique de sécurité

Les informations suivantes sont établies dans le cadre des critères de la politique de sécurité pour sélectionner le service et les mécanismes de sécurité dans une couche (N) pour une entité (N) donnée.

- Critères pour établir les services de sécurité sélectionnés pour une couche (N), notamment les niveaux minimaux et maximaux acceptables.
- Critères pour associer les services de sécurité sélectionnés aux mécanismes et aux spécifications de protection qui en découlent (c'est-à-dire, les règles de sécurité décrites dans l'article 10).

Là où des étiquettes de sécurité sont utilisées, ces informations sont établies dans le cadre de la politique de sécurité pour l'utilisation des étiquettes de sécurité (voir l'article 13).

Les informations sont établies dans le cadre de la politique de sécurité pour vérifier les aspects liés à la sécurité dans les protocoles des couches, et pour assurer les rétablissements.

16.2 Gestion des associations se sécurité

La gestion des associations de sécurité est examinée dans l'article 5.

16.3 Gestion des clés

La distribution et la sélection des clés peut être réalisée d'une des façons suivantes:

a) dans le cadre de l'établissement de l'association de sécurité;

b) dans le cadre d'un protocole de sécurité; ou

c) par des mécanismes sortant du cadre des couches inférieures de l'OSI.

16.4 Vérifications de sécurité

La collecte et l'analyse des informations de vérification de sécurité sont décrites dans le cadre général de la sécurité, partie 7: Vérifications de Sécurité (future Norme ISO/CEI 10181-7).

17 Confidentialité du flux de trafic

Le traitement du remplissage de trafic n'est pas bien maîtrisé. Dans l'environnement du service réseau en mode connexion (CONS), trois types de remplissage peuvent être associés à la confidentialité du flux de trafic:

a) remplissage de PDU sécurisées existantes;

b) génération de PDU sécurisées muettes;

c) génération de connexions muettes avec d'autres entités homologues de protocole NLSP.

Pour chaque type de remplissage, il y a des paramètres potentiels à définir (par exemple, toutes les PDU doivent avoir une longueur de 1024 octets; une PDU doit être transmise sur la connexion toutes les 500 millisecondes; lorsqu'une certaine entité de protocole NLSP établit une connexion avec une entité homologue particulière, six autres entités données doivent aussi être connectées et le même volume de trafic doit être échangé avec elles). Ces paramètres ne sont pas bien compris mais, dans les deux premiers cas de remplissage, ils doivent être inclus au sein de l'association de sécurité. Il s'ensuit qu'un attribut booléen n'est pas adapté. Un complément d'étude s'impose pour les types de paramètres requis.

18 Directives pour la définition des attributs d'association de sécurité

Un attribut d'association de sécurité est un élément d'information nécessaire pour contrôler la sécurité de communication et les homologues distants. Trois différentes classes d'attributs d'association de sécurité sont décrites à l'article 5.

Les attributs d'association de sécurité nécessaires au contrôle d'un protocole de sécurité sont définis dans le cadre du protocole de sécurité. Cette définition doit inclure:

a) un mnémonique utilisé pour se référer à l'attribut dans le protocole de sécurité;

b) le type de données de l'attribut;

c) une description de la sémantique de l'attribut;

d) une description de la façon dont la valeur de l'attribut est calculée.

Beaucoup des attributs nécessaires à un protocole de sécurité dépendront des mécanismes pris en charge.

Les descriptions suivantes sont des exemples de définition d'attributs d'association de sécurité:

Encipher: Booléen

Le chiffrement est utilisé pour assurer la confidentialité

La valeur de cet attribut est définie par un ensemble convenu de règles de sécurité en fonction des services de sécurité sélectionnés.

Enc_Alg: Identificateur d'objet attribué conformément à ISO 9979

Algorithme de chiffrement

La valeur de cet attribut est définie par un Ensemble convenu de règles de sécurité, en fonction des services de sécurité sélectionnés.

Enc_Key: Forme définie par l'ensemble convenu de règles de sécurité

Clé de chiffrement

Valeur donnée par la procédure d'établissement de l'association de sécurité.

19 Traitement d’erreurs

Les actions à entreprendre quand une erreur intervient dans un protocole de sécurité seront déterminées par la politique de sécurité locale. Elles peuvent consister à:

– ignorer la PDU erronée;

– émettre une PDU d'erreur;

– lancer une procédure de réinitialisation ou de déconnexion;

– établir un rapport de vérification.

Annexe A

Exemple d'ensemble convenu de règles de sécurité

(Cette annexe fait partie intégrante de la présente Recommandation | Rapport technique)

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