UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T T.123

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(05/99)

SÉRIE T: TERMINAUX DES SERVICES TÉLÉMATIQUES

Piles de protocoles de données propres au réseau pour conférences multimédias

Recommandation UIT-T T.123

(Antérieurement Recommandation du CCITT)

RECOMMANDATION UIT-T T.123

PILES DE PROTOCOLES DE DONNEES PROPRES AU RESEAU POUR CONFERENCES MULTIMEDIAS

Résumé

La présente Recommandation spécifie les aspects réseau de la série T.120 de protocoles de transmission de données pour service de conférences multimédias. Les réseaux actuellement identifiés sont le RNIS, le RDCC, le RDCP, le RTPC, le RNIS-LB et les LAN. Elle spécifie des profils de communication qui assurent des connexions point à point fiables entre un terminal et une unité de commande multipoint, entre deux terminaux ou entre deux unités de commande multipoint (MCU, *multipoint control unit*). Dans certains cas, une couche inférieure du protocole permet le multiplexage de signaux audio et vidéo en plus des connexions de données. Dans d'autres cas, on peut établir des communications distinctes, sur le même réseau ou sur un réseau différent, pour acheminer des signaux audio ou vidéo.

L'Annexe B spécifie en outre un protocole qui peut être utilisé pour négocier des services de connexion allant au-delà du transfert fiable de données. Ce protocole permet également l'utilisation d'une liste d'adresses d'alias lors de l'établissement de la connexion. Les listes d'alias permettront de créer et d'utiliser des services de serveur de proximité (proxy) pour des communications T.120.

Source

La Recommandation UIT-T T.123, révisée par la Commission d'études 16 de l'UIT-T (1997-2000), a été approuvée le 27 mai 1999 selon la procédure définie dans la Résolution n° 1 de la CMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la CMNT.

Dans certains secteurs des technologies 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.

NOTE

Dans la présente Recommandation, le terme *exploitation reconnue (ER)* désigne tout particulier, toute entreprise, toute société ou tout organisme public qui exploite un service de correspondance publique. Les termes *Administration*, *ER* et *correspondance publique* sont définis dans la *Constitution de l'UIT (Genève, 1992)*.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2000

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT.

TABLE DES MATIÈRES

Recommandation T.123

PILES DE PROTOCOLES DE DONNEES PROPRES AU RESEAU POUR CONFERENCES MULTIMEDIAS

(révisée en 1999)

1 Domaine d'application

La présente Recommandation, qui définit des piles protocolaires pour terminaux et pour unités de commande multipoint (ou unités MCU), spécifie les aspects propres au réseau de la suite de protocoles T.120, sous la forme de profils pour chacun des réseaux identifiés. Chaque profil spécifie un ensemble de protocoles qui peut aller jusqu'à la couche 4 du modèle de référence OSI.

Les raisons d'être de la présente Recommandation sont les suivantes: les conférences audiographiques et vidéographiques sont destinées à faire partie de l'ensemble des services intégrés dans les RNIS. Le service de téléconférence sur RNIS comporte l'intégration de supports de transmission multiples (audio, vidéo et données) dans une connexion qui peut être constituée par la réunion de plusieurs voies physiques. La fourniture de ces services n'est toutefois pas limitée aux RNIS et une série d'autres scénarios de réseau a été identifiée. A titre d'exemple, le RDCC peut assurer un service similaire à celui du RNIS, quoique moins souple et le RTPC peut assurer un service qui, bien que limité en performance, est plus facile à obtenir. La téléconférence peut aussi se prolonger sur un RDCP ou sur un RNIS-LB. Les LAN peuvent assurer des conférences locales dans le cadre d'une entreprise ou un moyen d'accès à des réseaux de zone étendue.

1.1 Réseaux identifiés

Des profils de réseau spécifiques sont définis pour le RNIS, le RDCC, le RDCP et le RTPC, comme le prescrit la Recommandation F.710. Le domaine d'application de la présente Recommandation comporte également le RNIS-LB et les LAN.

1.2 Signaux audio et vidéo

Le traitement des signaux audio et vidéo au cours d'une téléconférence multimédia ne fait pas partie de la présente Recommandation sauf en ce qui concerne la possibilité de leur transport multiplexé par la même connexion, le cas échéant.

1.3 Etablissement d'un appel RNIS

L'Appendice I contient des exemples de procédures d'établissement d'un appel RNIS pour la téléconférence multimédia. Ces procédures illustrent:

a) l'utilisation d'éléments d'information RNIS;

b) la coordination des canaux D et B;

c) les phases d'établissement de la connexion;

d) l'interfonctionnement avec les services téléphoniques.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui de ce fait en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte

étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

– Recommandation UIT-T F.702 (1996), *Services de conférence multimédia*.

– Recommandation UIT-T H.221 (1997), *Structure de trame pour un canal d'un débit de 64 à 1920 kbit/s pour les téléservices audiovisuels*.

– Recommandation UIT-T H.222.0 (1995) | ISO/CEI 13818-1:1996, *Technologies de l'information – Codage générique des images animées et du son associés: systèmes*.

– Recommandation UIT-T H.222.0 (1995)/Amd.1 (1996) | ISO/CEI 13818-1:1996/ Amd.1:1997, *Technologies de l'information – Codage générique des images animées et du son associés – Amendement 1: Enregistrement des identificateurs de droit d'auteur*.

– Recommandation UIT-T H.222.0 (1995)/Amd.2 (1996) | ISO/CEI 13818-1:1996/ Amd.2:1997, *Technologies de l'information – Codage générique des images animées et du son associés – Amendement 2: Enregistrement des identificateurs de format*.

– Recommandation UIT-T H.223 (1996), *Protocole de multiplexage pour communications multimédias à faible débit*.

– Recommandation UIT-T H.230 (1997), *Signaux de commande et d'indication synchrones de la trame pour les systèmes audiovisuels*.

– Recommandation UIT-T H.231 (1997), *Unités de commande multipoint pour les systèmes audiovisuels utilisant des canaux numériques fonctionnant à des débits inférieurs ou égaux à 1920 kbit/s*.

– Recommandation UIT-T H.233 (1995), *Système de confidentialité pour les services audiovisuels*.

– Recommandation UIT-T H.242 (1997), *Procédures pour l'établissement de communications entre terminaux audiovisuels sur des canaux numériques d'un débit allant jusqu'à 2 Mbit/s*.

– Recommandation UIT-T H.243 (1997), *Procédures pour l'établissement de communications entre trois terminaux audiovisuels ou plus sur des canaux numériques à débit allant jusqu'à 1920 kbit/s*.

– Recommandation UIT-T H.310 (1998), *Systèmes et terminaux de communication audiovisuels à large bande*.

– Recommandation UIT-T H.320 (1997), *Systèmes et équipements terminaux visiophoniques à bande étroite*.

– Recommandation UIT-T H.324 (1998), *Terminal pour communication multimédia à faible débit*.

– Recommandation UIT-T I.320 (1993), *Modèle de référence du protocole RNIS*.

– Recommandation CCITT I.321 (1991), *Modèle de référence pour le protocole du RNIS large bande et son application*.

– Recommandation UIT-T I.361 (1999), *Spécifications de la couche mode de transfert asynchrone pour le RNIS à large bande*.

– Recommandation UIT-T I.363.1 (1996), *Spécification de la couche d'adaptation ATM du RNIS-LB: AAL de type 1*.

– Recommandation UIT-T I.363.3 (1996), *Spécification de la couche d'adaptation ATM du RNIS-LB: AAL de type 3/4*.

– Recommandation UIT-T I.363.5 (1996), *Spécification de la couche d'adaptation ATM du RNIS-LB: AAL de type 5*.

– Recommandation UIT-T I.365.1 (1993), *Sous-couches de la couche d'adaptation ATM du RNIS-LB: sous-couche de convergence spécifique au service de relais de trames*.

– Recommandation UIT-T I.365.3 (1995), *Sous-couches de la couche d'adaptation ATM du RNIS-LB: fonction de coordination propre au service pour la fourniture du service de transport en mode connexion*.

– Recommandation UIT-T I.430 (1995), *Interface au débit de base usager-réseau – Spécification de la couche 1*.

– Recommandation UIT-T I.431 (1993), *Interface à débit primaire usager-réseau – Spécification de la couche 1*.

– Recommandation UIT-T I.432.1 (1999), *Interface utilisateur-réseau du RNIS-LB – Spécification de la couche Physique: caractéristiques générales*.

– Recommandation UIT-T I.432.2 (1999), *Interface utilisateur-réseau du RNIS-LB – Spécification de la couche Physique*: *exploitation à 155 520 k/bits et 622 080 kbit/s*.

– Recommandation UIT-T I.432.3 (1999), *Interface utilisateur-réseau du RNIS-LB – Spécification de la couche Physique*: *exploitation à 1544 kbit/s et 2048 kbit/s*.

– Recommandation UIT-T I.432.4 (1999), *Interface utilisateur-réseau du RNIS-LB – Spécification de la couche Physique*: *exploitation à 51 840 kbit/s*.

– Recommandation UIT-T Q.920 (1993), *Couche liaison de données à l'interface usager-réseau RNIS – Aspects généraux*.

– Recommandation UIT-T Q.921 (1997), *Interface usager-réseau du RNIS – Spécification de la couche de liaison de données*.

– Recommandation UIT-T Q.921 *bis* (1993), *Suite de tests abstraits pour les tests de conformité pour les procédures d'accès à la liaison sur le canal D*.

– Recommandation CCITT Q.922 (1992), *Spécification de la couche liaison de données RNIS pour les services supports en mode trame*.

– Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base*.

– Recommandation UIT-T Q.933 (1995), *Spécification de la signalisation pour la commande et la surveillance de l'état des connexions virtuelles commutées et permanentes en mode trame*.

– Recommandation UIT-T Q.2110 (1994), *Couche d'adaptation ATM du RNIS-LB – Protocole en mode connexion propre au service*.

– Recommandation UIT-T Q.2130 (1994), *Couche d'adaptation du mode de transfert asynchrone de signalisation dans le RNIS à large bande – Fonction de coordination propre au service pour la signalisation à l'interface utilisateur-réseau*.

– Recommandation UIT-T Q.2931 (1995), *Système de signalisation d'abonné numérique n° 2 – Spécification de la couche 3 de l'interface utilisateur-réseau pour la commande de connexion/appel de base*.

– Recommandation UIT-T Q.2931/Amd.1 (1997), *Système de signalisation d'abonné numérique n° 2 – Spécification de la couche 3 de l'interface utilisateur-réseau pour la commande de connexion/appel de base*.

– Recommandation CCITT T.90 (1992), *Caractéristiques et protocoles des terminaux applicables aux services de télématique dans le RNIS.*

– Recommandation UIT-T T.120 (1996), *Protocoles de données pour conférence multimédia*.

– Recommandation UIT-T T.122 (1998), *Service de communication multipoint – Définition du service*.

– Recommandation UIT-T T.124 (1998), *Commande générique de conférence*.

– Recommandation UIT-T T.125 (1998), *Spécification du protocole du service de communication multipoint.*

– Recommandation UIT-T T.126 (1997), *Protocole du service multipoint d'imagerie fixe et d'annotation*.

– Recommandation UIT-T T.127 (1995), *Protocole de transfert multipoint de fichiers binaires*.

– Recommandation CCITT V.7 (1988), *Définitions des termes relatifs aux communications de données sur le réseau téléphonique*.

– Recommandation UIT-T V.8 (1998), *Procédures de démarrage des sessions de transmission de données sur le réseau téléphonique public commuté*.

– Recommandation UIT-T V.8 *bis* (1996), *Procédures d'identification et de sélection des modes de fonctionnement communs entre ETCD et entre ETTD sur le réseau téléphonique public commuté et sur les circuits loués point à point de type téléphonique*.

– Recommandation UIT-T V.14 (1993), *Transmission de caractères arythmiques sur des voies supports synchrones*.

– Recommandation UIT-T V.34 (1998), *Modem fonctionnant à des débits allant jusqu'à 33 600 bit/s pour usage sur le réseau téléphonique général commuté et sur les circuits à 2 fils de type téléphonique loués point à point*.

– Recommandation UIT-T V.42 (1996), *Procédures de correction d'erreur pour les équipements de terminaison de circuits de données utilisant la conversion asynchrone/synchrone*.

– Recommandation CCITT V.42 *bis* (1990), *Procédures de compression des données pour les équipements de terminaison du circuit de données (ETCD) utilisant des procédures de correction d'erreur*.

– Recommandation UIT-T V.61 (1996), *Modem voix plus données simultanées fonctionnant à un débit voix plus données de 4800 bit/s avec commutation automatique optionnelle à des débits de données uniquement allant jusqu'à 14 400 bit/s, à utiliser sur le réseau téléphonique général commuté et sur les circuits téléphoniques 2 fils loués point à point*.

– Recommandation UIT-T V.70 (1996), *Procédures pour la transmission simultanée de données et de signaux vocaux à codage numérique sur le réseau téléphonique général commuté et sur les circuits téléphoniques à deux fils point à point loués*.

– Recommandation UIT-T V.120 (1996), *Prise en charge par un RNIS d'un équipement terminal de traitement de données muni d'interfaces de type série V permettant un multiplexage statistique*.

– Recommandation CCITT X.21 (1992), *Interface entre l'équipement terminal de traitement de données et l'équipement de terminaison du circuit de données pour fonctionnement synchrone dans les réseaux publics pour données*.

– Recommandation CCITT X.21 bis (1988), *Utilisation, sur les réseaux publics pour données, d'équipements terminaux de traitement de données (ETTD) destinés à assurer l'interface des modems synchrones de la série V.*

– Recommandation UIT-T X.25 (1996), *Interface entre équipement terminal de traitement de données et équipement de terminaison de circuit de données pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données.*

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

– Recommandation UIT-T X.213 (1995) | ISO/CEI 8348:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service de réseau*.

– Recommandation UIT-T X.214 (1995) | ISO/CEI 8072:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service de transport*.

– Recommandation UIT-T X.224 (1995) | ISO/CEI 8073:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole assurant le service de transport en mode connexion*.

– ISO/CEI 3309:1993, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Procédures de commande de liaison de données à haut niveau (HDLC) – Structure de trame*.

– ISO/CEI 7776:1995, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Procédures de commande de liaison de données de haut niveau – Description des procédures de liaison de données ETTD compatibles X.25 LAPB.*

– ISO/CEI 8208:1995, *Technologies de l'information – Communication de données – Protocole X.25 de couche paquet pour terminal de données*.

– ISO/CEI TR 8802-1:1997, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Exigences spécifiques – Partie 1: Vue d'ensemble des normes de réseaux locaux.*

3 Définitions

La présente Recommandation utilise les termes suivants, qui sont définis dans la Recommandation F.701:

– service de conférence audiographique;

– unité de commande multipoint.

La présente Recommandation utilise les termes suivants, qui sont définis dans la Recommandation I.320:

– plan de commande;

– plan utilisateur.

La présente Recommandation utilise le terme suivant, qui est défini dans la Recommandation Q.920:

– identificateur de connexion de liaison de données.

La présente Recommandation utilise le terme suivant, qui est défini dans la Recommandation Q.922:

– fonction de synchronisation et de convergence.

La présente Recommandation utilise le terme suivant, qui est défini dans la Recommandation V.7:

– transmission arythmique.

La présente Recommandation utilise le terme suivant, qui est défini dans les Recommandations X.213 et X.214:

– qualité de service.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AAL	couche d'adaptation ATM (*ATM adaptation layer*)
AL	couche d'adaptation (*adaptation layer*)
ATM	mode de transfert asynchrone (*asynchronous transfer mode*)
CPCS	sous-couche de convergence de partie commune (*common part convergence sublayer*)
DLCI	identificateur de connexion de liaison de données (*data link connection identifier*)
ETCD	équipement de terminaison de circuit de données
ETTD	équipement terminal de traitement de données
FCS	séquence de contrôle de trame (*frame check sequence*)
LAN	réseau local (*local area network*)
MCS	service de communication multipoint (*multipoint communication service*)
MCSAP	point d'accès au service MCS (*MCS service access point*)
MCU	unité de commande multipoint (*multipoint control unit*)
NSAP	point d'accès pour le service de réseau (*network service access point*)
OSI	interconnexion des systèmes ouverts (*open systems interconnection*)
PDU	unité de données protocolaire (*protocol data unit*)
PES	flux élémentaire paqueté (*packetized elementary stream*)
QS	qualité de service
RDCC	réseau pour données à commutation de circuits
RDCP	réseau pour données à commutation par paquets
RNIS	réseau numérique à intégration de services
RNIS-LB	réseau numérique à intégration de services à large bande
RTPC	réseau téléphonique public commuté
SCF	fonction de synchronisation et de convergence (*synchronization and convergence function*)
SDU	unité de données de service (*service data unit*)

TPDU unité de données protocolaire de transport (*transport protocol data unit*)

TSAP point d'accès au service de transport (*transport service access point*)

VC voie virtuelle (*virtual channel*)

5 Configuration multipoint

Une configuration multipoint est créée par des connexions de réseau point à point entre trois terminaux ou plus et une unité MCU. La Figure 1 représente une configuration type, dans laquelle des terminaux sont raccordés en étoile multipoint autour de chaque unité MCU. Cette figure montre en outre comment des unités MCU peuvent être interconnectées de manière à élargir la conférence.

La Figure 2 représente le cadre de la suite de protocoles T.120. La présente Recommandation définit les protocoles spécifiques de réseau pour toute connexion directe entre un terminal et une unité MCU, entre deux terminaux ou entre deux unités MCU.

Les connexions point à point à une même unité MCU peuvent ne pas avoir des profils de communication identiques. L'exploitation de la couche protocolaire du service MCS permet la communication entre réseaux différents.

Si deux terminaux n'ont pas de profil commun, ils ne peuvent pas être connectés directement l'un à l'autre. Dans ce cas, une unité MCU peut servir d'intermédiaire pour rendre la communication possible. Il s'agit d'un cas particulier d'une configuration multipoint.

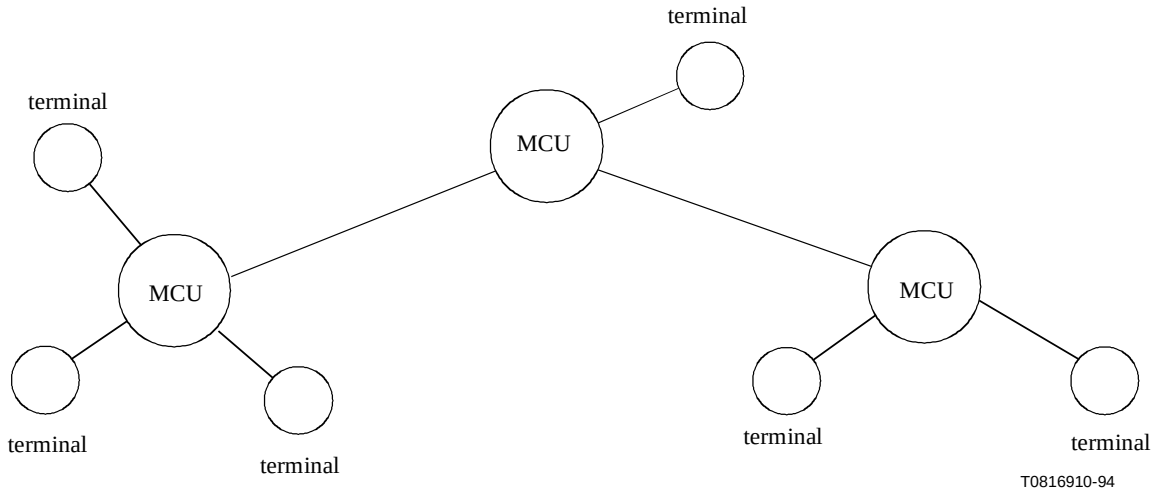


Figure 1/T.123 – Configuration multipoint type

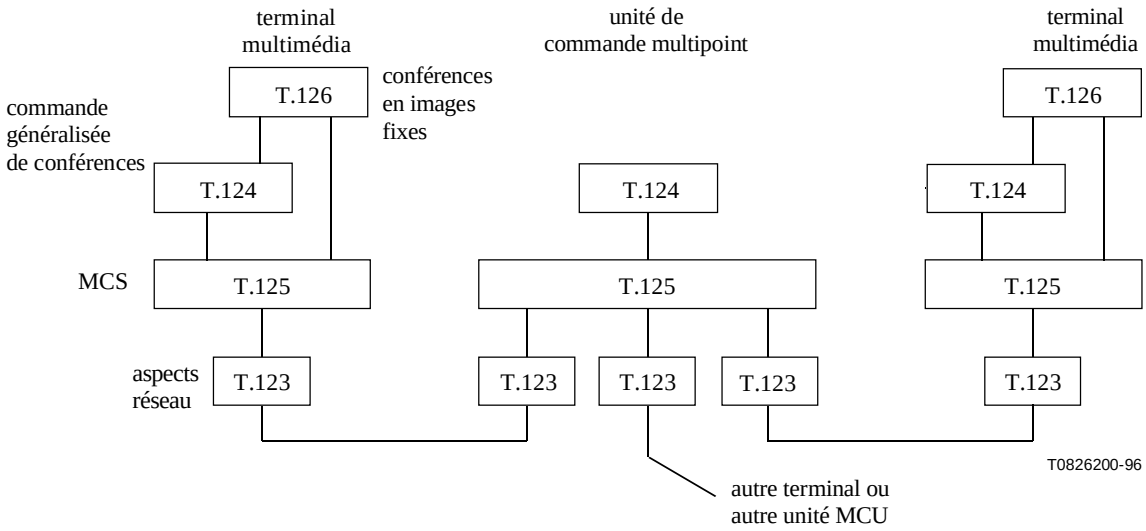


Figure 2/T.123 – Cadre général de la suite de protocoles T.120

6 Aperçu général des profils

La Figure 3 présente la structure générale des profils spécifiques du réseau. Ces profils sont définis en détail dans les paragraphes suivants.

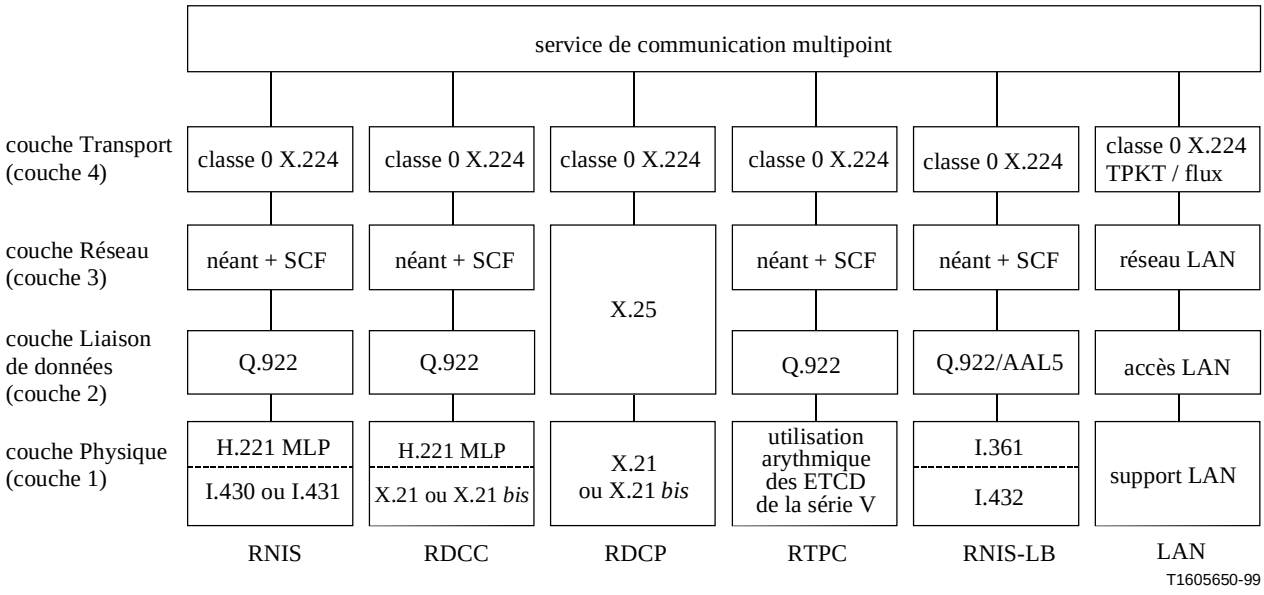


Figure 3/T.123 – Structure générale des profils de base

NOTE 1 – L'utilisation des fonctions de la Recommandation Q.922 sur le RNIS n'implique pas l'utilisation d'un service support à relais de trames. Les fonctions de la Recommandation Q.922 sont utilisées pour améliorer la qualité de service offerte par la couche Physique d'un RNIS, d'un RDCC, d'un RTPC ou d'un RNIS-LB. La présente Recommandation utilise les mécanismes de reprise sur erreur du mode multitrame acquitté de la Recommandation Q.922 afin d'exploiter une ou plusieurs liaisons de données sur une connexion point à point fournie par le réseau correspondant.

Le service requis des couches inférieures par le service MCS est le transfert fiable, séquentiel, à débit commandé d'unités de données d'une longueur quelconque. Une connexion de service MCS se

compose d'une à quatre connexions de transport. Leur nombre dépend de celui des priorités de transfert de données implémentées distinctement dans le service MCS.

Le multiplexage dans une couche inférieure du protocole permet d'obtenir plusieurs connexions de transport à partir d'une connexion point à point dans un réseau spécifique. Il s'agira de la couche 2 lorsque les fonctions de la Recommandation Q.922 sont utilisées et de la couche 3 lorsqu'un protocole Recommandation X.25 ou LAN sera utilisé.

La Figure 4 montre l'emplacement d'un fournisseur de service MCS dans le modèle de référence OSI. Un fournisseur de service MCS échange des unités de données protocolaires MCS avec des fournisseurs de service MCS distants. Il utilisera à cette fin des services de la couche Transport. Un fournisseur de service MCS communique avec les utilisateurs de ce service par l'intermédiaire de primitives MCS (définies dans la Recommandation T.122) passant par un point MCSAP.

Pour simplifier les informations d'adressage qui doivent toujours être fournies lors de l'établissement d'une connexion MCS, il est recommandé que les terminaux et les unités MCU soient gérés de manière qu'une valeur "néant" des sélecteurs de points NSAP et TSAP assure le relais jusqu'à un fournisseur de service MCS par défaut, situé dans le système de destination.

Cela n'exclut pas la possibilité qu'un sélecteur spécifique soit requis pour atteindre un fournisseur de service MCS dans un contexte particulier. Cela peut, par exemple, être le cas si la connexion de données doit être associée à une connexion audio ou vidéo établie indépendamment. Cela peut également être le cas si la connexion MCS sert à constituer une conférence implantée dans une partition d'une grande unité MCU. Théoriquement, le sélecteur spécifique à utiliser sera indiqué dynamiquement par un nœud antérieur quelconque.

NOTE 2 – Un sélecteur de point NSAP peut être indiqué dans la partie propre au domaine d'une adresse de point NSAP. Le format de cette indication n'est pas normalisé.

NOTE 3 – Dans chacun des profils spécifiés ici, le protocole de couche Transport est celui de la Recommandation X.224. Ce protocole achemine les sélecteurs de point TSAP sous la forme de paramètres d'identification TSAP-ID contenus dans les unités TPDU d'établissement de la connexion.

NOTE 4 – L'Annexe B spécifie les profils qui seront utilisés pour l'établissement de connexions de transport étendues T.120.

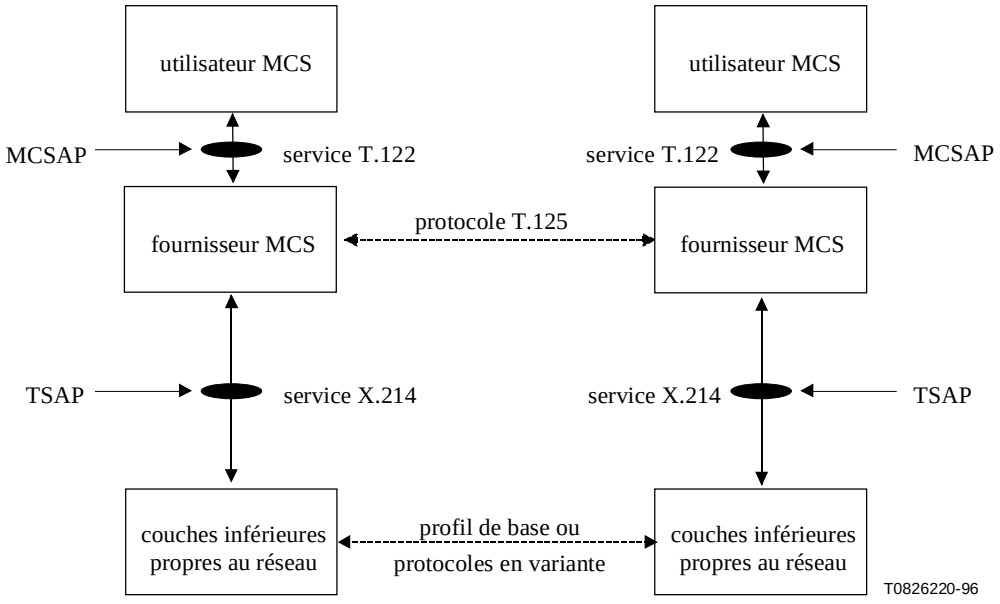


Figure 4/T.123 – Emplacement d'un fournisseur de service MCS dans le modèle de référence OSI

7 Profils de base

Lorsque des protocoles d'établissement d'appel ou des données audio et vidéo apparaissent dans les profils ci-après, ces éléments ne visent qu'à faciliter la compréhension. Ils ne représentent pas une partie normative de la présente Recommandation.

7.1 Profil de base RNIS

La Figure 5 définit le profil de base RNIS.

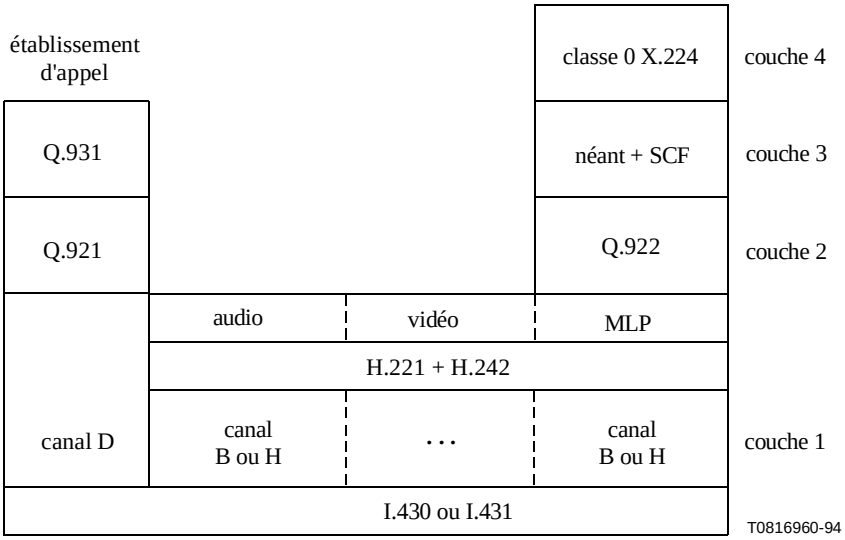


Figure 5/T.123 – Profil de base RNIS

Couche 4

– X.224.

– Classe 0 préférée; aucune classe en variante.

– La dimension maximale des unités TPDU ne doit pas dépasser la valeur du paramètre N201 de la couche 2.

Couche 3

– Plan d'usager: "néant" (aucun protocole supplémentaire au cours de transfert des données).

– Plan de commande: fonction SCF comme spécifié par le paragraphe 9.

Couche 2

– Q.922.

– Paramètres et options de protocole comme spécifié par le paragraphe 10 "Paramètres et options du protocole Q.922".

Couche 1

Sous-couche formée par les canaux en protocole multicouche MLP selon la Recommandation H.221:

• comme spécifié par le paragraphe 12, sous-couche constituée de canaux MLP H.221.

Sous-couche formée par le RNIS:

• 1 à 6 canaux B, ou 1 à 5 canaux H0, ou 1 canal H1;

• informations numériques sans restriction, sur option avec tonalités et annonces;

- canaux B pouvant être adaptés au débit de 56 kbit/s pour les réseaux restreints;
- utilisation du canal D pour la seule signalisation du réseau et non pour acheminer des données d'utilisateur.

NOTE – La présente Recommandation ne spécifie pas l'établissement d'appel dans le RNIS (bien que des exemples de scénarios possibles soient présentés dans l'Appendice I). La fonction SCF représentée ici ne fonctionne que dans le canal MLP, une fois que l'établissement d'appel dans le RNIS et la commutation en mode H.242 ont eu lieu.

7.2 Profil de base RDCC

La Figure 6 définit le profil de base RDCC. Les couches supérieures à la sous-couche H.221 seront identiques au profil de base RNIS.

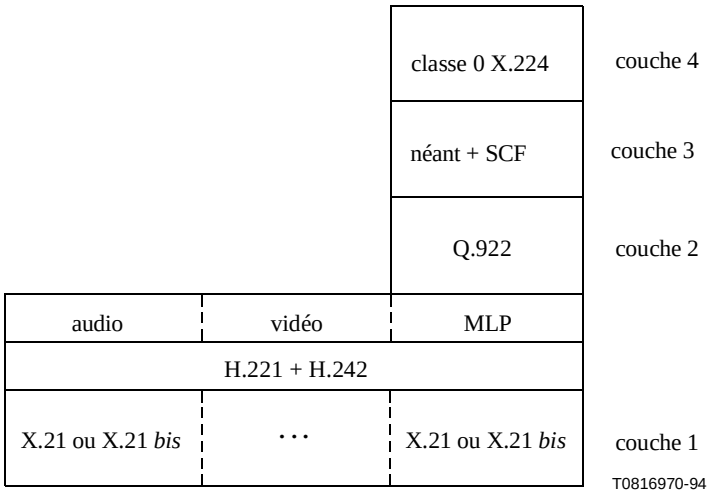


Figure 6/T.123 – Profil de base RDCC

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 1

Sous-couche formée par les canaux du protocole MLP selon la Recommandation H.221:

- comme spécifié par le paragraphe 12, Sous-couche constituée de canaux MLP H.221.

Sous-couche formée par RDCC:

- trames X.21 ou X.21 *bis* pour chaque connexion à commutation de circuits;
- débits en multiples uniformes de 64 kbit/s ou de 56 kbit/s.

7.3 Profil de base RDCP

La Figure 7 définit le profil de base RDCP.

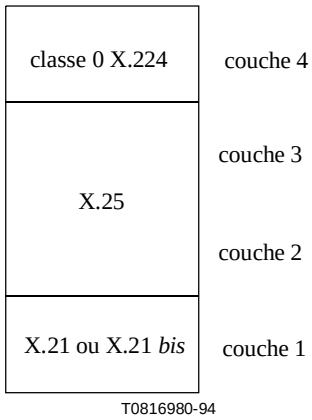


Figure 7/T.123 – Profil de base RDCP

Couche 4

– X.224.

– Classe 0 préférée; aucune classe en variante.

Couche 3

– Service d'appel virtuel X.25.

Couche 2

– Protocole de liaison unique à accès en mode symétrique (LAPB) X.25.

Couche 1

– X.21 ou X.21 *bis.*

7.4 Profil de base RTPC

La Figure 8 définit le profil de base RTPC. Les couches supérieures à la couche Q.922 sont identiques au profil de base RNIS.

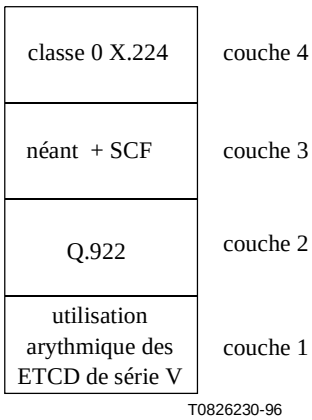


Figure 8/T.123 – Profil de base RTPC

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Q.922.

– Paramètres et options de protocole comme spécifié par le paragraphe 10, Paramètres et options du protocole Q.922.

– Transparence modifiée de structure de trame selon l'ISO/CEI 3309, comme spécifiée au paragraphe 11, Transparence aux structures de trame de la couche Liaison de données pour la transmission arythmique.

Couche 1

– Transmission arythmique par l'équipement terminal de traitement de données (ETTD).

– Un bit de départ, un bit d'arrêt, huit bits de données, pas de parité, en utilisation V.14.

– Utilisation possible de tout ETCD compatible avec la série V et utilisables sur le RTPC.

– Les ETTD et les ETCD peuvent être des fonctions logiques qui ne sont pas séparées physiquement, si l'équipement intégré peut produire les mêmes signaux de transmission.

– Le choix des ETCD selon la série V n'est pas restreint et inclut, par exemple, les modems V.34, V.61 et V.70, avec utilisation facultative des fonctions V.42 et V.42 *bis*. La sélection d'un mode de fonctionnement compatible peut être facilitée par les procédures V.8 ou V.8 *bis*.

NOTE 1 – Si la fonction de correction d'erreur V.42 est activée, les paramètres du système doivent être réglés de façon à éviter une interaction intempestive avec l'opération de correction d'erreur du protocole Q.922. Les éléments importants sont: la temporisation d'acquittement, le nombre maximal d'octets contenus dans un champ d'information et les conditions d'envoi des données.

NOTE 2 – L'efficacité de la compression des données V.42 *bis* variera en fonction de la mesure dans laquelle les données d'application échangées lors d'une conférence auront déjà été comprimées par d'autres moyens.

NOTE 3 – Si les équipements de circuit de données V.70 ont connaissance de l'utilisation de ce profil, ils peuvent alors négocier mutuellement des techniques étendues telles que le tunnel UNERM pour le protocole T.120, tant que le service fourni à l'interface de l'équipement de circuit de données reste une transmission arythmique.

7.5 Profil de base RNIS-LB

La Figure 9 définit le profil de base RNIS-LB. Les couches supérieures à la couche Q.922 sont identiques au profil de base RNIS.

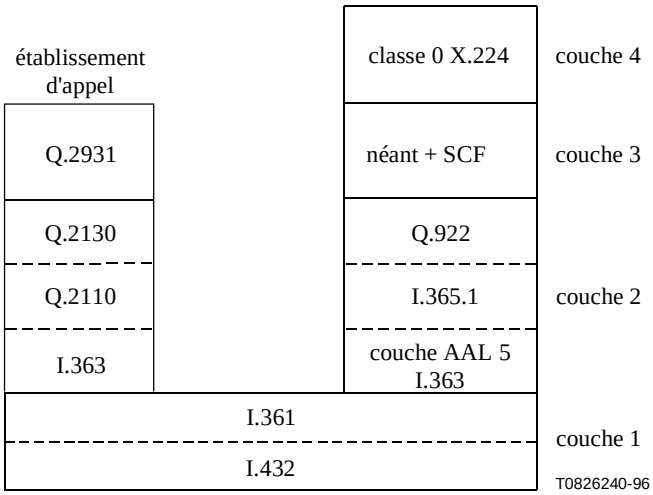


Figure 9/T.123 – Profil de base RNIS-LB

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Q.922.

– Paramètres et options de protocole comme spécifié par le paragraphe 10, Paramètres et options du protocole Q.922.

– Structure d'unité PDU définie dans la Figure 3/I.365.1 (pas d'utilisation de fanions, transparence, ou séquence FCS).

– Octets d'unité PDU acheminés sous forme d'une seule unité CPCS-SDU au moyen de la couche d'adaptation ATM de type 5 (AAL 5).

Couche 1

– voie virtuelle ATM.

7.6 Profil LAN de base

La Figure 10 définit le profil LAN de base.

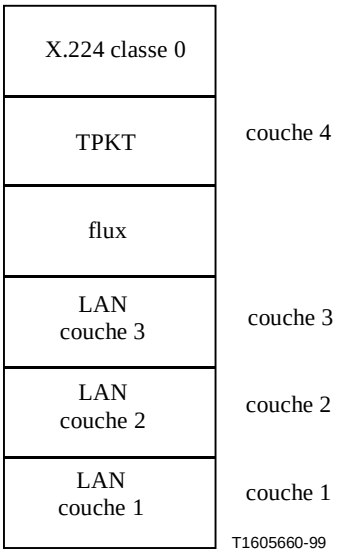


Figure 10/T.123 – Profil LAN de base

Couche 4

– X.224 classe 0 préférée; aucune classe en variante.

– Longueur par défaut des unités TPDU: 65531 octets; mais des valeurs inférieures peuvent être négociées.

– En-tête de paquet TPKT délimitant les unités TPDU comme spécifié par le paragraphe 8, En-tête de paquet délimitant des unités de données dans un flux d'octets.

NOTE 1 – Les paquets TPKT sont requis parce qu'un service de flux d'octets ne marque pas les emplacements des frontières d'unité de données.

– Transfert de flux d'octets avec les caractéristiques suivantes:

  a) service en mode connecté préservant la séquence des octets;

  b) frontières entre unités de données *non* conservées dans le cadre du transfert;

  c) taux d'erreurs résiduel suffisamment faible pour permettre une utilisation comme service réseau de type A;

  d) mécanisme de contrôle de flux permettant d'exercer une action en retour sur l'émetteur.

NOTE 2 – On peut donner, à titre d'exemple commun pour ce qui précède, la spécification de protocole suivante:

  a) Norme RFC 793, *protocole de commande de transmission*;

  b) numéro de port 1503 par défaut, conformément aux *numéros assignés* par la Norme RFC 1700, mais d'autres peuvent être utilisés.

Couche 3

– En général, Normes RFC 791, 792, 919, 922, 950, 1112, protocole Internet.

Couche 2

– En général, l'ISO/CEI 8802: sous-couches de commande de liaison logique et d'accès au média.

Couche 1

– En général, l'ISO/CEI 8802: média physique.

8 En-tête de paquet délimitant des unités de données dans un flux d'octets

La Recommandation X.224 prévoit que les informations soient émises et reçues sous forme d'unités distinctes appelées unités de données de service réseau (NSDU, *network service data unit*) qui peuvent contenir une séquence arbitraire d'octets. Bien que d'autres classes du protocole de transport puissent combiner plusieurs unités TPDU dans le cadre d'une seule unité NSDU, la classe 0 selon la Recommandation X.224 ne fait pas appel à cette possibilité. Dans le contexte des piles protocolaires de la présente Recommandation, une unité TPDU peut donc être identifiée par son unité NSDU sous-jacente.

Une différence fondamentale entre le service de couche Réseau prévu selon la Recommandation X.224 et un service de transfert par flux d'octets, tel que défini au 7.6, est que ce dernier service achemine une séquence continue d'octets, sans limites explicites entre groupes d'octets associés.

Le présent paragraphe spécifie une couche protocolaire distincte qui pallie cette divergence et répond ainsi aux prescriptions de la Recommandation X.224. Il définit un simple format de paquet de transport, dont le rôle est de délimiter les unités TPDU. Chaque paquet, appelé TPKT, est une unité composée d'un nombre entier d'octets, de longueur variable.

Un paquet TPKT se compose de deux parties: un en-tête de paquet, suivi d'une unité TPDU. Le format de l'en-tête de paquet est constant et indépendant du type d'unité TPDU. L'en-tête de paquet se compose de quatre octets, comme représenté sur la Figure 11.

L'octet 1 contient le numéro de version, dont la valeur binaire est 0000 0011. L'octet 2 est réservé pour complément d'étude. Les octets 3 et 4 contiennent le codage binaire sur 16 éléments non signés de la longueur du paquet TPKT. Il s'agit de la longueur totale du paquet exprimée en octets, y compris l'en-tête de paquet et l'unité TPDU.

Etant donné qu'une unité TPDU X.224 occupe au moins 3 octets, la longueur minimale du paquet TPKT est de 7 octets. Sa longueur maximale est de 65535 octets, ce qui permet une longueur maximale d'unité TPDU de 65531 octets.

NOTE – Cette description de la couche protocolaire à paquets TPKT est en accord avec la demande d'observations RFC 1006, *ISO transport service on top of the TCP* [service de transport ISO au-dessus du protocole de commande de transmission (TCP)].

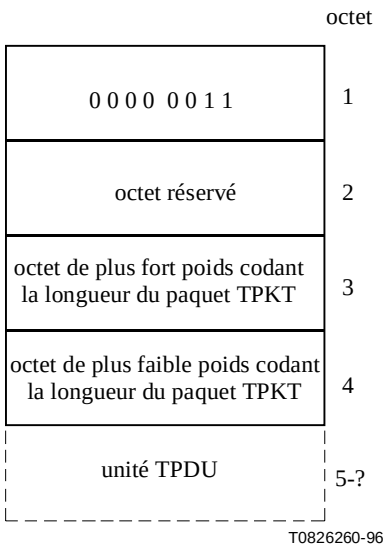


Figure 11/T.123 – Format de l'en-tête de paquet TPKT

9 Fonction de synchronisation et de convergence

9.1 Aperçu général de la fonction SCF

La fonction SCF réside dans la couche Réseau de chaque profil de communication dont la couche Liaison de données est spécifiée comme étant de type Q.922. Cette fonction coordonne l'établissement et la libération des connexions de couche Réseau entre le plan de commande et le plan d'usager, comme décrit au paragraphe 4/Q.922. L'objet de la fonction SCF est de fournir des services de couche Réseau à la couche Transport. La Figure 12 constitue le modèle architectural de la fonction SCF.

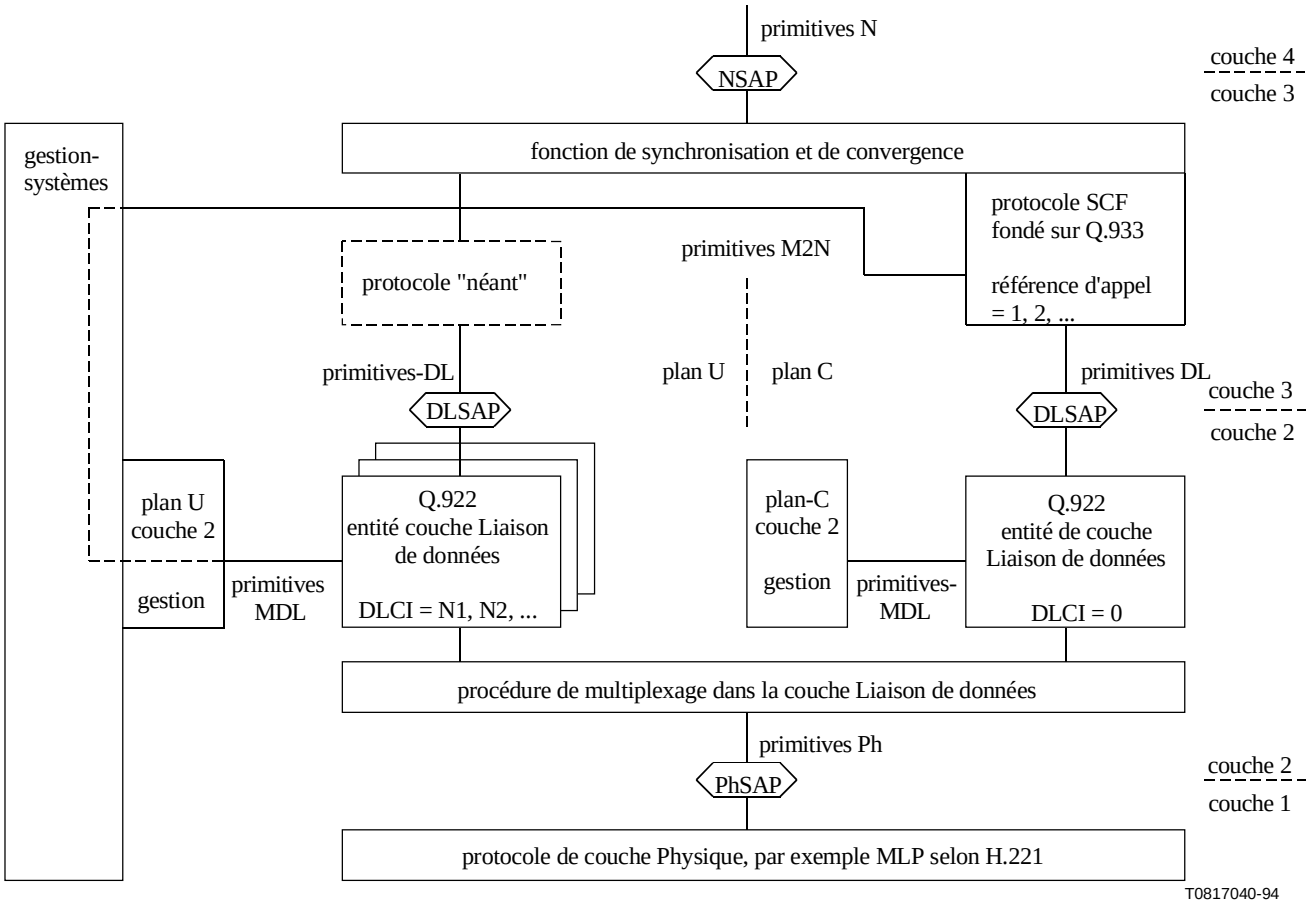


Figure 12/T.123 – Modèle architectural de la fonction SCF

Le Tableau 1 énumère les services de couche Réseau qui sont requis par le protocole de transport X.224. Ce tableau est fondé sur le Tableau 2/X.224, après exclusion des facilités facultatives et de la primitive N-RESET (car celle-ci n'est jamais requise, conformément au Tableau A.3/X.224 et toute indication de réinitialisation du réseau peut être remontée jusqu'au niveau de la primitive N-DISCONNECT).

Tableau 1/T.123 – Services de couche Réseau requis par le protocole X.224

Primitives	Paramètres
demande N-CONNECT indication N-CONNECT	Adresse de l'entité appelée Adresse de l'entité appelante Ensemble des paramètres de QS
réponse N-CONNECT confirmation N-CONNECT	Adresse en réponse Ensemble des paramètres de QS
demande N-DATA indication N-DATA	Données d'utilisateur du service réseau
demande N-DISCONNECT indication N-DISCONNECT	

La fonction SCF implémente les primitives N-CONNECT et N-DISCONNECT. Au cours du transfert des données, cette fonction est inactive et les primitives N-DATA s'appliquent directement sur les primitives DL-DATA sans protocole supplémentaire. Cela implique que la gestion de couche Transport limite la longueur de ses unités TPDU à une seule trame I de structure Q.922.

La Recommandation Q.922 admet des connexions multiples en couche Liaison de données, distinguées par leur identificateur DLCI. Agissant par l'intermédiaire de la gestion de couche 2, la fonction SCF contrôle les affectations d'identificateurs DLCI. Elle communique avec une fonction SCF homologue par l'envoi et la réception de messages en structure Q.933 identifiés par le DLCI 0, qui est réservé à la signalisation dans la voie au profit du plan de commande car il permet la commande par fonction SCF. D'autres identificateurs DLCI sont affectés au plan d'usager car ils permettent le transfert de données.

Les procédures de la fonction SCF sont fondées sur celles qui sont spécifiées dans la Recommandation Q.933, qui définit un cas A d'accès par commutation de circuits à un dispositif de traitement de trames distant et un cas B d'accès intégré à un dispositif local de traitement de trames. L'utilisation, par la fonction SCF, de messages Q.933 peut être considérée comme formant un nouveau cas C, concernant l'accès direct, par commutation de circuits, à un autre utilisateur du réseau. Ce nouveau cas C n'affecte pas d'identificateurs DLCI aux connexions pour distinguer leurs différentes destinations. Il utilise des identificateurs DLCI pour opérer la distinction entre plusieurs connexions ayant les deux mêmes points d'extrémité. Chacune de ces connexions peut avoir une qualité de service différente.

La séquence d'actions permettant d'obtenir un circuit physique entre deux utilisateurs peut varier selon le profil de communication et d'autres circonstances. Un circuit peut être établi sans l'aide de la fonction SCF, avant les premières primitives de demande et d'indication N-CONNECT. Lorsque ces primitives seront finalement invoquées, les adresses des entités appelée et appelante pourront être omises ou ignorées. En variante, la primitive de demande N-CONNECT pourra lancer des événements et demander des adresses réseau pour l'aiguillage du circuit.

9.2 Procédures de fonction SCF

La fonction SCF doit présenter le même comportement qu'un utilisateur du réseau dans le cas A du protocole de relais de trames selon la Recommandation Q.933. Elle doit se comporter comme si elle était en présence d'une connexion semi-permanente à un dispositif distant de traitement de trames, même si le débit attribué au circuit physique ne correspond pas exactement au débit de transfert d'informations dans un RNIS.

La seule exception est celle du 5.6/Q.933, concernant les collisions entre identificateurs DLCI. Afin de conserver une relation symétrique entre deux utilisateurs du réseau, la fonction SCF ne doit donner la préférence entrante à aucun des deux sens de transmission. Elle doit au contraire résoudre

les collisions en forçant l'attribution de nouveaux identificateurs DLCI de part et d'autre, comme spécifié en détail ci-dessous.

La fonction SCF doit être conforme aux prescriptions supplémentaires qui sont indiquées dans le reste du présent sous-paragraphe.

Dès qu'un circuit physique en mode duplex est activé, la fonction SCF doit établir l'identificateur DLCI 0 et l'affecter au plan de commande. Cet identificateur acheminera les messages Q.933 dans les trames d'information de structure Q.922. S'il arrive que l'identificateur DLCI 0 fasse l'objet d'un rétablissement, ce qui indique une erreur de protocole, la fonction SCF doit en provoquer la libération. S'il arrive que l'identificateur DLCI 0 soit libéré, la fonction SCF doit éliminer tous les autres identificateurs DLCI affectés au circuit physique puis doit indiquer que leurs connexions de couche Liaison de données sont interrompues. La fonction SCF peut ensuite tenter de rétablir l'identificateur DLCI 0 et de réinitialiser la signalisation Q.933.

En réponse favorable au message SETUP, la fonction SCF doit envoyer le message CONNECT, qui doit provoquer une réponse de type CONNECT ACKNOWLEDGE. Dans cette situation, il n'y a aucun avantage à envoyer des messages de type ALERTING, CALL PROCEEDING ou PROGRESS. Si, toutefois, de tels messages sont reçus, ils peuvent être ignorés.

La réponse défavorable au message SETUP est RELEASE COMPLETE. Il s'agit également du plus simple moyen pour libérer une communication active. Dans cette situation, il n'y a aucun avantage à envoyer des messages de type DISCONNECT, STATUS ou STATUS ENQUIRY. Si, toutefois, de tels messages sont reçus, ils peuvent provoquer l'envoi du message RELEASE COMPLETE. Si le message RELEASE est reçu lors de la plupart des états de communication spécifiés dans la Recommandation Q.933, par exemple alors que la communication est active mais non pendant l'attente d'une réponse au message SETUP ou RELEASE, cela doit provoquer l'émission du message RELEASE COMPLETE. Un message RELEASE COMPLETE non sollicité, bien que considéré comme une erreur dans la séquence de messages, réalise l'action prévue de forcer le récepteur à libérer une communication.

La Figure 13 montre les messages échangés et les primitives invoquées au cours d'une phase de connexion réseau (N-CONNECT) réussie. Cette figure suppose que l'identificateur DLCI 0 ait déjà été établi lors de l'activation du circuit physique, à la suite de l'échange d'une commande d'établissement du mode asynchrone symétrique étendu (SABME) et d'un accusé de réception non numéroté (UA).

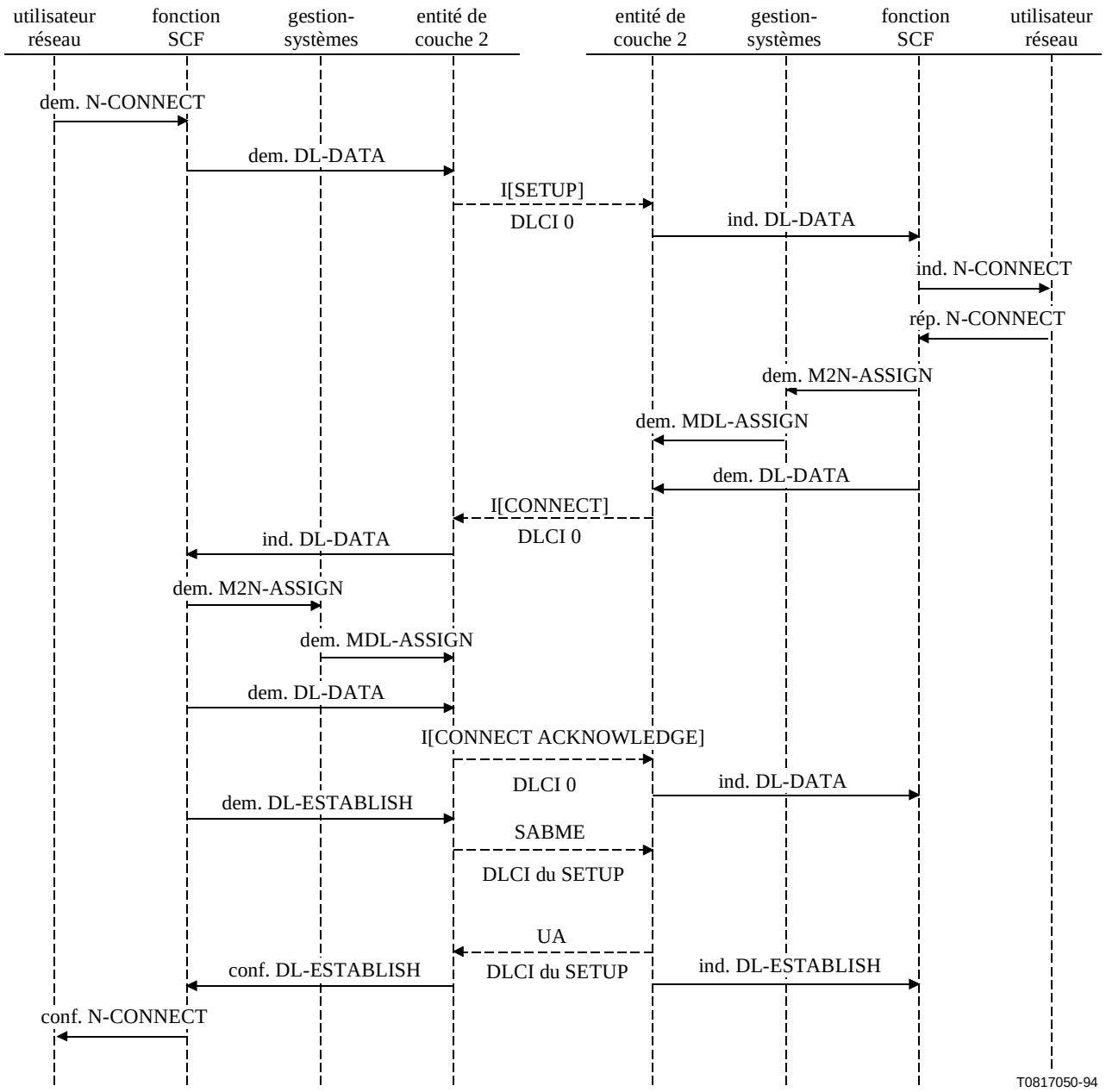


Figure 13/T.123 – Séquence d'actions pour N-CONNECT

La fonction SCF doit utiliser des valeurs de référence d'appel comportant un seul octet (entre 1 et 127 de part et d'autre) et des valeurs d'identificateur DLCI de deux octets (sur 10 éléments binaires). Les identificateurs DLCI doivent être sélectionnés aléatoirement dans l'étendue attribuée par la Recommandation Q.922 pour prendre en charge les informations d'utilisateur, à savoir de 16 à 991 inclus.

Une fonction SCF qui traite une demande N-CONNECT doit proposer, dans un message SETUP, une valeur préférée d'identificateur DLCI. Une fonction SCF qui reçoit un message SETUP doit vérifier la valeur d'identificateur DLCI qu'il contient: si cette valeur est déjà affectée, il s'agit d'une erreur. Si la fonction SCF du côté réception a proposé la même valeur d'identificateur DLCI dans un message SETUP encore sans réponse, elle doit répondre au nouveau message SETUP par le message RELEASE COMPLETE avec le numéro de cause 44: *circuit/canal demandé non disponible*. Si elle n'a pas déjà proposé la même valeur, elle doit accepter la valeur reçue de l'identificateur DLCI. Sa réponse au message SETUP dépendra alors du contrôle d'autres paramètres et de la décision de l'utilisateur réseau. Si la réponse est favorable à l'établissement, la même valeur d'identificateur DLCI

doit être retournée dans le message CONNECT; si ce n'est pas le cas, un numéro de cause autre que 44 doit être retourné dans le message RELEASE COMPLETE. Une fonction SCF qui reçoit une réponse de type RELEASE COMPLETE avec le numéro de cause 44 doit renouveler son message SETUP non suivi d'effet, avec une nouvelle valeur d'identificateur DLCI, choisie au hasard. Si le nombre de réessais paraît excessif, la fonction SCF peut choisir de rafraîchir son générateur de nombres aléatoires. Une fonction SCF qui reçoit une réponse de type RELEASE COMPLETE avec un numéro de cause autre que 44 doit signaler, par un message N-DISCONNECT, que la demande N-CONNECT n'a pas été suivie d'effet.

La Figure 14 montre les messages échangés et les primitives invoquées à la suite d'une demande N-DISCONNECT issue d'un utilisateur. On notera que la demande DL-RELEASE et l'envoi du message DISC ne sont pas obligatoires car MDL-REMOVE rétablira de chaque côté l'état correct des identificateurs DLCI en cause.

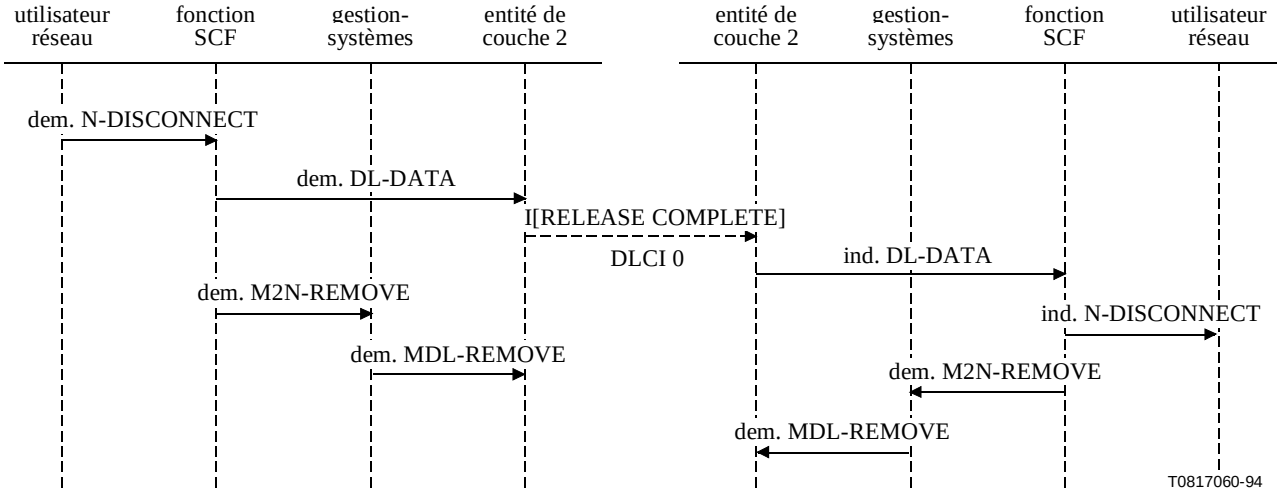


Figure 14/T.123 – Séquence d'actions pour N-DISCONNECT

Pour éviter une situation de compétition, il faut que la fonction SCF retarde la réutilisation de sa référence d'appel libérée pour un nouvel appel, si elle a lancé une demande N-DISCONNECT. La raison en est que si les deux extrémités se déconnectent et que le demandeur se reconnecte au moyen de la même valeur de référence d'appel, un message RELEASE COMPLETE en transit pour l'appel précédent peut être interprété à tort comme indiquant un échec du nouvel appel. La probabilité de cet événement est minimisée si la fonction SCF choisit plutôt sa valeur de référence d'appel la moins utilisée récemment. En pratique, une affectation séquentielle de valeurs (progressant d'une référence à chaque appel) peut suffire. En variante, la fonction SCF peut choisir d'employer une procédure de déconnexion plus compliquée, avec émission du message RELEASE puis attente de la réponse RELEASE ou RELEASE COMPLETE.

Une erreur non corrigée lors du transfert de données au moyen d'un identificateur DLCI est indiquée par un message de type DL-ESTABLISH ou DL-RELEASE, selon le résultat de la réinitialisation de la liaison de données. L'un de ces messages doit faire commencer la déconnexion par une indication N-DISCONNECT au lieu d'une demande, suivie des actions suivantes de la Figure 14. L'exception possible est que l'identificateur DLCI 0 soit déjà affecté, ce qui entraîne les conséquences plus graves qui ont été spécifiées plus haut.

9.3 Messages de fonction SCF

Les éléments d'information apparaissent en ordre fixe, comme indiqué dans les Tableaux 2 à 5. Les éléments de type M sont soit obligatoires dans la Recommandation Q.933 ou requis dans le cadre de la spécification de cette fonction SCF. Les éléments de type O sont facultatifs. Les éléments d'information qui ne sont pas énumérés ici ne devront pas être émis et pourront être ignorés s'ils sont reçus.

NOTE 1 – Si les sélecteurs de point NSAP vers un fournisseur de service MCS par défaut sont administrés de manière à avoir une valeur "Néant", comme recommandé au paragraphe 6, il peut n'y avoir aucun avantage à acheminer les éléments d'information de type sous-adresse dans le cadre des messages SETUP et CONNECT. Des sélecteurs spécifiques peuvent être cependant requis afin d'atteindre un fournisseur de service MCS dans un contexte particulier. La possibilité de les utiliser pour supporter des protocoles autres que T.125 avec partage du même circuit physique doit faire l'objet d'un complément d'étude.

NOTE 2 – Le codage binaire préféré pour une adresse de point NSAP est spécifié dans A.8.3.1/X.213.

Tableau 2/T.123 – Contenu du message SETUP

Elément d'information	Type	Notes
Discriminateur de protocoles	M	
Référence d'appel	M	
Type de message	M	
Capacité support	M	Q.922
Identificateur DLCI	M	Valeur préférée
Délai de transit de bout en bout	O	Valeur cumulée, valeur demandée, valeur maximale
Paramètres communs de couche DL	O	N201, débit(s), valeur(s) minimale(s)
Paramètres protocolaires de couche DL	O	k, T200
Priorité X.213	O	Priorité des données, plus petite valeur acceptable
Sous-adresse du demandeur	O	Adresse du point NSAP
Sous-adresse du demandé	O	Adresse du point NSAP

Tableau 3/T.123 – Contenu du message CONNECT

Elément d'information	Type	Notes
Discriminateur de protocoles	M	
Référence d'appel	M	
Type de message	M	
Identificateur DLCI	M	Valeur exclusive
Délai de transit de bout en bout	O	Valeur cumulée
Paramètres communs de couche DL	O	N201, débit(s)
Paramètres protocolaires de couche DL	O	k, T200
Sous-adresse de ligne connectée	O	Adresse de point NSAP
Priorité X.213	O	Priorité des données

Tableau 4/T.123 – Contenu du message CONNECT ACKNOWLEDGE

Elément d'information	Type
Discriminateur de protocoles	M
Référence d'appel	M
Type de message	M

Tableau 5/T.123 – Contenu du message RELEASE COMPLETE

Elément d'information	Type
Discriminateur de protocoles	M
Référence d'appel	M
Type de message	M
Cause	M

9.4 Paramètres de qualité de service

La performance en termes de transfert de données a pour importantes caractéristiques le débit utile, le délai de transit et la priorité, qui font partie de l'ensemble de paramètres de QS des messages N-CONNECT. Les paramètres de QS sont distincts des paramètres de protocole mais peuvent avoir une influence sur eux. Ces deux types de paramètres peuvent être acheminés par la fonction SCF au moyen d'éléments d'information de type facultatif, insérés dans les messages SETUP et CONNECT.

Les négociations de paramètres doivent être conformes aux règles 5.1.3.3/Q.933 et 5.2.3.3/Q.933.

Les paramètres système de type Q.922 qui peuvent être négociés sont les suivants: k, N201 et T200. Leur valeur doit être la même dans les deux sens du transfert. Si ces paramètres ne sont pas explicitement signalés, ils doivent prendre les valeurs par défaut du paragraphe 10 ci-après.

Si les paramètres de QS ne sont pas explicitement signalés, les qualités de service correspondantes sont indéterminées et peuvent prendre toute valeur convenant aux fournisseurs de service.

Les paramètres de QS et de protocole contenus dans les messages CONNECT, complétés de toutes valeurs par défaut éventuelles, doivent être des valeurs finales pour l'identificateur DLCI assigné. La fonction SCF doit les transmettre à l'entité de couche 2 sous-jacente au moyen d'un message M2N-ASSIGN, qui émerge du plan de gestion sous la forme d'un message MDL-ASSIGN. Ce processus est en accord avec 4.1.1.5/Q.922 et 4.1.1.10/Q.922, qui indiquent que d'autres paramètres peuvent, sur option, être inclus dans ces primitives.

Les paramètres de QS et de protocole de l'identificateur DLCI 0 ne sont pas explicitement signalés. Les valeurs de QS doivent être, par défaut, égales ou supérieures à celles de tout autre identificateur DLCI. Les paramètres de protocole k, N201 et T200 doivent prendre, pour l'identificateur DLCI 0, leurs valeurs par défaut.

Une entité de couche 2 peut implémenter ou ne pas implémenter la priorité de données sous forme de paramètre de QS. Si elle l'implémente, il convient que la priorité relative des identificateurs DLCI détermine l'ordre de prise en charge des demandes de données d'utilisateur mises en file d'attente pour transmission, étant admis que leurs états protocolaires respectifs ont tous la valeur prêt. Il y a lieu de traiter impartialement les identificateurs DLCI de même priorité.

La fonction SCF doit exprimer les priorités de données au moyen du codage de valeur de l'élément d'information *priorité X.213* (qui est conforme au codage de l'élément couche paquet X.25). Le niveau de priorité le plus faible doit être 0 et le niveau le plus élevé doit être 14 au plus. Les priorités

demandées doivent être négociées par ordre décroissant en fonction de l'étendue (commençant à 0) des valeurs que l'entité de couche 2 sous-jacente peut explicitement implémenter.

10 Paramètres et options du protocole Q.922

Le format du champ d'adresse est de deux octets (identificateurs DLCI de 10 éléments binaires).

Trois éléments binaires du champ d'adresse sont réservés au service de relais de trames: notification d'encombrement explicite émise vers l'avant (FECN, *forward explicit congestion notification*), notification d'encombrement explicite émise vers l'arrière (BECN, *backward explicit congestion notification*) et priorité de mise à l'écart (DE, *discard eligibility*). Ces éléments binaires doivent être mis à 0 par l'émetteur et doivent être ignorés par le récepteur.

Le transfert des informations sera effectué en trames I au moyen des procédures d'exploitation par multitrames avec accusé de réception.

Les trames de types UI et XID ne doivent pas être transmises.

Les paramètres système sont associés à chaque connexion de couche Liaison de données. Il convient de fixer leurs valeurs en tenant compte des caractéristiques du circuit physique sous-jacent. Les valeurs par défaut sont spécifiées dans le Tableau 6.

Tableau 6/T.123 – Valeurs par défaut des paramètres système de liaison de données

Paramètres système	Valeur par défaut	Description du paramètre
k	40	Nombre maximal de trames I en attente
N200	10	Nombre maximal de réémissions
N201	260	Nombre maximal d'octets dans un champ d'information
T200	1,5 s	Temporisation de réémission
T203	30 s	Temporisation d'inactivité

Les valeurs de k, N201 et T200 peuvent être négociées par la fonction SCF telle que spécifiée au paragraphe 9. Les valeurs de N200 et de T203 n'ont pas besoin d'être communiquées par l'émetteur au récepteur; elles peuvent être réglées localement de part et d'autre.

La valeur par défaut de k est le maximum indiqué au 5.9.4/Q.922 (pour un débit de liaison compris entre 1536 et 1920 Mbit/s). C'est également la valeur citée dans l'Appendice VI/T.90, indépendamment du débit de liaison, pour un débit utile optimal avec une longueur de paquet de 256 octets.

Une trop grande valeur de k est préférable à une trop faible valeur. Un récepteur de type Q.922 n'a pas besoin d'accepter une fenêtre entière de trames I si ses mémoires tampons sont proches de la saturation; il peut indiquer l'état *récepteur interne occupé* à un point intermédiaire quelconque. De plus, un émetteur Q.922 peut s'autolimiter à un plus petit nombre de trames I en instance; il n'est pas obligé de remplir toute la capacité de la fenêtre. Par ailleurs, si le paramètre k est réglé à une valeur faible et que la fenêtre se remplisse trop rapidement, un émetteur est obligé de s'arrêter, ce qui peut avoir une incidence défavorable sur le débit utile et sur la réponse.

L'Appendice I/Q.933 suggère une procédure permettant de négocier la valeur de k au moyen d'une formule qui tient compte de la longueur, en octets, de la trame de données.

Il y a lieu que les implémenteurs envisagent la possibilité de limiter dynamiquement la longueur de trame à une valeur inférieure à celle qui est autorisée par le paramètre système N201. Cela peut

nécessiter une coordination avec l'entité de couche Transport qui assemble les unités TPDU. Il est sans doute plus prudent de restreindre la durée de transmission en série de données de très basse priorité dans le cas le moins favorable, de manière que les données de priorité plus élevée, venant d'être mises en file d'attente, puissent être prises en charge rapidement. On a proposé une temporisation maximale de 60 ms.

On pourra également examiner l'autre possibilité, qui consiste à interrompre une émission déjà en cours de données à faible priorité.

11 Transparence aux structures de trame de la couche Liaison de données pour la transmission arythmique

Etant donné que la transmission arythmique est organisée sous la forme d'une séquence d'octets, il est logique d'utiliser un procédé de bourrage d'octets pour assurer la transparence aux structures de trame de la couche Liaison de données. Il s'agit d'une variante admise du procédé de bourrage d'octets approprié à la transmission synchrone (insertion d'un bit 0 après toutes les séquences de cinq éléments binaires 1 contigus). Ce système rend plus facile et plus efficace l'implémentation de la Recommandation Q.922 au profil RTPC, en particulier lorsqu'on utilise la sortie série d'un ordinateur personnel courant.

Pour le cas d'un RTPC, le 2.6/Q.922, qui définit la transparence aux structures de trame en fonction de la Recommandation Q.921, ne doit pas être implementé. En revanche, les procédures suivantes, extraites du 4.5.2 de l'ISO/CEI 3309, doivent être implémentées.

L'octet d'échappement vers la commande est un indicateur de transparence qui désigne un octet présent dans une trame à laquelle est appliquée la procédure de transparence suivante. Le codage de cet octet d'échappement est indiqué dans la Figure 15.

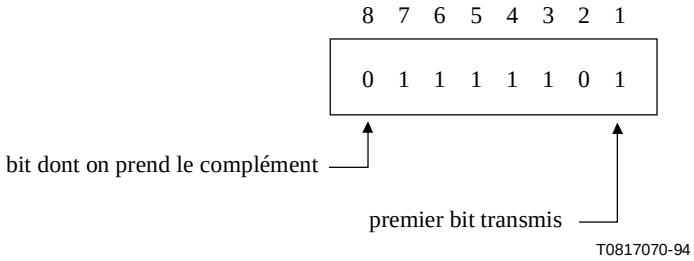


Figure 15/T.123 – Octet d'échappement-commande pour la transparence aux trames arythmiques

L'émetteur doit examiner le contenu des trames entre les séquences délimitant l'ouverture et la fermeture, y compris les champs d'adresse, de commande et de séquence de verrouillage de trames; il doit ensuite, une fois le calcul du verrouillage de trames effectué:

a) prendre le complément du 6^{e} élément binaire de l'octet dès l'apparition du fanion ou d'un octet d'échappement-commande;

b) insérer un octet d'échappement vers la commande immédiatement avant l'octet qui résulte de l'opération précédente, avant l'émission.

D'autres valeurs d'octet peuvent, en option, être incluses par l'émetteur dans la procédure de transparence.

Le récepteur doit examiner le contenu des trames entre les deux octets délimiteurs et doit, dès réception d'un octet d'échappement-commande et avant le calcul de la séquence de contrôle de trame:

a) ignorer l'octet d'échappement-commande;

b) rétablir l'octet qui le suit immédiatement en prenant le complément de son 6e élément binaire.

Une trame qui se termine par un octet d'échappement-commande suivi d'un fanion de clôture est non valide et doit être ignorée par le récepteur (abandon de trame).

NOTE – Cette procédure n'exclut pas l'apparition d'un caractère particulier quelconque dans le flux des données transmises. Dans le cas d'ETTD et d'ETCD séparés, la commande du débit entre ces équipements, au moyen de caractères de commande (XON/XOFF) doit être désactivée parce que ces caractères ne peuvent pas être distingués de la transmission des mêmes caractères d'ETTD à ETTD. Dans ce cas précis et dans le cadre de la présente Recommandation, la commande de débit est une fonction assurée par le protocole Q.922.

12 Sous-couche physique formée par les canaux de protocole MLP H.221

L'utilisation des canaux MLP et H-MLP de la Recommandation H.221 doit être conforme aux spécifications des Recommandations H.221, H.230, H.233, H.242 et H.243 pour l'intégration de signaux multimédias:

– déterminer un mode d'exploitation compatible en appliquant la séquence A d'échange des codes de capacités selon la Recommandation H.242;

– tous les systèmes compatibles avec le protocole multicouche (MLP) doivent déclarer au moins la capacité commune MLP-6,4k;

– on pourra également déclarer d'autres débits pour canaux MLP et H-MLP selon la Recommandation H.221;

– la séquence B de commutation de mode selon la Recommandation H.242 est applicable à l'établissement ou au changement de mode;

– dès qu'il reçoit un signal H.221 de commande d'ouverture de canal MLP ou H-MLP, un système doit faire en sorte qu'au moins un de ces canaux soit ouvert dans le sens inverse, de façon qu'une communication bilatérale puisse s'établir;

– les débits des canaux MLP et H-MLP peuvent ne pas être les mêmes dans les deux sens de transmission, sauf si la symétrie a été explicitement commandée;

– la commande multipoint de transmission symétrique des données de la Recommandation H.230 est applicable aux canaux MLP et H-MLP mais elle implique que les débits sortants soient alignés sur les débits entrants.

Comme le suggère 9.2/H.242, si MLP et H-MLP sont ouverts en même temps, leurs débits doivent être combinés de façon à former un seul train binaire séquentiel. Les positions des éléments binaires doivent être numérotées horizontalement dans les trames H.221 synchronisées du canal initial et des canaux additionnels, comme indiqué dans les Tableaux 7 à 9.

Les commandes H.221 de réglage du débit des canaux MLP ou H-MLP ne doivent pas interrompre la continuité logique du flux séquentiel composite. L'injection ou l'extraction d'éléments binaires doivent simplement se poursuivre dans la sous-multitrame suivante, à un débit différent. Il convient que le fonctionnement des protocoles des couches supérieures ne soit pas influencé, à moins que le débit soit trop fortement réduit pendant une longue période.

En particulier, le canal MLP ou H-MLP (ou les deux) peut être temporairement interrompu lors du processus de réaffectation des débits dans un multiplex multimédia. Par lui-même, ce processus ne suffit pas à provoquer une déconnexion intempestive des liaisons de données à protocole Q.922. Cette interruption ne doit intervenir, en l'absence d'erreurs détectées par protocole, que lors de la réception de la commande H.221 "T.120-hors service".

Tableau 7/T.123 – Positions des bits pour la capacité MLP-6,4k avec restriction et chiffrement activé

Canal initial							
1	2	3	4	5	6	7	8
							1
						FAS	1
							1
							1
						BAS	1
							1
							1
						ECS	1
							1
						M1	1
						M2	1
						•	1
						•	1
						M55	1
						M56	1

FAS signal de verrouillage de trames (*frame alignment signal*)
BAS signal d'attribution de débit (*bit-rate allocation signal*)
ECS signal de commande de chiffrement (*encryption control signal*)

Tableau 8/T.123 – Positions des bits pour les capacités MLP-6,4k plus H-MLP-62,4k

Canal initial								Canal additionnel							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
								M1	M2	M3	M4	M5	M6	M7	
							FAS	M8	•	•	•	•	•	M14	FAS
								•	•	•	•	•	•	•	
								•	•	•	•	•	•	•	
							BAS	•	•	•	•	•	•	•	BAS
								M106	•	•	•	•	•	M112	
							M113	M114	•	•	•	•	•	M120	M121
							•	•	•	•	•	•	•	•	•
							•	•	•	•	•	•	•	•	•
							M680	•	•	•	•	•	•	•	M688

Tableau 9/T.123 – Positions des bits pour la capacité H-MLP-128k dans un canal H0

Intervalle de temps 1	Intervalle de temps 2			Intervalle de temps 3			Intervalle de temps 4	Intervalle de temps 5	Intervalle de temps 6
	M1	• • •	M8	M9	• • •	M16			
	M17	• • •	•	•	• • •	M32			
	•	• • •	•	•	• • •	•			
	•	• • •	•	•	• • •	•			
	M1265	• • •	•	•	• • •	M1280			

13 Profils en variante

Ces variantes sont conçues de façon à permettre d'établir des connexions point à point entre terminaux ou entre unités MCU dans certaines circonstances particulières. Leur utilisation peut être spécifiée dans la recommandation du système pour un service particulier ou peut faire l'objet d'un accord bilatéral.

L'ensemble des profils en variante n'est pas complet et ne vise pas à constituer une liste exhaustive de toutes les possibilités.

Aucune procédure n'est ici proposée pour que les terminaux puissent déterminer qu'ils partagent un profil commun. Aucune prescription n'est non plus donnée pour la négociation dans le cas où les terminaux se partagent plusieurs profils. Le codage des éléments d'information *Commande d'appel* selon Q.931 ou Q.2931 peut restreindre l'ensemble des profils qui peuvent être pris en considération mais ne peut garantir un résultat satisfaisant. De telles questions relèvent d'un concept plus vaste, qui peut faire référence à la présente Recommandation.

13.1 Variante: RNIS fondée sur la Recommandation Q.922

La Figure 16 définit un profil en variante pour le RNIS fondé sur la Recommandation Q.922. Lorsque la capacité vidéo n'est pas requise et qu'on peut attribuer aux données audio leur propre canal, la pile protocolaire à implémenter est moins coûteuse que celle qui est fondée sur les trames H.221. Les couches supérieures aux canaux B ou H sont identiques au profil RNIS de base.

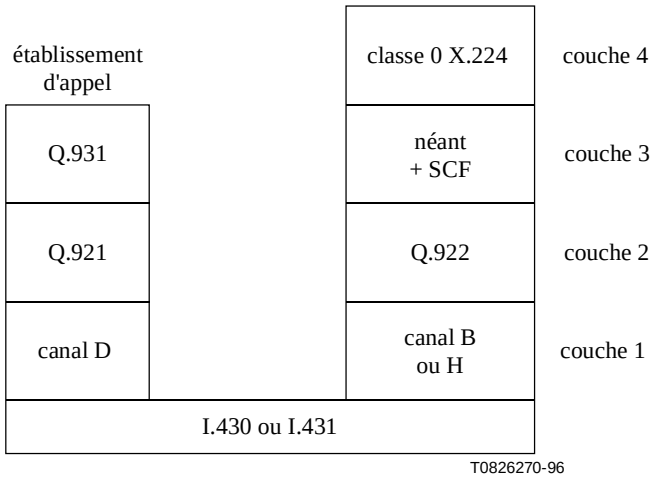


Figure 16/T.123 – Profil en variante pour RNIS fondé sur la Recommandation Q.922

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 1

– Un seul canal B, un seul canal H0 ou un seul canal H1.

– Certains réseaux peuvent aussi offrir des canaux à débit intermédiaire.

13.2 Variante: RNIS fondée sur la Recommandation T.90

La Figure 17 définit un profil en variante pour le RNIS fondé sur la Recommandation T.90. Bien que moins efficace que le protocole Q.922, la pile protocolaire X.25 est une composante plus courante des terminaux télématiques.

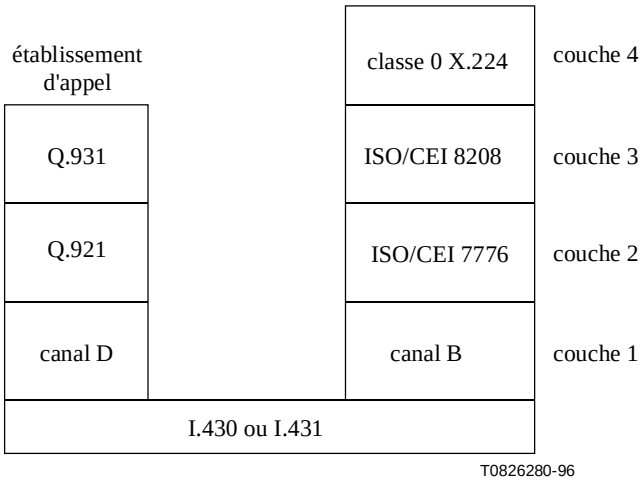


Figure 17/T.123 – Profil en variante pour RNIS fondé sur la Recommandation T.90

Couche 4

– X.224.

– Classe 0 préférée; aucune classe en variante.

Couche 3

– Communication ETTD-ETTD comme spécifié par le paragraphe 2/T.90.

Couche 2

– Communication ETTD-ETTD comme spécifié par le paragraphe 2/T.90.

Couche 1

– Communication ETTD-ETTD comme spécifié par le paragaphe 2/T.90.

13.3 Variante: RNIS fondée sur la Recommandation V.120

La Figure 18 définit un profil en variante pour le RNIS fondé sur la Recommandation V.120. Cette pile protocolaire permet à un ordinateur personnel type d'accéder aux vitesses du RNIS au moyen d'un adaptateur de terminal courant. Les couches supérieures à l'adaptation du terminal sont identiques au profil de base du RTPC.

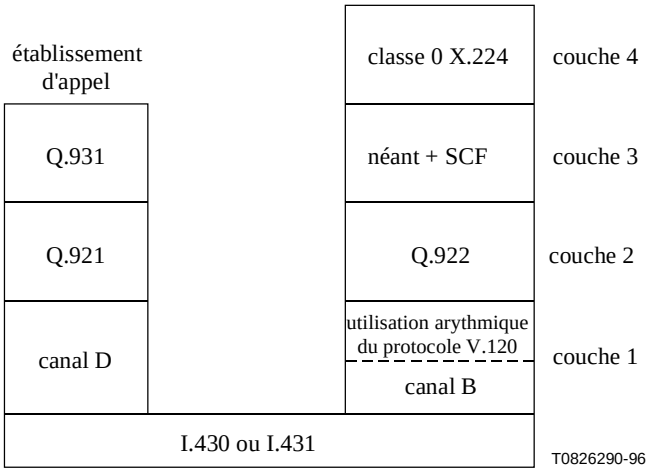


Figure 18/T.123 – Profil en variante pour RNIS fondé sur la Recommandation sur V.120

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 1

– Transmission arythmique par ETTD.

– ETCD en mode d'exploitation asynchrone conformément à la Recommandation V.120.

– L'ETTD et l'ETCD peuvent assurer des fonctions logiques non séparées physiquement, si l'équipement intégré peut émettre les même signaux.

13.4 Variante: RTPC fondée sur la Recommandation H.324

La Figure 19 définit un profil en variante pour le RTPC fondé sur la Recommandation H.324. Cette variante permet de déployer largement la communication de données en conférence, en conjonction avec la visiophonie par RTPC. Le mappage de trames Q.922 sur des unités AL-SDU permet de mieux utiliser la rare largeur de bande qu'avec les autres types de trames possibles. Les couches supérieures à l'adaptation sont identiques au profil de base RTPC.

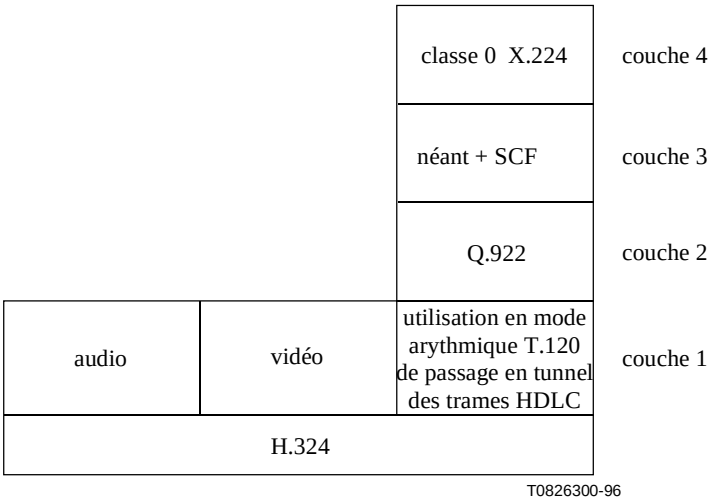


Figure 19/T.123 – Profil en variante pour RTPC fondé sur la Recommandation H.324

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Comme spécifié au 7.4, Profil RTPC de base.

Couche 1

– Transmission arythmique par ETTD.

– ETCD en mode HDLC tunnel H.324 pour T.120.

– L'ETTD et l'ETCD peuvent assurer des fonctions logiques non séparées physiquement, si l'équipement intégré peut émettre les même signaux.

NOTE – L'effet final est que le contenu d'une trame Q.922 (y compris la séquence FCS mais sans fanions ni indicateurs de transparence) est acheminé sous forme d'une seule unité AL-SDU au moyen des trames de couche AL1 dans un canal logique H.223 ouvert pour l'application de transmission de données T.120.

13.5 Variante: RNIS-LB fondée sur la Recommandation H.222

La Figure 20 définit un profil en variante pour le RNIS-LB fondé sur la Recommandation H.222. Cette pile protocolaire multiplexe des données audio, vidéo et télématiques pour les regrouper dans une même voie virtuelle en mode ATM. Les couches supérieures au protocole Q.922 sont identiques au profil RNIS de base.

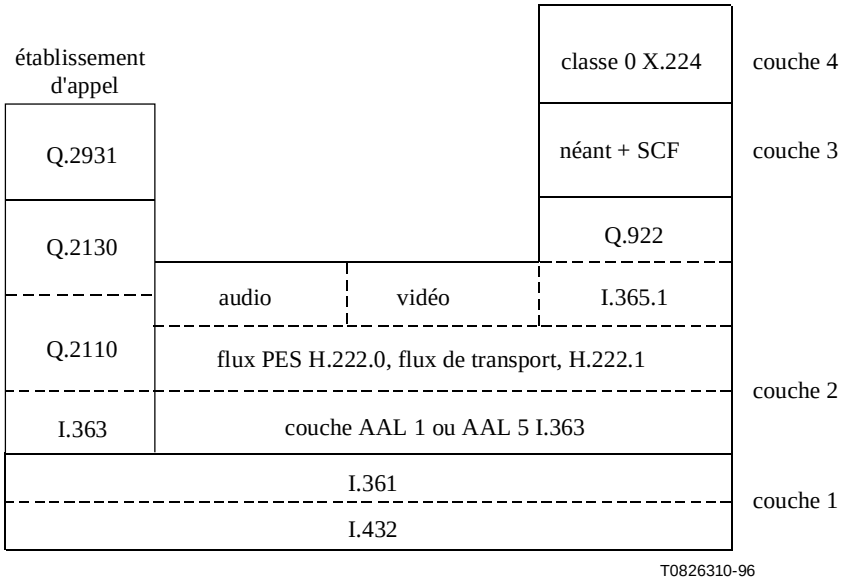


Figure 20/T.123 – Profil en variante pour RNIS-LB fondé sur la Recommandation H.222

Couche 4

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 3

– Comme spécifié au 7.1, Profil RNIS de base.

Couche 2

– Q.922.

– Paramètres et options de protocole comme spécifié par le paragraphe 10, Paramètres et options du protocole Q.922.

– Structure de trame modifiée: pas d'utilisation de fanions ni d'indicateurs de transparence.

– Chaque trame (des octets d'adresse jusqu'à la séquence FCS) est acheminée dans les octets de données d'un même paquet de flux PES acheminé dans le flux élémentaire de données défini dans la Recommandation H.222.1, pour le sous-canal T.120 de type protocolaire.

– Transmission du flux de transport comme spécifié dans la Recommandation H.222.1.

NOTE – L'indicateur de début d'unité de capacité utile classifie chaque paquet du flux de transport comme contenant soit le premier segment soit un segment de continuation d'un paquet de flux PES. Si un segment a une longueur inférieure à la valeur maximale, la différence est absorbée par des octets de bourrage de capacité utile avant l'en-tête de paquet de flux PES, de façon à atteindre une longueur totale de 188 octets.

Couche 1

– Voie virtuelle ATM.

13.6 Variante: LAN fondée sur le transfert d'unités de données

La Figure 21 définit un profil en variante pour les LAN fondé sur le transfert d'unités de données. En alignant les unités TPDU sur les unités de données du LAN sous-jacent, une telle pile protocolaire peut éliminer certaines opérations de gestion des mémoires tampons. La procédure X.224, bien que sa caractéristique de segmentation puisse ne rien ajouter à ce qui est déjà offert par le LAN, est recommandée par souci d'uniformité et comme base pour de futures améliorations.

NOTE – Aucun protocole pour LAN n'est désigné ici car les services importants sur le plan commercial sont mieux connus par leur interface de programmation d'application. Les protocoles qui prennent en charge un tel service ne sont pas toujours divulgués ni documentés.

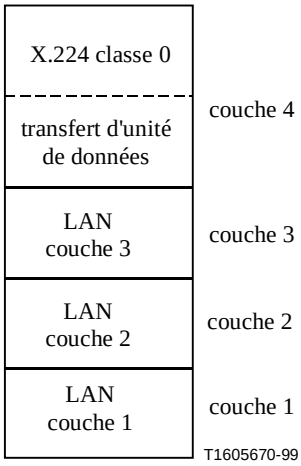


Figure 21/T.123 – Variante de profil LAN fondée sur le transfert d'unités de données

Couche 4

– X.224 classe 0 préférée; aucune classe en variante.

– La longueur maximale des unités TPDU ne doit pas dépasser celle des unités de données LAN.

– Transfert d'unités de données avec les caractéristiques suivantes:

  a) service en mode avec connexion préservant la succession des octets;

  b) frontières entre unités de données conservées dans le cadre du transfert;

  c) taux d'erreurs résiduel suffisamment faible pour permettre une utilisation comme service réseau de type A;

  d) mécanisme de contrôle de flux permettant d'exercer une action en retour sur l'émetteur.

NOTE 1 – Exemples de ce qui précède: NetBIOS Extended User Interface (NetBEUI), NetWare Sequenced Packet Exchange (SPX) et AppleTalk Data Stream Protocol (ADSP).

NOTE 2 – Dans le cas des protocoles SPX et ADSP, les frontières entre unités de données sont marquées par le positionnement d'un bit de fin de message (EOM, *end-of-message*).

Couche 3

– Le protocole NetWare Internetwork Packet eXchange (IPX) et le protocole Apple de livraison de datagrammes (DDP, *datagram delivery protocol*) constituent des exemples généraux.

Couche 2

– En général, l'ISO/CEI 8802: sous-couches de commande de liaison logique et d'accès au média.

Couche 1

– En général, l'ISO/CEI 8802: média physique.

ANNEXE A

Intégration de signaux multimédias à trames de structure H.221 conformément à la Recommandation

La Figure A.1 montre comment les trames de structure H.221 intègrent le débit utile d'un ou de plusieurs canaux numériques puis répartissent le débit de transfert total entre les différents médias.

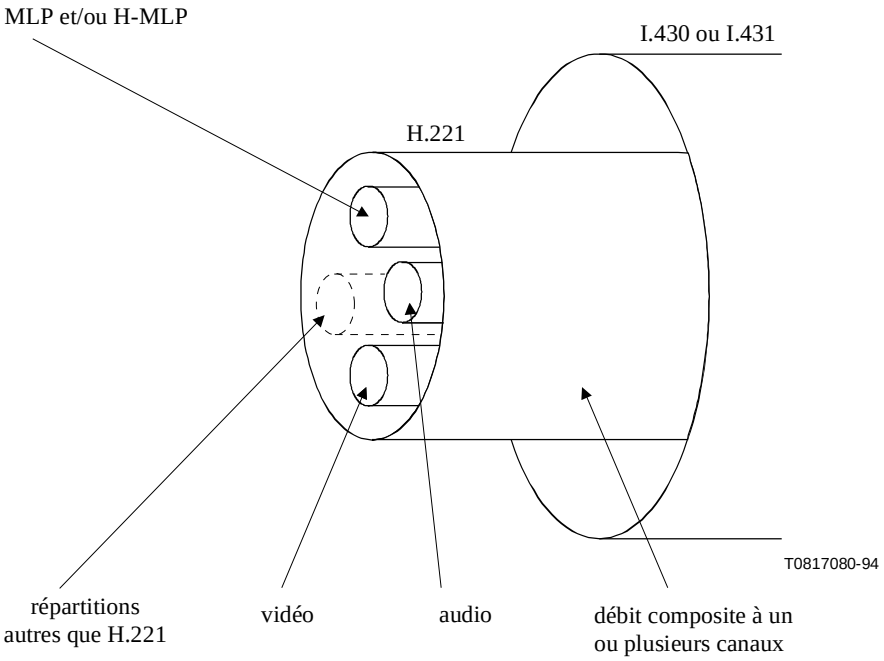


Figure A.1/T.123 – Intégration de signaux multimédias dont la trame de structure est conforme à la Recommandation H.221

ANNEXE B

Connexions de transport étendues

B.1 Domaine d'application

La présente annexe définit une procédure et un protocole qui permettront à des connexions de transport d'une conférence T.120 de négocier la disponibilité des services de transport étendus. Ces services peuvent englober l'utilisation de protocoles de sécurité, de protocoles de transport, de niveaux de fiabilité pour le transfert de données et de prise en charge d'alias d'adresses. Ces négociations sont conçues de manière à fournir une compatibilité en amont avec les piles de protocoles T.123 qui prennent uniquement en charge des connexions de transport de base.

B.2 Références normatives

– Recommandation UIT-T H.225.0 (1998), *Protocoles de signalisation d'appel et mise en paquets d'un train multimédia pour des systèmes de communication multimédias en mode paquet*.

– 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.234 (1994)/Amd. 1 (1995) | ISO/CEI 8602:1995/Amd. 1:1996, *Technologies de l'information – Protocole assurant le service de transport en mode sans connexion de l'interconnexion des systèmes ouverts – Amendement 1: adjonction de la capacité de multidiffusion en mode sans connexion.*

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

– Recommandation UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base*.

– Recommandation UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels*.

– Recommandation UIT-T X.691 (1997) | ISO/CEI 8825-2:1998, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact*.

B.3 Définitions

B.3.1 pile de transport de base: pile de transport ne prenant pas en charge les procédures et le protocole définis dans la présente annexe, mais qui est par ailleurs conforme à la Recommandation T.123.

B.3.2 pile de transport étendue: pile de transport T.123 prenant en charge les procédures et le protocole définis dans la présente annexe.

B.3.3 connexion réseau: connexion établie entre deux nœuds T.120, prenant en charge un ensemble spécifique de protocoles.

B.3.4 protocole fiable: protocole garantissant que les données seront livrées à leur destination d'une manière complète, sans altération et dans l'ordre de leur émission. Le protocole TCP est un exemple de protocole fiable.

B.3.5 connexion de transport: connexion logique entre deux nœuds T.120, utilisant une ou plusieurs connexions réseau.

B.3.6 protocole non fiable: protocole ne garantissant pas la livraison des données seront livrées à leur destination d'une manière complète, sans altération et dans l'ordre de leur émission. Le protocole UDP est un exemple de protocole non fiable.

B.4 Abréviations

CNP protocole de négociation de connexion (*connection negotiation protocol*)

CNPPDU unité PDU de protocole de négociation de connexion (*connection negotiation protocol – protocol data unit*)

IP protocole Internet (*Internet protocol*)

IPSec sécurité de protocole Internet (*Internet protocol security*)

MAP protocole d'adaptation de multidiffusion (défini dans l'Annexe A/T.125) (*multicast adaptation protocol*)

MCS service de communication multipoint (*multipoint communication service*)

NSDU unité de données de service réseau (*network service data unit*)

PDU unité de données protocolaire (*protocol data unit*)

SAR segmentation et réassemblage (*segmentation and reassembly*)

SSL couche de "réceptacles" sécurisés (*secure sockets layer*)

TCP protocole de commande de sécurité (*transmission control protocol*)

TLS sécurité de couche Transport (protocole défini par le projet de norme Internet du groupe IETF) (*transport layer security*)

TLSP protocole de sécurité de couche Transport (défini par la Recommandation X.274) (*transport layer security protocol*)

TPDU unité de données protocolaire de transport (*transport protocol data unit*)

TSDU unité de données de service de transport (*transport service data unit*)

UDP protocole de datagrammes utilisateur (*user datagram protocol*)

B.5 Conventions

– L'emploi du terme "doit" (ou de la forme future) dans la présente annexe fait référence à une prescription obligatoire, alors que le terme "devrait" (ou la forme conditionnelle) fait référence à une fonctionnalité ou une procédure suggérée mais optionnelle. L'emploi du terme "peut" exprime une action optionnelle sans indiquer de préférence.

– La variante alignée des règles de codage PER de la notation ASN.1 sera utilisée, sauf spécification contraire, pour toutes les descriptions ASN.1 de la présente annexe.

– Les bits sont numérotés de 1 à 8 à l'intérieur d'un octet, le bit 1 étant le bit d'ordre le plus faible.

– Les octets dans une unité TPDU sont numérotés à partir de 1 dans l'ordre de leur entrée dans une unité NSDU.

– Les messages X.224 et leurs champs sont indiqués en caractères *MAJUSCULES ITALIQUES.*

– La notation ASN.1 et les éléments de structure du protocole CNP sont indiqués en caractères **gras**.

B.6 Aperçu général

Le service de transport T.123 de base se limite à un transfert totalement fiable de données entre nœuds. On a identifié le besoin de services de transport qui ne sont pas pris en charge par les piles de transport de base. Ces services englobent la sécurité, le transfert de données non fiable et l'adressage par alias.

Comme il n'est pas possible d'étendre de manière arbitraire le protocole X.224, ces services ne peuvent pas être simplement ajoutés à la définition de la connexion de transport de base T.123 tout en conservant la compatibilité amont. Les procédures et le protocole de la présente annexe

fournissent une réponse à ce problème en définissant une connexion de transport étendue dont les services peuvent être négociés et étendus.

B.6.1 Modèle de connexion de transport étendue

La Figure B.1 présente le modèle pour une connexion de transport de base. Les connexions de ce type fournissent un service de communication entre nœuds T.120 qui utilise une seule connexion réseau fiable. L'adresse réseau spécifique du nœud appelé doit être connue avant l'établissement d'une connexion de ce type qui, en outre, n'est pas en mesure de fournir des services de sécurité ou des services de transport de données non fiable.

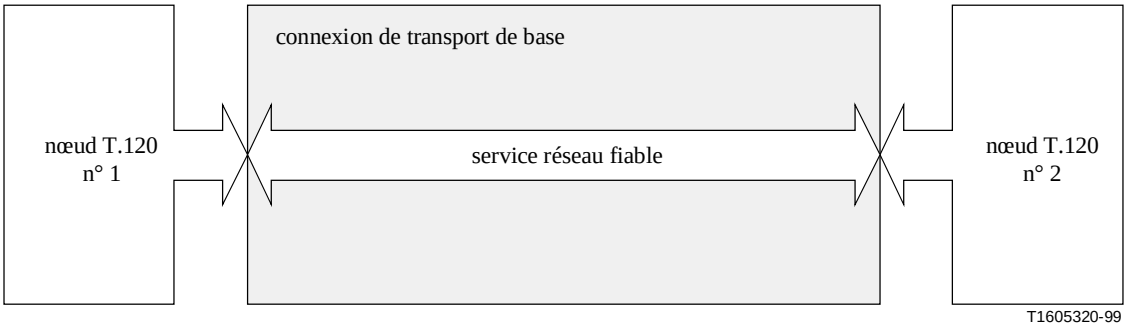


Figure B.1/T.123 – Modèle de connexion de transport de base

La Figure B.2 présente un nouveau modèle de connexion qui a été défini pour l'ajout de services étendus au protocole de transport T.123. Une connexion de transport se constitue dans ce modèle d'un ou plusieurs services réseau en relation logique. Ces services peuvent englober des transferts de données fiables ou non, ainsi que des services de sécurité pour les données transmises. Le modèle est fonctionnellement équivalent au modèle de base lorsque aucun service optionnel n'est utilisé.

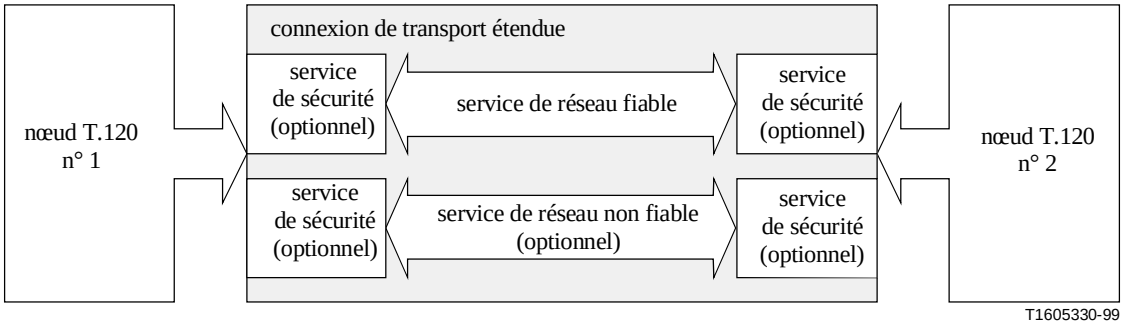


Figure B.2/T.123 – Modèle de connexion de transport étendue

La présente annexe spécifie, en plus des services de sécurité et de fiabilité, une méthode permettant d'utiliser une liste d'alias pour l'établissement de connexions de transport étendues. Ces alias peuvent être utilisés à des fins diverses telles que pour l'utilisation de serveurs de proximité (*proxy*), de passerelle et de renvoi d'appel pour des communications T.120. La Figure B.3 donne un exemple de ces types de connexions de transport étendues.

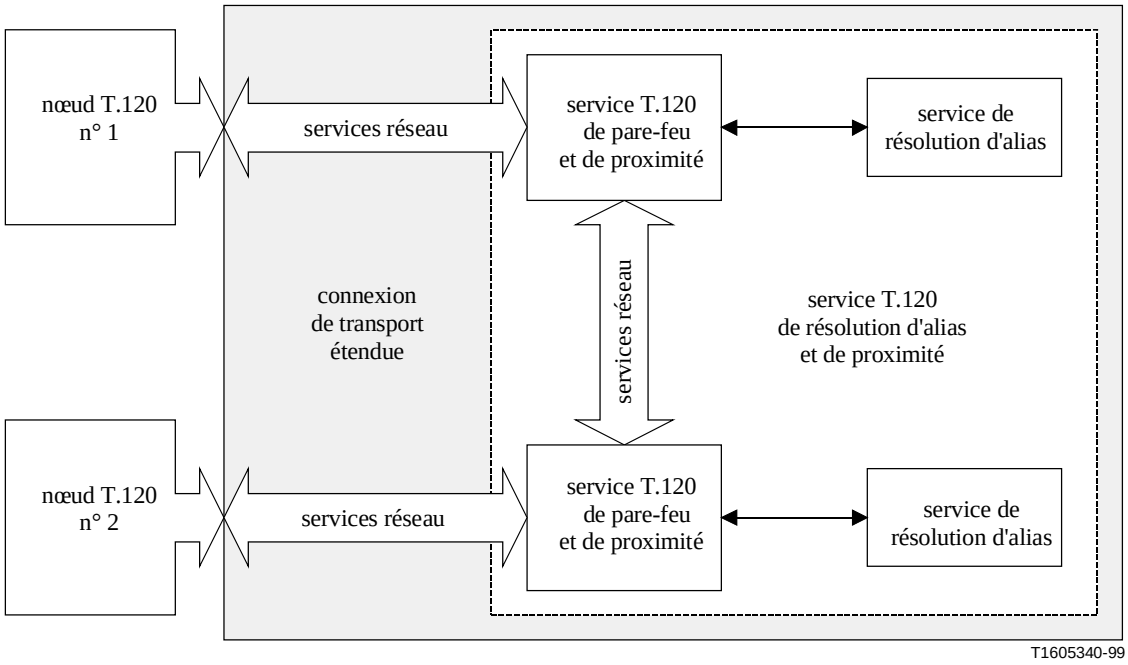


Figure B.3/T.123 – Exemple de connexion de transport étendue avec un serveur de proximité T.120

B.6.2 Services de transport

Il est possible de négocier un certain nombre de services de transport au moyen des procédures et du protocole décrits dans la présente annexe, mais la spécification d'un grand nombre de ces services est en dehors du domaine d'application de la présente Recommandation. En particulier les définitions de service pour les passerelles et serveurs de proximité T.120 appellent une étude ultérieure.

Il convient également de noter que beaucoup de services de sécurité sont définis de manière implicite dans la présente annexe. La définition des mécanismes utilisés pour fournir ces services (par exemple, l'obtention de certificats et l'échange de clés hors bande) est un problème d'implémentation, lorsque ces mécanismes ne sont pas spécifiés par ailleurs.

B.6.3 Modifications dans l'utilisation du protocole X.224

La Recommandation T.123 impose l'utilisation du protocole X.224 de classe 0 pour les connexions de base. Il est souhaitable que l'établissement de connexions étendues reste compatible avec l'établissement des connexions de base. Les informations utilisées pour les négociations de connexion étendue seront, de ce fait, encapsulées dans les unités TPDU X.224 *CONNECTION REQUEST (CR)*, *CONNECTION CONFIRM (CC)* et *DISCONNECT REQUEST (DR)* [respectivement *demande de connexion*, *confirmation de connexion* et *demande de déconnexion*]. Le paragraphe B.7 fournit les détails de cette procédure.

B.6.4 Protocole de négociation de connexion

La présente annexe définit le protocole qui sera utilisé pour établir des connexions de transport étendues. Le protocole de négociation de connexion (CNP, *connection negotiation protocol*) est conçu de manière à pouvoir être encapsulé dans le protocole X.224 ou utilisé de façon autonome sur une connexion réseau fiable. Les unités PDU de commande du protocole CNP sont définies en utilisant la notation ASN.1, afin de permettre l'extension de ce protocole. Le paragraphe B.9 fournit les détails concernant le protocole CNP.

B.7 Connexions de transport étendues

Le présent sous-paragraphe définit la procédure d'établissement de connexions de transport étendues. Ces procédures sont conçues pour permettre à un nœud T.120 d'établir une connexion de transport vers un autre nœud T.120 sans savoir au départ si ce dernier peut prendre en charge des connexions de transport étendues.

B.7.1 Etablissement de la connexion initiale

La Recommandation X.224 définit le champ *TRANSPORT-SELECTOR* (*sélecteur de transport*) sous la forme d'un champ optionnel de longueur variable contenu dans la partie variable de son unité PDU. Le paragraphe 6.5.5/X.224 précise que ce champ "indique les points d'accès des services de transport appelant et appelé". Ce champ optionnel n'est pas utilisé par le protocole X.224 ou par le protocole T.123 de base. Le présent sous-paragraphe définit son utilisation par des nœuds T.120 à des fins de prise en charge de connexions de transport étendues.

Les nœuds prenant en charge des connexions de transport étendues prendront en charge l'utilisation du champ *TRANSPORT-SELECTOR* dans les unités TPDU *CONNECTION REQUEST (CR)* et TPDU *CONNECTION CONFIRM (CC)*. La partie variable de l'unité TPDU *DISCONNECT REQUEST (DR)* sera également prise en charge. Le champ *TRANSPORT-SELECTOR* des unités TPDU *CR, CC* et la partie variable de l'unité TPDU *DR* contiendront des unités PDU du protocole CNP telles qu'elles sont spécifiées au B.9. La limite de 128 octets imposée par la Recommandation X.224 pour les unités TPDU *CR* et *DR* sera respectée dans tous les cas.

Les nœuds T.120 prenant en charge des connexions de transport étendues prendront en charge les modèles d'appel décrits ci-dessous.

B.7.1.1 Etablissement d'appel à partir d'un transport de base

Ce modèle d'appel est utilisé lorsqu'un nœud T.120 prenant uniquement en charge des connexions de base tente de se connecter à un nœud qui prend en charge des connexions étendues. Se référer à la Figure B.4.

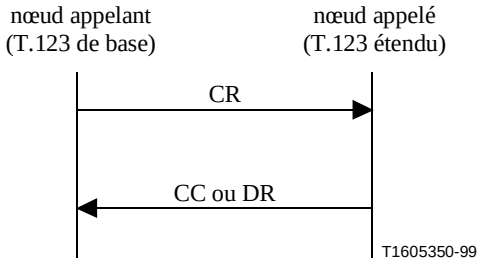


Figure B.4/T.123 – Appel d'un nœud T.123 de base vers un nœud T.123 étendu

La signalisation de ce modèle vers le nœud appelé se fait lorsqu'une unité TPDU *CR* reçue ne contient pas de champ *TRANSPORT-SELECTOR*. Le nœud appelé répondra dans ce cas conformément à la procédure d'établissement définie pour une connexion T.123 de base. L'unité TPDU *CC* de réponse ne contiendra pas de champ *TRANSPORT-SELECTOR*. Une unité TPDU de réponse *DR* ne contiendra pas de partie variable d'en-tête d'unité PDU. Le nœud appelé traitera la connexion comme une connexion de base si elle est acceptée.

B.7.1.2 Etablissement d'appel vers un transport de base

Ce modèle d'appel est utilisé lorsqu'un nœud T.120 prenant en charge des connexions étendues tente de se connecter à un nœud qui prend uniquement en charge des connexions de base. Se référer à la Figure B.5.

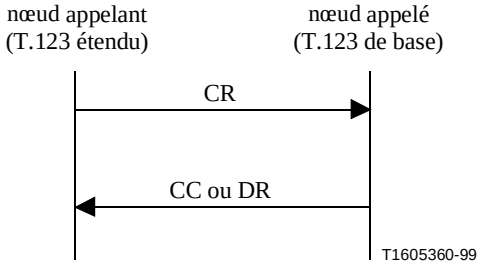


Figure B.5/T.123 – Appel d'un nœud T.123 étendu vers un nœud T.123 de base

Dans ce modèle, le nœud appelant insérera un champ *TRANSPORT-SELECTOR* dans l'unité TPDU *CR*. Le nœud de base ignorera ce champ et répondra par une unité TPDU *CC* ne contenant pas de champ *TRANSPORT-SELECTOR* ou par une unité PDU *DR* ne contenant pas de partie variable. La signalisation de ce modèle vers le nœud appelant se fait lorsque l'unité TPDU de réponse reçue ne contient pas le champ optionnel adéquat. Le nœud appelant traitera la connexion comme une connexion de base si elle est acceptée.

B.7.1.3 Etablissement d'appel utilisant la connexion réseau initiale

Ce modèle d'appel est utilisé lorsqu'un nœud T.120 prenant en charge des connexions étendues tente de se connecter à un nœud qui prend également en charge ce type de connexion. Le nœud appelé détermine dans ce cas que les services disponibles pour la connexion réseau existante sont suffisants et la connexion T.120 est acceptée. Se référer à la Figure B.6.

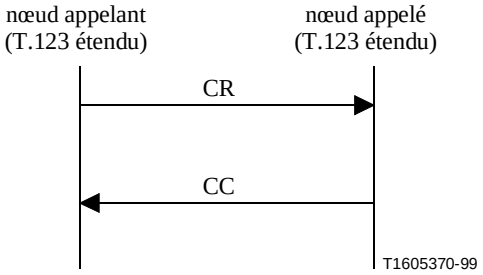


**Figure B.6/T.123 – Appel entre nœuds T.123 étendus –
Sélection de la connexion réseau existante**

Dans ce modèle, le nœud appelant insérera un champ *TRANSPORT-SELECTOR* dans l'unité TPDU *CR*. Le nœud appelé examinera ce champ pour déterminer si la connexion réseau existante peut être conservée. Il répondra dans l'affirmative au moyen d'une unité TPDU *CC* contenant un champ *TRANSPORT-SELECTOR*. La signalisation de ce modèle d'appel vers le nœud appelant se fait lorsque ce dernier reçoit l'unité TPDU *CC* contenant le champ optionnel.

Il convient de noter que les modifications négociées du protocole de transport peuvent s'effectuer après la fin de l'échange initial d'unités PDU, du fait que la connexion réseau existante est conservée. Les modifications de protocole de transport devront s'effectuer comme si la connexion réseau venait

d'être créée. Les procédures de connexion complète pour le protocole de transport négocié utiliseront la connexion réseau existante.

B.7.1.4 Etablissement d'appel au moyen d'une nouvelle connexion réseau

Ce modèle d'appel est utilisé lorsqu'un nœud T.120 prenant en charge des connexions étendues tente de se connecter à un nœud qui prend également en charge des connexions étendues. Le nœud appelé détermine dans ce cas que les services disponibles pour la connexion réseau existante ne sont pas suffisants pour la connexion T.120. La tentative de connexion est rejetée mais des informations suffisantes sont renvoyées au demandeur pour lui permettre de renouveler avec succès sa tentative de connexion. Se référer à la Figure B.7.

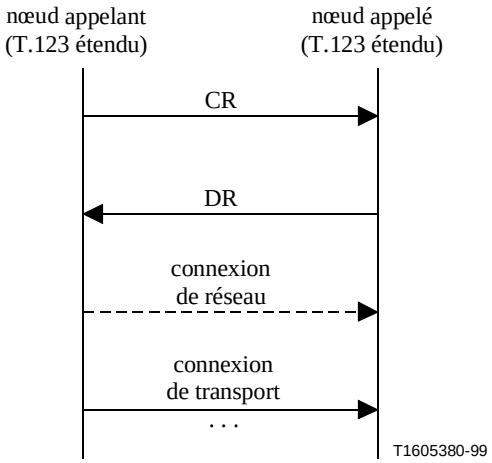


Figure B.7/T.123 – Appel entre nœuds T.123 étendus – Sélection d'une nouvelle connexion réseau

Dans ce modèle, le nœud appelant insérera un champ *TRANSPORT-SELECTOR* dans l'unité TPDU *CR*; le nœud appelé examinera ce champ. Une nouvelle connexion réseau peut être nécessaire si le nœud appelé détermine que les services de la connexion réseau existante ne sont pas suffisants. Le nœud appelé répond dans ce cas au moyen d'une unité TPDU *DR* contenant une partie variable.

La signalisation de ce modèle d'appel vers le nœud appelant se fait lorsque ce dernier reçoit une unité TPDU *DR* contenant le champ optionnel.

Le nœud appelant mettra fin à la connexion réseau existante une fois qu'il a reçu l'unité TPDU *DR* contenant le champ optionnel. L'appelant établira ensuite une nouvelle connexion réseau en utilisant les protocoles, les services et les adresses renvoyés dans la partie variable de l'en-tête de l'unité PDU *DR*. Le paragraphe B.9.5.2 fournit les détails de la procédure de nouvelle connexion.

Il convient de noter que cette procédure de nouvelle connexion peut s'appliquer plus d'une fois lors de l'établissement d'une connexion de transport unique, si l'on estime nécessaire d'établir les services de transport adéquats.

B.7.1.5 Refus de connexion

Ce modèle d'appel est utilisé lorsqu'un nœud T.120 prenant en charge des connexions étendues tente de se connecter à un nœud qui refuse d'accepter la connexion. Se référer à la Figure B.8.

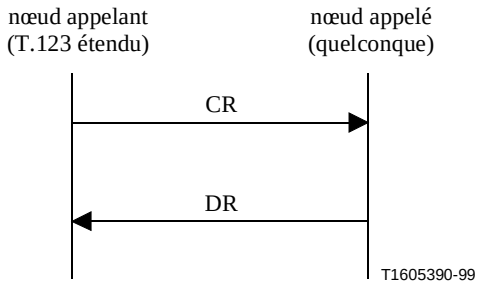


Figure B.8/T.123 – Refus d'appel

Dans ce modèle, le nœud appelant insérera un champ *TRANSPORT-SELECTOR* dans l'unité TPDU *CR*. Le nœud appelé peut examiner ce champ. Si le nœud appelé décide que la connexion de transport doit être refusée, l'appelant répondra alors au moyen d'une unité TPDU *DR* ne contenant pas de partie variable. La signalisation de ce modèle d'appel vers le nœud appelant se fait lorsque ce dernier reçoit l'unité TPDU *DR* sans champ optionnel.

Les raisons du refus d'une connexion constituent un problème local d'implémentation. Il peut s'agir d'une incompatibilité de sécurité, du dépassement de limites de connexion ou d'autres violations de politique locale.

B.7.1.6 Abandon d'une tentative de connexion

Ce modèle d'appel est utilisé lorsqu'un nœud T.120 prenant en charge des connexions étendues tente de se connecter à un nœud et le nœud appelant décide d'abandonner la tentative d'appel avant la fin de l'établissement de la connexion. Se référer à la Figure B.9.

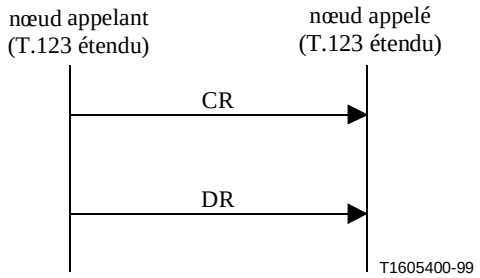


Figure B.9/T.123 – Abandon d'une tentative d'appel

Dans ce modèle, le nœud appelant insérera un champ *TRANSPORT-SELECTOR* dans l'unité TPDU *CR*. Si le nœud appelant a décidé d'abandonner la tentative d'appel avant la réception d'une unité TPDU *CC* ou *DR*, il émettra alors une unité TPDU *DR* contenant une partie variable. La signalisation de ce modèle d'appel vers le nœud appelé se fait lorsque ce dernier reçoit l'unité TPDU *DR* contenant le champ optionnel.

Les raisons de l'abandon d'une connexion constituent un problème local d'implémentation. Il peut s'agir de l'expiration d'une temporisation pour une tentative de connexion ou d'autres violations de politique locale.

B.7.2 Rétablissement de connexion

La réception par un nœud appelant d'une unité TPDU *DR* contenant la partie variable de l'en-tête d'unité PDU en réponse à une unité TPDU *CR* indique que les services réseau existants ne

conviennent pas pour l'ensemble de services de transport sélectionné par le nœud appelant. Ce dernier mettra alors immédiatement fin à la connexion réseau associée à la tentative d'appel.

Une fois que la connexion aura été libérée, le nœud appelant établira une nouvelle connexion réseau qui fournit les services (par exemple de sécurité) indiqués dans la partie variable de l'en-tête de l'unité PDU *DR*. La procédure complète de connexion sera alors appliquée pour les protocoles de transport sélectionnés lorsque la nouvelle connexion réseau aura été établie.

Un cas possible de nouvelle connexion peut se présenter si la taille de la liste des paramètres souhaités est supérieure à la limite de 128 octets imposée aux unités PDU par la Recommandation X.224. Le nœud appelant devrait négocier dans un tel cas l'utilisation du protocole CNP pour le transport. La limite de 128 octets ne s'applique pas à l'unité **ConnectRequestPDU** qui est émise ensuite, ce qui permet d'y inclure la liste des paramètres désirés.

Il convient de noter qu'il peut être nécessaire de rétablir un certain nombre de fois la connexion réseau avant d'établir la connexion de transport définitive.

B.7.3 Service réseau non fiable

Si un service de transmission de données non fiable doit être fourni par une connexion de transport, il sera alors négocié par le même échange de protocole CNP que pour l'établissement final d'un service de transmission de données fiable. L'établissement du service de données non fiable ne sera pris en considération qu'après l'établissement du service de transmissions de données fiable.

B.8 Profils étendus

B.8.1 Transports fiables

B.8.1.1 Profil CNP étendu

La Figure B.10 définit le profil CNP étendu pour le service de transport fiable. Ce profil est identique à l'un quelconque des profils de base ou en variante définis dans la présente Recommandation, avec la différence que la couche CNP est utilisée à la place de la couche X.224 de classe 0.

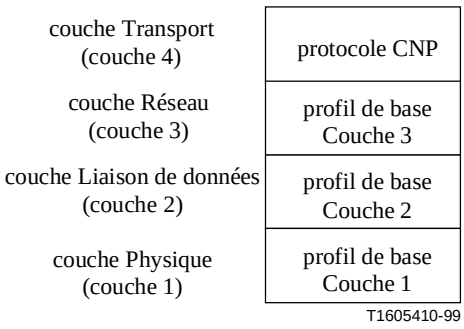


Figure B.10/T.123 – Profil étendu utilisant le protocole CNP pour un service de transport fiable

Couche 4

– Protocole CNP.

Couche 3

– Telle qu'elle est spécifiée par le profil de base ou les variantes de profil dans la Recommandation T.123.

Couche 2

– Telle qu'elle est spécifiée par le profil de base ou les variantes de profil dans la Recommandation T.123.

Couche 1

– Telle qu'elle est spécifiée par le profil de base ou les variantes de profil dans la Recommandation T.123.

B.8.1.2 Profils étendus SSL/TLS

La Figure B.11 définit les profils étendus permettant d'ajouter des services de sécurité au protocole T.123 au moyen du service SSL ou TLS. Ces profils sont identiques aux profils de réseau local de base, en variante ou étendu, avec l'exception que le service SSL ou TLS est ajouté à la couche Transport entre la couche TPKT et la couche de flux.

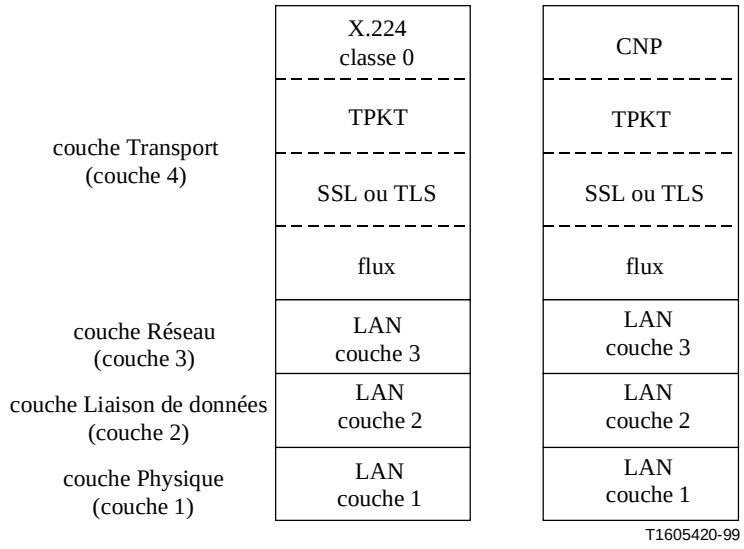


Figure B.11/T.123 – Profils étendus utilisant les services SSL ou TLS comme services de sécurité

Couche 4

– Protocole X.224 de classe 0 ou protocole CNP pour le service de transport fiable.

– Unités TPDU délimitées par des en-têtes de paquet TPKT, comme spécifié au paragraphe 8, En-tête de paquet délimitant des unités de données dans un flux d'octets.

NOTE 1 – Le paquet TPKT est nécessaire parce qu'un service de flux d'octets ne fournit pas de marqueurs pour la séparation des unités de données.

– Service SSL ou TLS

– Service de transfert par flux d'octets avec les caractéristiques suivantes:

  a) service en mode avec connexion préservant la succession des octets;

  b) taux d'erreurs résiduel suffisamment faible pour permettre une utilisation comme service réseau de type A;

  c) mécanisme de contrôle de flux permettant d'exercer une action en retour sur l'émetteur.

NOTE 2 – On peut donner, à titre d'exemple général, la spécification suivante pour le transfert par flux d'octets ci-dessus:

a) Norme RFC 793, protocole de commande de transmission;

b) numéro de port 1503 par défaut, conformément aux *numéros assignés* par la Norme RFC 1700, mais d'autres peuvent être utilisés.

Couche 3

– En général, Normes RFC 791, 792, 919, 922, 950, 1112, protocole Internet.

Couche 2

– En général, l'ISO/CEI 8802: sous-couches de commande de liaison logique et d'accès au média.

Couche 1

– En général, l'ISO/CEI 8802: média physique.

B.8.1.3 Profils étendus IPSec

La Figure B.12 définit les profils étendus permettant d'ajouter des services de sécurité au protocole T.123 au moyen du service IPSec. Ces profils sont identiques aux profils de réseau local de base, en variante ou étendu, avec l'exception que le service IPSec est ajouté à la couche Liaison de données.

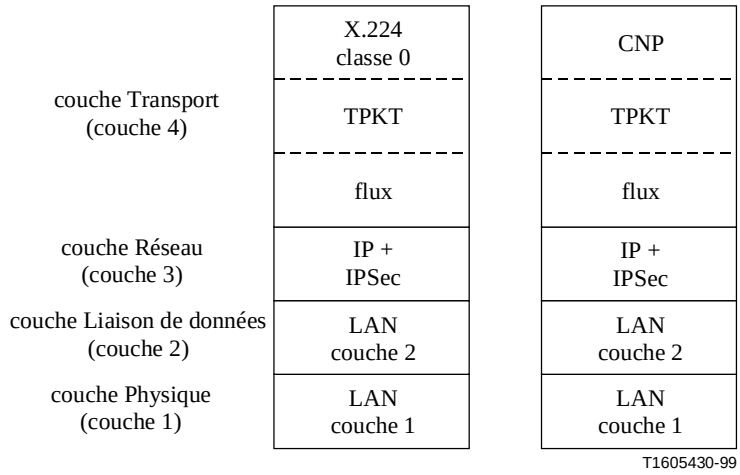


Figure B.12/T.123 – Profils étendus utilisant le service IPSec comme service de sécurité

Couche 4

– Protocole X.224 de classe 0 ou protocole CNP pour le service de transport fiable.

– Unités TPDU délimitées par des en-têtes de paquet TPKT, comme spécifié au paragraphe 8, En-tête de paquet délimitant des unités de données dans un flux d'octets.

NOTE 1 – Le paquet TPKT est nécessaire parce qu'un service de flux d'octets ne fournit pas de marqueurs pour la séparation des unités de données.

– Service de transfert de flux d'octets avec les caractéristiques suivantes:

a) service en mode avec connexion préservant la succession des octets;

b) taux d'erreurs résiduel suffisamment faible pour permettre une utilisation comme service réseau de type A;

c) mécanisme de contrôle de flux permettant d'exercer une action en retour sur l'émetteur.

NOTE 2 – On peut donner à titre d'exemple le protocole en couches suivant pour le transfert par flux d'octets ci-dessus:

a) Norme RFC 793, *protocole de commande de transmission*;

b) numéro de port 1503 par défaut, conformément aux *numéros assignés* par la Norme RFC 1700, mais d'autres peuvent être utilisés.

Couche 3

– Normes RFC 791, 792, 919, 922, 950, 1112, protocole Internet.

Couche 2

– En général, l'ISO/CEI 8802: sous-couches de commande de liaison logique et d'accès au média.

Couche 1

– En général, l'ISO/CEI 8802: média physique.

B.8.1.4 Profils étendus X.274

La Figure B.13 définit les profils étendus permettant d'ajouter des services de sécurité au protocole T.123 au moyen du service X.274. Ces profils sont identiques aux profils de base ou en variante, ou encore au profil étendu du B.8.1.1, à l'exception du protocole X.274 qui est ajouté à la couche Transport immédiatement sous la couche de protocole CNP ou X.224 de classe 0.

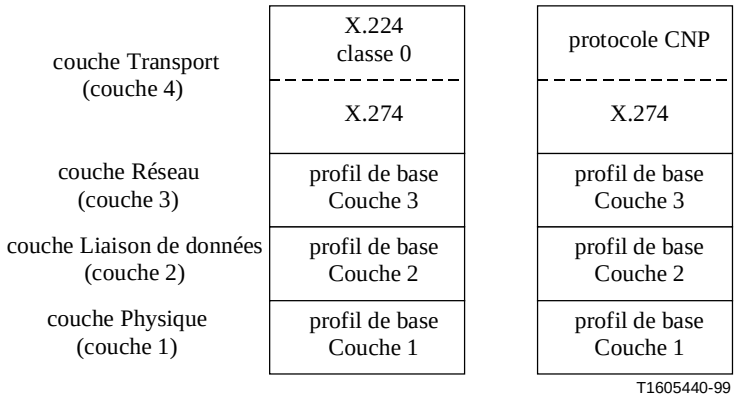


Figure B.13/T.123 – Profils étendus utilisant le protocole X.274 pour les services de sécurité

Couche 4

– Protocole X.224 de classe 0 ou protocole CNP pour le service de transport fiable.

– Protocole X.274 pour le service de sécurité.

Couche 3

– Telle qu'elle est spécifiée par le profil de base ou les variantes de profil dans la Recommandation T.123.

Couche 2

– Telle qu'elle est spécifiée par le profil de base ou les variantes de profil dans la Recommandation T.123.

Couche 1

– Telle qu'elle est spécifiée par le profil de base ou les variantes de profil dans la Recommandation T.123.

B.8.1.5 Profils étendus GSS-API

La Figure B.14 définit les profils étendus permettant d'ajouter des services de sécurité au protocole T.123 au moyen du cadre de sécurité GSS-API de l'IETF. Ces profils sont identiques aux profils de réseau local de base, en variante ou étendu, avec la différence que la passation de jeton GSS-API est ajoutée dans la couche de transport au-dessus de la couche X.224 de classe 0 ou CNP.

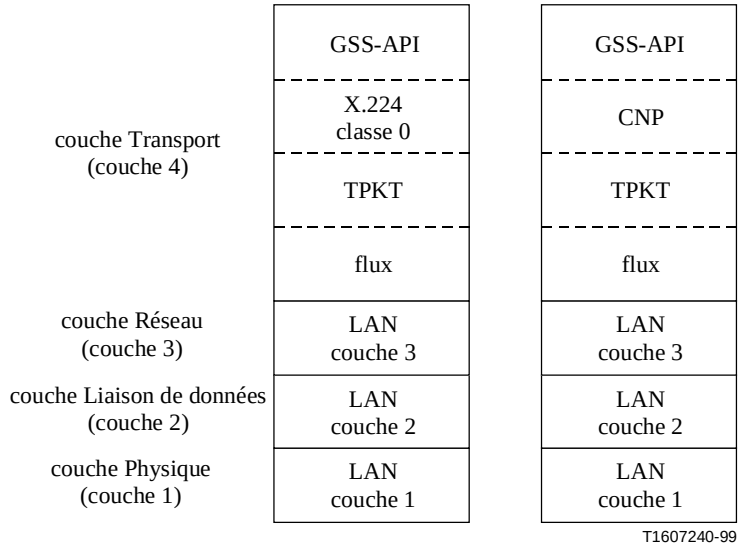


Figure B.14/T.123 – Profils étendus utilisant le cadre de sécurité GSS-API pour les services de sécurité

Couche 4

– Echange de jeton GSS-API.

– X.224 classe 0 ou CNP pour un service de transport fiable.

– en-têtes de paquet TPKT pour la délimitation des unités TPDU, comme spécifié au paragraphe 8, En-tête de paquet délimitant des unités de données dans un flux d'octets.

NOTE 1 – L'en-tête de paquet TPKT est nécessaire car un service utilisant des flux d'octets ne fournit pas de marqueur pour la séparation des unités de données.

– Service de transfert par flux d'octets avec les caractéristiques suivantes:

a) service en mode connexion conservant la séquence des octets;

b) *non*-conservation de la séparation entre les unités de données dans le cadre du transfert;

c) taux d'erreurs résiduel suffisamment faible pour permettre une utilisation comme service réseau de type A;

d) mécanisme de contrôle de flux permettant d'exercer une action en retour sur l'émetteur.

NOTE 2 – On peut donner, à titre d'exemple général, le protocole suivant pour le transfert par flux d'octets ci-dessus:

a) Norme RFC 793, *protocole de commande de transmission*;

b) numéro de port de destination 1503 par défaut, conformément aux *numéros assignés* par la Norme RFC 1700 mais d'autres peuvent être utilisés.

Couche 3

– En général, Normes RFC 791, 792, 919, 922, 950, 1112, protocole Internet.

Couche 2

– En général, l'ISO/CEI 8802: sous-couches de commande de liaison logique et d'accès au média.

Couche 1

– En général, l'ISO/CEI 8802: média physique.

B.8.2 Transport non fiable

B.8.2.1 Profil de réseau local non fiable

La Figure B.15 définit les profils étendus permettant d'ajouter des services de transport non fiables au protocole T.123 au moyen de connexions par réseau local (LAN). Les couches 1, 2 et 3 sont identiques à l'un quelconque des profils de LAN de base ou en variante.

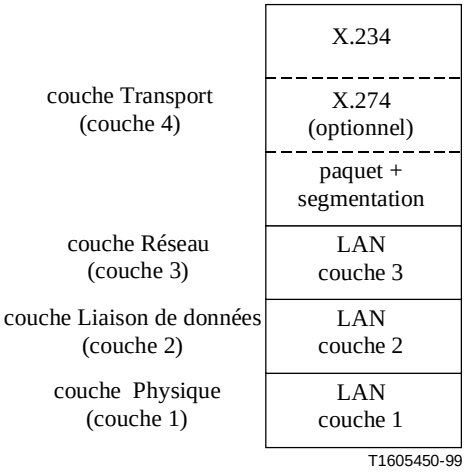


Figure B.15/T.123 – Profil de réseau local non fiable

Couche 4

– Protocole X.234, mode sans connexion.

– Protocole X.274 (négocié de manière optionnelle par le protocole CNP).

– Transfert de données non fiable sous forme de paquets avec segmentation.

NOTE – Le protocole de datagrammes utilisateur (UDP, *user datagram protocol*) est un exemple général de la couche ci-dessus.

Couche 3

– Comme spécifié dans la Recommandation T.123 pour les profils de LAN de base.

Couche 2

– Comme spécifié dans la Recommandation T.123 pour les profils de LAN de base.

Couche 1

– Comme spécifié dans la Recommandation T.123 pour les profils de LAN de base.

B.8.2.2 Profil RTPC non fiable

Voir la Figure B.16.

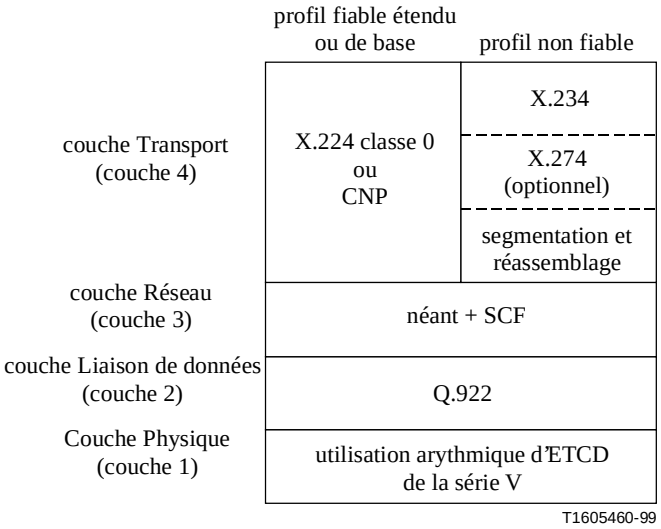


Figure B.16/T.123 – Profil RTPC non fiable

Couche 4

– Protocole X.234, mode sans connexion.

– Protocole X.274 (négocié de manière optionnelle par le protocole CNP).

– Protocole non fiable de segmentation et de réassemblage tel qu'il est défini dans le B.10, protocole non fiable de segmentation et de réassemblage.

Couche 3

– Comme spécifié dans le profil T.123 de base pour le RTPC.

Couche 2

– Protocole Q.922 utilisant des informations non numérotées (UI, *unnumbered information*).

Couche 1

– Comme spécifié dans le profil T.123 de base pour le RTPC.

B.9 Protocole de négociation de connexion (CNP, *connection negotiation protocol*)

B.9.1 Aperçu général

Les unités PDU définies pour ce protocole sont basées sur leurs contreparties du protocole X.224 de classe 0. Les protocoles X.224 et CNP fournissent les unités TPDU Connect Request, Connect Confirm, Disconnect Request, Data and Error (respectivement *demande de connexion, confirmation de connexion, demande de déconnexion, données et erreur*). Le protocole fournit en outre une unité TPDU **NonStandardPDU** (*non normalisée*) à des fins d'extension de protocole.

B.9.2 Structure des unités TPDU du protocole CNP

Toutes les unités de données protocolaires de transport (TPDU, *transport protocol data unit*) du protocole CNP contiendront un nombre entier d'octets. L'octet de numéro le moins élevé aura la valeur la plus significative lorsque des octets consécutifs sont utilisés pour la représentation d'un

nombre binaire. Les entités de transport CNP respecteront les conventions d'ordre de bit et d'octet, ce qui rend possible la communication.

La Figure B.17 présente la structure des unités TPDU du protocole CNP.

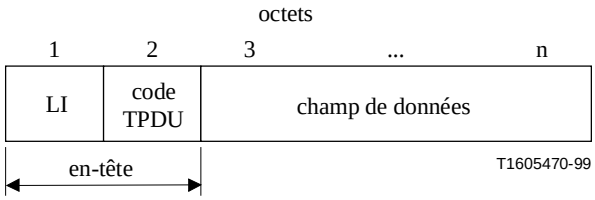


Figure B.17/T.123 – Structure générale de l'unité TPDU du protocole CNP

Les unités TPDU du protocole CNP contiendront, dans l'ordre, les informations suivantes:

- l'en-tête, contenant:
  a) le champ indicateur de longueur (LI, *length indicator*);
  b) le code TPDU;
- le champ de données.

Les unités TPDU du protocole CNP sont des unités de commande ou des unités de données. Le Tableau B.1 donne les valeurs de champs d'en-tête de chacun de ces types d'unité TPDU. Le champ "données" des unités TPDU de commande contiendra une structure ASN.1 telle qu'elle est définie au B.9.3, unités TPDU de commande. Le champ "données" des unités TPDU de données contiendra des structures d'octet, telles qu'elles sont définies au B.9.4, unité TPDU de données.

Tableau B.1/T.123 – Valeurs des champs de l'unité TPDU de commande CNP

Unité TPDU	Type	LI	Code TPDU	Champ de données
Demande de connexion	Commande	0000 0001	0100 0111	ASN.1
Confirmation de connexion	Commande	0000 0001	0100 0111	ASN.1
Demande de déconnexion	Commande	0000 0001	0100 0111	ASN.1
Erreur	Commande	0000 0001	0100 0111	ASN.1
Non normalisée	Commande	0000 0001	0100 0111	ASN.1
Données	Données	0000 0001	0100 0110	Structures d'octet

B.9.3 Unités TPDU de commande

La Figure B.18 présente la structure des unités TPDU de commande du protocole CNP.

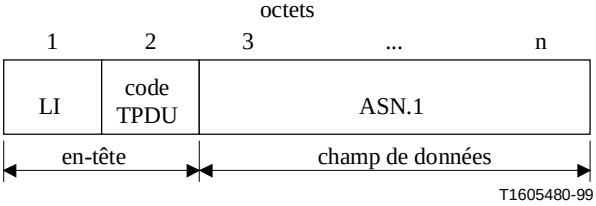


Figure B.18/T.123 – Structure de l'unité TPDU de commande CNP

Toutes les unités TPDU de commande du protocole CNP utiliseront les valeurs d'octet suivantes pour les champs d'en-tête:

Indicateur LI 0000 0001

Code TPDU 0100 0111

Le champ de données de ces unités TPDU se constituera d'une structure **CNPControlPDU** codée en utilisant la notation ASN.1, telle qu'elle est définie au B.9.6, Définitions ASN.1. Les champs composant cette structure sont décrits ci-dessous.

B.9.3.1 Eléments d'information communs

Certaines parties de la description ASN.1 du protocole CNP sont issues d'autres sources, à savoir:

1) le champ **Priority** est déduit de l'Annexe A/T.125 (1998) – *Spécification du protocole du service de communication multipoint*.

2) les champs **H221NonStandard, NonStandardIdentifier, NonStandardParameter** et **AliasAddress** (ainsi que les sous-types nécessaires, tels que **TransportAddress** et **PartyNumber**) sont déduits de la Recommandation H.225.0 (1998) – *Protocoles de signalisation d'appel et mise en paquets d'un train multimédia pour des systèmes de communication multimédias en mode paquet*.

ReliableTransportProtocol (*protocole de transport fiable*) – Spécifie un protocole de transport fiable unique ainsi que ses conditions d'utilisation. Cette structure contient les éléments suivants:

– **type**: spécifie un protocole CNP, X.224, MAP ou un protocole non normalisé;

– **maxTPDUSize** (*taille maximale d'unité TPDU*): indique la taille maximale (en octets) prise en charge par une unité TPDU unique, y compris l'en-tête;

– **nonStandardParameters** (*paramètres non normalisés*): contient des informations qui ne sont pas définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

ReliableSecurityProtocol (*protocole de sécurité fiable*) – Spécifie un protocole de sécurité unique utilisé avec transfert de données fiable. Cette valeur spécifiera l'un des protocoles suivants:

- aucun;
- protocole TLS;
- protocole SSL;
- protocole IPSec (avec une gestion de clé IKE ou manuelle);
- protocole X.274 (avec ou sans prise en charge d'identificateur SA);
- protocole GSS-API
- protocole physique[1];
- protocole non normalisé.

UnreliableTransportProtocol (*protocole de transport non fiable*) – Spécifie un protocole de transport non fiable unique ainsi que ses conditions d'utilisation. Cette structure contient les éléments suivants:

---

[1] Indique l'existence d'une connexion sécurisée physiquement entre les nœuds connectés qui fournit des communications fiables. La vérification de l'existence de cette situation est un problème d'implémentation qui est en dehors du domaine d'application de la présente Recommandation. Il convient de noter que cette condition doit être proposée et acceptée lors de l'établissement de la connexion pour être considérée comme effective.

- **type** – Spécifie le protocole X.234 ou un protocole non normalisé;
- **maxTPDUSize** – Indique la taille maximale (en octets) prise en charge par une unité TPDU unique, y compris l'en-tête;
- **sourceAddress** (*adresse source*) – Adresse réseau devant être utilisée conjointement à ce protocole. Il s'agit de l'adresse de l'émetteur de la structure **UnreliableTransportProtocol** qui sera utilisée pour la réception de données non fiables pour la connexion en cours de négociation;
- **sourceTSAP** (*point TSAP source*) – Point TSAP devant être utilisé conjointement à ce protocole. L'émetteur de la structure **UnreliableTransportProtocol** peut utiliser cet identificateur pour faire la distinction entre des données issues de cette connexion ou d'autres connexions, lorsque ces données sont reçues à une même adresse réseau;
- **nonStandardParameters** – Informations non définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

UnreliableSecurityProtocol (*protocole de sécurité non fiable*) – Spécifie un protocole de sécurité unique utilisé avec un transfert de données non fiable. Cette valeur spécifiera l'un des protocoles suivants:

- aucun;
- protocole IPSec (avec une gestion de clé IKE ou manuelle);
- protocole X.274 (avec ou sans prise en charge d'identificateur SA);
- protocole physique[2];
- protocole non normalisé.

B.9.3.2 Connect Request (*demande de connexion*)

protocolIdentifier (*identificateur de protocole*) – Version du protocole CNP prise en charge par l'appelant.

reconnectRequested (*nouvelle connexion demandée*) – Lorsqu'un nœud appelé reçoit une demande de connexion avec ce champ positionné sur Vrai, il répondra au moyen d'une demande de déconnexion. Ce champ devrait être positionné sur Vrai par le nœud appelant dans une demande de connexion X.224 encapsulée lorsque la totalité des informations de connexion ne correspond pas aux contraintes de taille de l'unité TPDU *CR*. Le protocole CNP devrait être négocié dans un tel cas pour la nouvelle connexion de manière à permettre l'échange de l'ensemble complet des informations de connexion.

priority – Priorité des données devant être émises sur cette connexion de transport. La connexion sera utilisée pour le transfert de données de priorité quelconque si ce champ est absent.

reliableTransportProtocols – Liste des protocoles de transport fiables pris en charge par le nœud appelant, classés par ordre de préférence. L'utilisation du protocole se poursuivra si ce champ est omis.

reliableSecurityProtocols – Liste des protocoles de sécurité fiables pris en charge par le nœud appelant, classés par ordre de préférence. L'absence de ce champ indique que l'appelant ne prend pas en charge des protocoles de sécurité fiables.

---

[2] Indique l'existence d'une connexion sécurisée physiquement entre les nœuds connectés qui fournit des communications non fiables. La vérification de l'existence de cette situation est un problème d'implémentation qui est en dehors du domaine d'application de la présente Recommandation. Il convient de noter que cette condition doit être proposée et acceptée lors de l'établissement de la connexion pour être considérée comme effective.

unreliableTransportProtocols – Liste des protocoles de transport non fiables pris en charge par le nœud appelant, classés par ordre de préférence. L'absence de ce champ indique que l'appelant ne prend pas en charge des protocoles de transport non fiables.

unreliableSecurityProtocols – Liste des protocoles de sécurité non fiables pris en charge par le nœud appelant, classés par ordre de préférence. L'absence de ce champ indique que l'appelant ne prend pas en charge des protocoles de sécurité non fiables.

destinationAddress (*adresse de destination*) – Liste d'une succession d'alias de transport utilisés pour l'établissement de la connexion.

nonStandardParameters – Informations non définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

B.9.3.3 Connect Confirm (*confirmation de connexion*)

protocolIdentifier – Version du protocole CNP devant être utilisée par cette connexion de transport.

reliableTransportProtocol – Protocole de transport fiable devant être utilisé par cette connexion de transport. L'utilisation du protocole existant (X.224 ou CNP) se poursuivra si ce champ est absent.

reliableSecurityProtocol – Protocole de sécurité fiable devant être utilisé par cette connexion de transport. L'absence de ce champ indique que cette connexion n'utilisera pas de protocole de sécurité fiable.

unreliableTransportProtocol – Protocole de transport non fiable devant être utilisé par cette connexion de transport. L'absence de ce champ indique que cette connexion n'utilisera pas de protocole de transport non fiable.

unreliableSecurityProtocol – Protocole de sécurité non fiable devant être utilisé par cette connexion de transport. L'absence de ce champ indique que cette connexion n'utilisera pas de protocole de sécurité non fiable.

nonStandardParameters – Informations non définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

B.9.3.4 Disconnect Request (*demande de déconnexion*)

disconnectReason (*motif de déconnexion*) – Motif de la déconnexion. Ce champ peut prendre les valeurs suivantes:

- **unacceptableVersion** (*version non acceptable*) – Emis en réponse à une demande de connexion, ce champ indique que la version de protocole CNP utilisée dans la demande de connexion n'est pas acceptable;
- **incompatibleParameters** (*paramètres incompatibles*) **–** Emis en réponse à une demande de connexion, ce champ indique qu'il n'a pas été possible de déterminer un ensemble commun de paramètres de connexion valides;
- **securityDenied** (*refus de sécurité*) – Indique que les politiques locales de sécurité n'ont pas autorisé l'établissement de la connexion[3] ou la poursuite du fonctionnement d'une connexion établie;
- **destinationUnreachable** (*destination inaccessible*) – Emis en réponse à une demande de connexion, ce champ indique que le nœud appelé ne peut pas réaliser la connexion telle qu'elle est spécifiée par l'appelant;

---

[3] L'émission d'une unité TPDU *DR* dans le champ optionnel (tel qu'il est décrit au B.7.1.5, Refus de connexion) est acceptable si le nœud appelé ne souhaite pas révéler le motif de rejet d'une tentative de connexion.

- **userRejected** (*utilisateur rejeté*) – Emis en réponse à une demande de connexion, ce champ indique que la tentative de connexion a été rejetée à un niveau supérieur à celui du transport;
- **userInitiated** (*à l'initiative de l'utilisateur*) – Emis après l'établissement de la connexion, ce champ indique qu'une déconnexion a été demandée à un niveau supérieur à celui du transport;
- **protocolError** (*erreur de protocole*) – Indique qu'une erreur fatale s'est manifestée lors du traitement d'une unité TPDU;
- **unspecifiedFailure** (*défaillance non spécifiée*) – Une erreur non spécifique s'est manifestée;
- **routeToAlternate** (*acheminement vers une autre destination*) – Emis en réponse à une demande de connexion, ce champ indique qu'une connexion est souhaitée, mais que l'appelant devrait tenter d'établir une nouvelle connexion en utilisant les informations contenues dans les champs restants;
- **nonStandardDisconnectReason** (*motif de déconnexion non normalisé*) – Motif non défini dans la présente Recommandation (par exemple, propre au fournisseur).

reliableTransportProtocol – Protocole de transport fiable devant être utilisé après une nouvelle connexion. L'utilisation du protocole X.224 se poursuivra si ce champ est absent. Ce champ est uniquement valide si la valeur du champ **disconnectReason** est égale à **routeToAlternate**.

reliableSecurityProtocol – Protocole de sécurité fiable devant être utilisé après une nouvelle connexion. L'absence de ce champ indique qu'un protocole de sécurité fiable ne sera pas utilisé après une nouvelle connexion. Ce champ est uniquement valide si la valeur du champ **disconnectReason** est égale à **routeToAlternate**.

unreliableTransportProtocol – Protocole de transport non fiable devant être utilisé après une nouvelle connexion. L'absence de ce champ indique qu'un protocole de transport non fiable ne sera pas utilisé après une nouvelle connexion. Ce champ est uniquement valide si la valeur du champ **disconnectReason** est égale à **routeToAlternate**.

unreliableSecurityProtocol – Protocole de sécurité non fiable devant être utilisé après une nouvelle connexion. L'absence de ce champ indique qu'un protocole de sécurité non fiable ne sera pas utilisé après une nouvelle connexion. Ce champ est uniquement valide si la valeur du champ **disconnectReason** est égale à **routeToAlternate**.

destinationAddress – Liste d'une succession d'alias de transport utilisés pour l'établissement de la connexion. Ce champ est uniquement valide si la valeur du champ **disconnectReason** est égale à **routeToAlternate**.

nonStandardParameters – Informations non définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

B.9.3.5 **Error** (*erreur*)

rejectCause (*motif de rejet*) – Motif du rejet de l'unité PDU. Ce champ peut prendre l'une des valeurs suivantes:

- **unrecognizedPDU** (*unité PDU non reconnue*) – Indique que l'unité PDU n'a pas pu être décodée sous une forme reconnaissable;
- **invalidParameter** (*paramètre non valide*) – Indique que l'unité PDU contenait une ou plusieurs valeurs de paramètre non valides;
- **causeUnspecified** – Motif non spécifique;
- **nonStandardRejectCause** (*motif de rejet non normalisé*) – Motif non défini dans la présente Recommandation (par exemple, un motif propre au fournisseur).

rejectedPDU – Unité PDU rejetée.

nonStandardParameters – Informations non définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

B.9.3.6 Unité PDU non normalisée

nonStandardParameters – Informations non définies dans la présente Recommandation (par exemple, des données propres au fournisseur).

B.9.4 Unité TPDU de données

B.9.4.1 Structure

La Figure B.19 présente la structure des unités TPDU de données du protocole CNP.

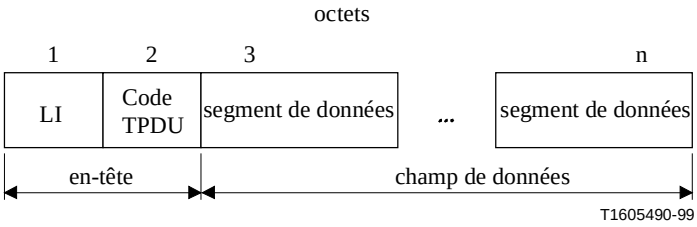


Figure B.19/T.123 – Structure de l'unité TPDU de données du protocole CNP

Toutes les unités TPDU de commande du protocole CNP utiliseront les valeurs d'octet suivantes pour les champs d'en-tête:

Indicateur LI 0000 0001

Code TPDU 0100 0110

Le champ de données pour une unité TPDU de données consistera en un ou plusieurs segments de données, comme décrit ci-dessous.

B.9.4.2 Segments de données

La Figure B.20 présente la structure du segment de données.

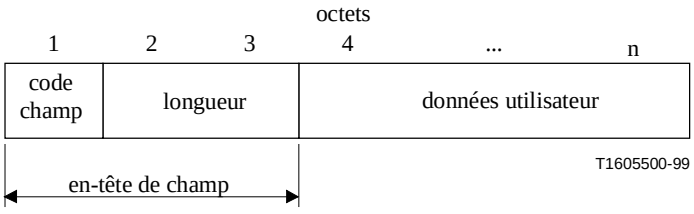


Figure B.20/T.123 – Structure de l'unité TPDU de données du protocole CNP

Un segment de données est une structure d'octet se composant d'un en-tête de longueur fixe suivi d'un nombre variable d'octets de données utilisateur.

Un segment de données doit contenir les paramètres suivants:

a) Code champ (octet 1)

Longueur du paramètre: un octet

Valeur du paramètre: 000y zzzz:

y est l'indicateur de dernier segment d'un paquet de données; le positionnement y sur 1 indique le dernier segment.

zzzz est une valeur binaire égale à la priorité MCS des données.

b) Longueur (octets 2 et 3)

Longueur du paramètre: deux octets

Valeur du paramètre: valeur binaire indiquant le nombre *L* d'octets de données utilisateur avec une valeur maximale de 65530.

c) Données utilisateur (octet 4 à octet *L*+4)

Longueur du paramètre: ***L*** octets.

Valeur du paramètre: octets de données utilisateur.

B.9.5 Utilisation du protocole CNP avec le protocole X.224

B.9.5.1 Encapsulation des unités TPDU

Les unités TPDU du protocole CNP seront encapsulées de la manière suivante dans des unités TPDU X.224 pendant les procédures de connexion décrites au B.7.1, Etablissement de la connexion initiale:

– le champ *TRANSPORT-SELECTOR* d'une unité TPDU *CR* contiendra une unité **Connect Request TPDU**;

– le champ *TRANSPORT-SELECTOR* d'une unité TPDU *CC* contiendra une unité **Connect Confirm TPDU**;

– la partie variable d'une unité TPDU *DR* contiendra une unité **Disconnect Request TPDU** ou une unité **Error TPDU**.

B.9.5.2 Procédure de nouvelle connexion

– Si le protocole de transport fiable indiqué dans une unité **Connect Confirm TPDU** est le protocole X.224, l'un ou l'autre des côtés peut alors émettre immédiatement une unité TPDU *DATA (DT)* ou toute autre unité PDU de protocole X.224 valide.

– Si le protocole de transport fiable indiqué dans une unité **Connect Confirm TPDU** est le protocole CNP, l'un ou l'autre des côtés peut alors émettre immédiatement une unité **Data TPDU** ou toute autre unité PDU de protocole CNP valide.

– Si le protocole de transport fiable indiqué dans une unité **Connect Confirm TPDU** est aucun des protocoles X.224 ou CNP, le nœud appelant et le nœud appelé appliqueront la procédure complète d'établissement de connexion pour le protocole sélectionné (c'est-à-dire que l'appelant émettra l'unité PDU adéquate de demande de connexion).

B.9.6 Définitions ASN.1

```
--*****************************************************************************
--*   Définitions ASN.1 des unités PDU de commande du protocole CNP
--*****************************************************************************

CNP-PROTOCOL {itu-t (0) recommendation (0) t (20) 123 annexb (2) 1}

DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
```

```
--
--  Définitions importées
--

IMPORTS
      NonStandardParameter,
      TransportAddress,
      AliasAddress
   FROM H323-MESSAGES
         -- H.225.0 Version 2
         -- {itu-t (0) recommendation (0) h (8) 2250 version (0) 2}

      Priority
   FROM MAP-PROTOCOL;
         -- T.125 Annexe A Version 1

ProtocolIdentifier ::= OBJECT IDENTIFIER
   -- sera positionné sur la valeur
   -- {itu-t (0) recommendation (0) t (20) 123 annexb (2) 1}

--
--  Types de négociation de service
--

TPDUSize ::= INTEGER (128..65535)

ReliableTransportProtocolType ::= CHOICE
{
   cnp                              NULL,
   x224                             NULL,
   map                              NULL,
   nonStandardTransportProtocol     NonStandardParameter,
   ...
}

ReliableTransportProtocol ::= SEQUENCE
{
   type                       ReliableTransportProtocolType,
   maxTPDUSize                TPDUSize,
   nonStandardParameters      SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

ReliableSecurityProtocol ::= CHOICE
{
   none              NULL,
   tls               NULL,
   ssl               NULL,
   ipsecIKEKeyManagement      NULL,
   ipsecManualKeyManagement   NULL,
   x274WithoutSAID            NULL,
   x274WithSAID               X274WithSAIDInfo,
    gssApi                    NULL,
   physical                   NULL,
   nonStandardSecurityProtocol NonStandardParameter,
   ...
}
```

```
UnreliableTransportProtocolType ::= CHOICE
{
   x234                              NULL,
   nonStandardTransportProtocol      NonStandardParameter,
   ...
}

UnreliableTransportProtocol ::= SEQUENCE
{
   type                              UnreliableTransportProtocolType,
   maxTPDUSize                       TPDUSize,
   sourceAddress                     TransportAddress,
   sourceTSAP                        OCTET STRING OPTIONAL,
   nonStandardParameters             SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

UnreliableSecurityProtocol ::= CHOICE
{
   none                              NULL,
   ipsecIKEKeyManagement             NULL,
   ipsecManualKeyManagement          NULL,
   x274WithoutSAID                   NULL,
   x274WithSAID                      X274WithSAIDInfo,
   physical                          NULL,
   nonStandardSecurityProtocol       NonStandardParameter,
   ...
}

X274WithSAIDInfo ::= SEQUENCE
{
   localSAID                         OCTET STRING,
   peerSAID                          OCTET STRING,
   ...
}

--
-- Types d'unités PDU de commande du protocole CNP
--

ConnectRequestPDU ::= SEQUENCE
{
   protocolIdentifier                ProtocolIdentifier,
   reconnectRequested                BOOLEAN,
   priority                          Priority OPTIONAL,
   reliableTransportProtocols        SEQUENCE OF ReliableTransportProtocol OPTIONAL,
   reliableSecurityProtocols         SEQUENCE OF ReliableSecurityProtocol OPTIONAL,
   unreliableTransportProtocols      SEQUENCE OF UnreliableTransportProtocol OPTIONAL,
   unreliableSecurityProtocols       SEQUENCE OF UnreliableSecurityProtocol OPTIONAL,
   destinationAddress                SEQUENCE OF AliasAddress OPTIONAL,
   nonStandardParameters             SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

ConnectConfirmPDU ::= SEQUENCE
{
   protocolIdentifier                ProtocolIdentifier,
   reliableTransportProtocol         ReliableTransportProtocol OPTIONAL,
   reliableSecurityProtocol          ReliableSecurityProtocol OPTIONAL,
   unreliableTransportProtocol       UnreliableTransportProtocol OPTIONAL,
```

```
   unreliableSecurityProtocol          UnreliableSecurityProtocol OPTIONAL,
   nonStandardParameters               SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

DisconnectReason ::= CHOICE
{
   unacceptableVersion                 NULL,
   incompatibleParameters              NULL,
   securityDenied                      NULL,
   destinationUnreachable              NULL,
   userRejected                        NULL,
   userInitiated                       NULL,
   protocolError                       NULL,
   unspecifiedFailure                  NULL,
   routeToAlternate                    NULL,
   nonStandardDisconnectReason         NonStandardParameter,
   ...
}

DisconnectRequestPDU ::= SEQUENCE
{
   disconnectReason                    DisconnectReason,
   reliableTransportProtocol           ReliableTransportProtocol OPTIONAL,
   reliableSecurityProtocol            ReliableSecurityProtocol OPTIONAL,
   unreliableTransportProtocol         UnreliableTransportProtocol OPTIONAL,
   unreliableSecurityProtocol          UnreliableSecurityProtocol OPTIONAL,
   destinationAddress                  SEQUENCE OF AliasAddress OPTIONAL,
   nonStandardParameters               SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

RejectCause ::= CHOICE
{
   unrecognizedPDU             NULL,
   invalidParameter            NULL,
   causeUnspecified            NULL,
   nonStandardRejectCause      NonStandardParameter,
   ...
}

ErrorPDU ::= SEQUENCE
{
   rejectCause                 RejectCause,
   rejectedPDU                 OCTET STRING,
   nonStandardParameters       SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

NonStandardPDU ::= SEQUENCE
{
   nonStandardParameters       SEQUENCE OF NonStandardParameter OPTIONAL,
   ...
}

CNPControlPDU ::= CHOICE
{
   connectRequest          ConnectRequestPDU,
   connectConfirm          ConnectConfirmPDU,
   disconnectRequest       DisconnectRequestPDU,
```

```
    error                   ErrorPDU,
    nonStandardCNPPDU       NonStandardPDU,
    ...
}

END
```

B.10 Protocole non fiable de segmentation et de réassemblage

B.10.1 Aperçu général

Ce protocole a été conçu pour une utilisation sur des connexions non fiables en mode paquet; il se base sur la fonction de segmentation et de réassemblage SAR définie dans la Norme RFC 791 "protocole Internet". Le protocole définit une unité PDU unique qui permettra à un émetteur de segmenter une unité TSDU sous la forme d'une ou plusieurs unités TPDU de taille suffisamment réduite pour pouvoir être transmises par une couche Réseau sous-jacente qui impose des contraintes de taille. Les segments TPDU peuvent être réassemblés au niveau du récepteur en vue de fournir la totalité de l'unité TSDU d'origine à une couche Réseau supérieure. Ce protocole suppose que les paquets reçus ne sont pas altérés, mais que leur livraison est garantie ou ordonnée.

B.10.2 Structure des unités TPDU SAR non fiables

Toutes les unités de données protocolaires de transport SAR contiendront un nombre entier d'octets. Lorsque des octets consécutifs sont utilisés pour représenter un nombre binaire, l'octet de numéro le plus faible possédera la valeur la plus significative. Les entités SAR de transport non fiable respecteront les conventions de succession des bits et des octets, ce qui permettra une communication.

Il convient de noter que les problèmes de remise en ordre éventuelle des fragments sont une affaire d'implémentation.

La Figure B.21 présente la structure d'une unité TPDU SAR non fiable.

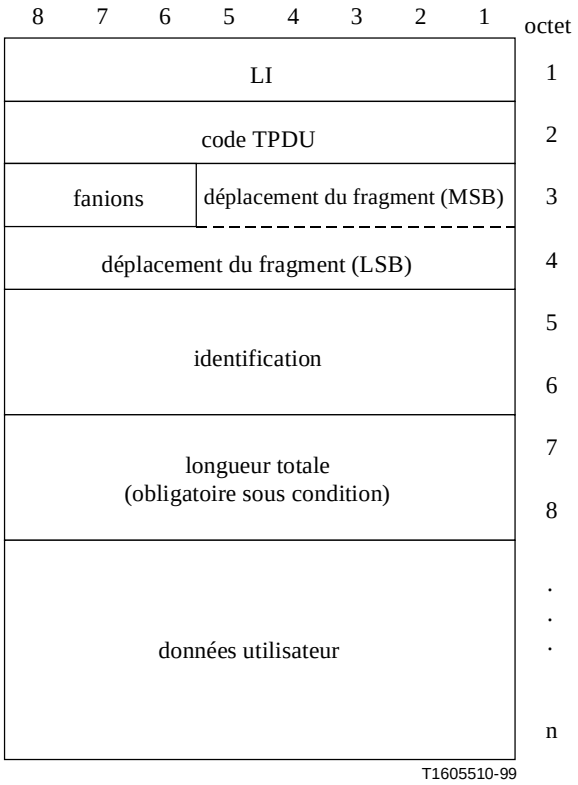


Figure B.21/T.123 – Structure d'unité TPDU SAR non fiable

Les unités TPDU SAR non fiables contiendront, dans l'ordre, les informations suivantes:

- en-tête, avec les champs suivants:
  a) indicateur de longueur (LI)
  b) code TPDU
  c) fanions
  d) déplacement du fragment
  e) identification
  f) longueur totale (sous condition)
- champ de données utilisateur

B.10.2.1 Champ "indicateur de longueur"

Longueur du champ: un octet

Valeur du champ: valeur binaire indiquant la taille de l'en-tête en octets, compte tenu des champs optionnels, mais pas du champ "indicateur de longueur" et des données utilisateur.

B.10.2.2 Code TPDU

Longueur du champ: un octet

Valeur du champ: valeur binaire: 0100 0110

B.10.2.3 Champ de fanion

Longueur du champ: 3 bits

Valeur du champ:

Bit 8: réservé, doit être positionné sur 0

Bit 7: réservé, doit être positionné sur 0

Bit 6: fanion "segment à suivre" (MF, *more fragments*)

0 = dernier fragment de l'unité TSDU

1 = fragment à suivre dans l'unité TSDU

B.10.2.4 Champ "déplacement du fragment"

Longueur du champ: 13 bits

Valeur du champ: valeur binaire indiquant la position que doit occuper ce fragment dans l'unité TSDU réassemblée. Le déplacement du fragment est exprimé en unités de 8 octets. Le déplacement du premier fragment est nul. Le bit 5 de l'octet 3 correspond au bit le plus significatif de ce champ.

B.10.2.5 Champ d'identification

Longueur du champ: deux octets

Valeur du champ: valeur binaire identifiant les fragments appartenant à un même datagramme. Ce nombre non signé sera nul pour la première unité TPDU émise sur une connexion et sera incrémenté de 1 pour chaque unité TPDU suivante.

B.10.2.6 Champ "longueur totale" (obligatoire sous condition)

Longueur du champ: deux octets

Valeur du champ: valeur binaire indiquant le nombre total d'octets de l'unité TSDU. Cette valeur sera présente dans le premier fragment de toute unité TSDU segmentée en fragments multiples. La valeur sera présente dans chaque ou tout autre fragment.

B.10.2.7 Champ "données utilisateur"

Longueur du champ: variable

Valeur du champ: octets de données utilisateur

Bibliographie

– RFC 2078 de l'IETF (janvier 1997), *Generic Security Service Application Program Interface* (interface de programmation d'application pour services de sécurité génériques, GSS-API)

APPENDICE I

Etablissement d'appel de conférence multimédia dans le RNIS

I.1 Introduction

Les terminaux de conférence multimédia (MMC, *multimedia conference*) qui font actuellement l'objet d'une normalisation à l'UIT-T, sont destinés fondamentalement à fonctionner dans le RNIS. Toutefois, divers terminaux de différents types tels que les postes téléphoniques, les télécopieurs du Groupe 4, les vidéophones et les systèmes de téléconférence sont, eux aussi, connectés au RNIS.

Les scénarios suivants sont extraits de la Recommandation Q.931, qui donne de plus amples renseignements et décrit d'autres possibilités. Il convient de prêter attention au codage des éléments d'information pour la capacité support (BC), la capacité de couche inférieure (LLC) et la capacité de couche supérieure (HLC), en raison de l'importance qu'ils revêtent pour l'interfonctionnement.

Le Tableau I.1 propose des valeurs pouvant être utilisées dans un message SETUP. Le terminal du côté appelé doit aussi accepter d'autres valeurs des éléments d'information pour les capacités BC, LLC et HLC. D'autres paramètres peuvent être utilisés, dont les suivants: information numérique sans restriction avec tonalités et annonces (UDI-TA, *unrestricted digital information with tones and announcements*), adaptation du débit à 56 kbit/s pour les réseaux avec restriction, double BC/HLC et absence de LLC. Lorsque la HLC est utilisée, la configuration d'acceptation d'appel retenue par l'utilisateur doit permettre la téléphonie à 7 kHz, la visiophonie ou la téléphonie à 3,1 kHz.

Tableau I.1/T.123 – Réglage des paramètres dans le message SETUP au départ

Elément d'information	BC	LLC	HLC
Capacité de transfert des informations	Informations numériques sans restriction	Informations numériques sans restriction	
Mode de transfert	Circuit	Circuit	
Débit de transfert des informations	64 kbit/s	64 kbit/s	
Protocole d'informations d'utilisateur (Couche 1)		H.221	
Identification des caractéristiques de couche supérieure			AC[a)]

[a)] AC téléconférence multimédia (*audiographic teleconference*)

VC (vidéoconférence), VP (vidéophone) et AV (audiovisuel) sont acceptables pour ce qui est du côté appelé.

I.2 Prescriptions de base

Il est nécessaire de remplir, pour l'essentiel, les conditions suivantes:

1) un terminal MMC possède la capacité intrinsèque d'interfonctionnement avec le RNIS et il est directement connecté à ce réseau en un point S (T);

2) un terminal MMC permet d'établir des communications avec les terminaux suivants:

   a) un autre terminal MMC;

   b) un vidéophone, un terminal de téléconférence acceptant la structure de trame conforme à la Recommandation H.221.

   Dans la suite du texte, les terminaux mentionnés aux points a) et b) ci-dessus seront désignés par le sigle AV (audiovisuel).

La demande fondamentale concerne l'intercommunication entre terminaux MMC et téléphones. Or, chaque extrémité utilise des services RNIS différents (par exemple MMC: informations numériques sans restriction, téléphone: parole); ce type d'intercommunication serait donc difficile sans l'emploi de séquences spéciales, comme le décrivent les Figures I.2 et I.3;

3) cette description concerne uniquement les connexions point à point. Le schéma de la séquence est représenté à la Figure I.1.

I.3 Phase de connexion

On peut diviser la procédure de connexion en trois phases, qui sont les suivantes:

1) phase A (protocole du canal D du RNIS) – En utilisant le protocole de signalisation du canal D (voir Recommandation Q.931), un terminal MMC applique la commande d'appel de façon à établir un canal B du RNIS, pour communiquer avec un terminal AV;

2) phase B (protocole H.242) – Un terminal MMC fondé sur la Recommandation H.221 établit un verrouillage de trames, choisit un mode de communication fondé sur la séquence H.242 (mode MMC/mode parole) et établit le conduit en protocole MLP;

3) phase C (protocole de la série T.120) – Si les deux terminaux ont des fonctionnalités MMC et décident de communiquer en mode MMC, le protocole de la Recommandation T.120 est enclenché et la fonction de communication finale est définie de manière détaillée, ce qui conduit au début de la communication proprement dite.

I.4 Phase A (protocole du canal D RNIS)

En appliquant la commande d'appel fondée sur la Recommandation Q.931 (protocole de signalisation du canal D), il convient de régler, dans le message SETUP du côté départ, les paramètres spécifiés dans le Tableau I.1. Toutefois, dans la présente Recommandation, le tableau ne porte que sur les éléments d'information suivants:

1) capacité support (BC, *bearer capability*);

2) capacité de couche inférieure (LLC, *low layer capability*);

3) capacité de couche supérieure (HLC, *high layer capability*),

qui sont tous nécessaires pour reconnaître la capacité de communication des autres terminaux.

Du côté appelant, un terminal MMC doit régler les paramètres ci-dessus dans le message SETUP pour l'envoi, alors que du côté appelé, il doit vérifier les paramètres de façon à statuer sur la possibilité d'une communication. S'il trouve qu'il est possible de communiquer, il peut accepter l'appel et établir une connexion avec un canal B. Par la suite, le terminal MMC commence à communiquer avec un terminal audiovisuel qui peut être un autre terminal MMC ou un autre type de terminal audiovisuel tel qu'un vidéophone.

I.5 Phase B (protocole H.242)

Après connexion au canal B, il convient d'appliquer les procédures ci-après, fondées sur la Recommandation H.242:

1) le mode à choisir est le verrouillage de trames conforme à la Recommandation H.221. Puis, en utilisant le signal d'allocation dynamique de débit (BAS), la séquence d'échange de capacités est exécutée en mode MIC sur 7 éléments binaires (mode 0F);

2) après avoir reconnu mutuellement leurs capacités, les deux côtés décident de leur propre mode de communication et notamment d'un mode commun. Autrement dit, lorsque les deux côtés ont la certitude de posséder une capacité de protocole MLP, le conduit MLP est établi et le protocole T.120 est enclenché, ce qui conduit à la phase C;

3) si un côté ne possède pas de capacité MLP, les communications seront limitées au mode audio et éventuellement vidéo (par exemple si un côté est un terminal MMC et l'autre un vidéophone).

I.6 Phase C (protocole de la série T.120)

1) établir une connexion de liaison de données sur le conduit MLP;

2) établir la Couche 4;

3) après établissement des canaux conformément à la Recommandation T.125, les négociations qui se déroulent en vue de reconnaître la fonction de chaque côté concernant MMC et les informations nécessaires à la conférence sont échangées par commande généralisée de conférence après consultation de la liste des applications.

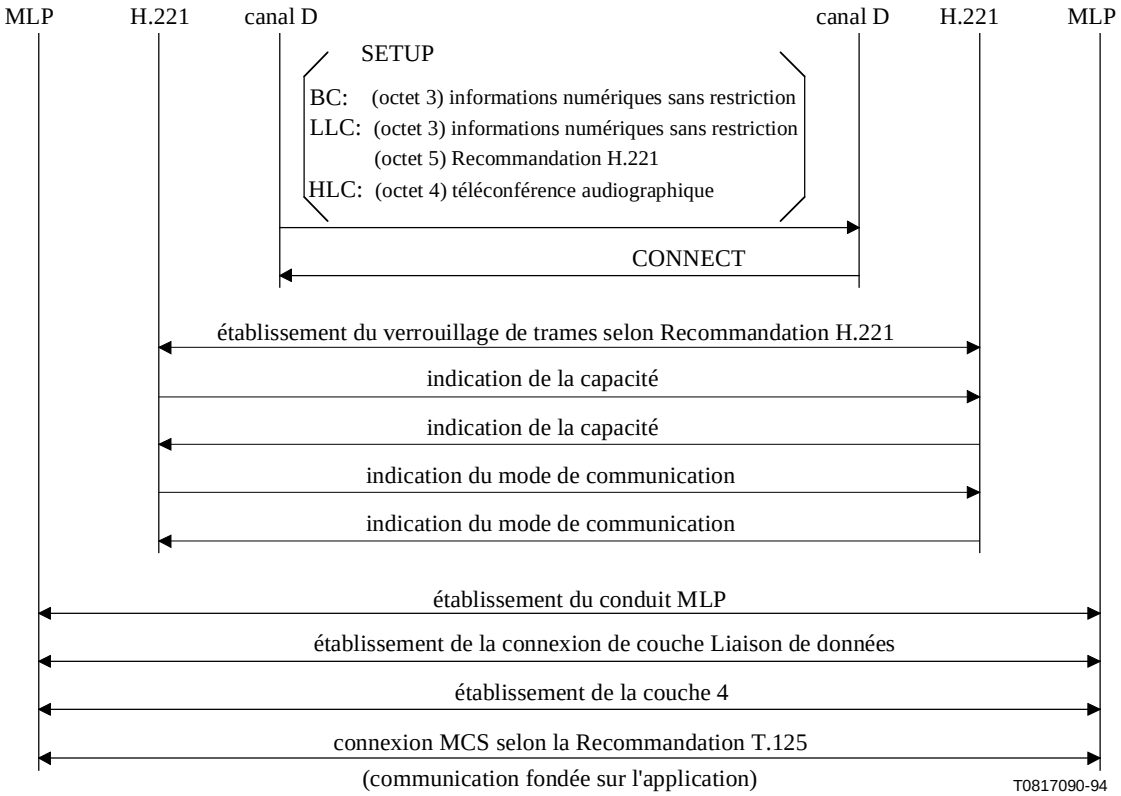
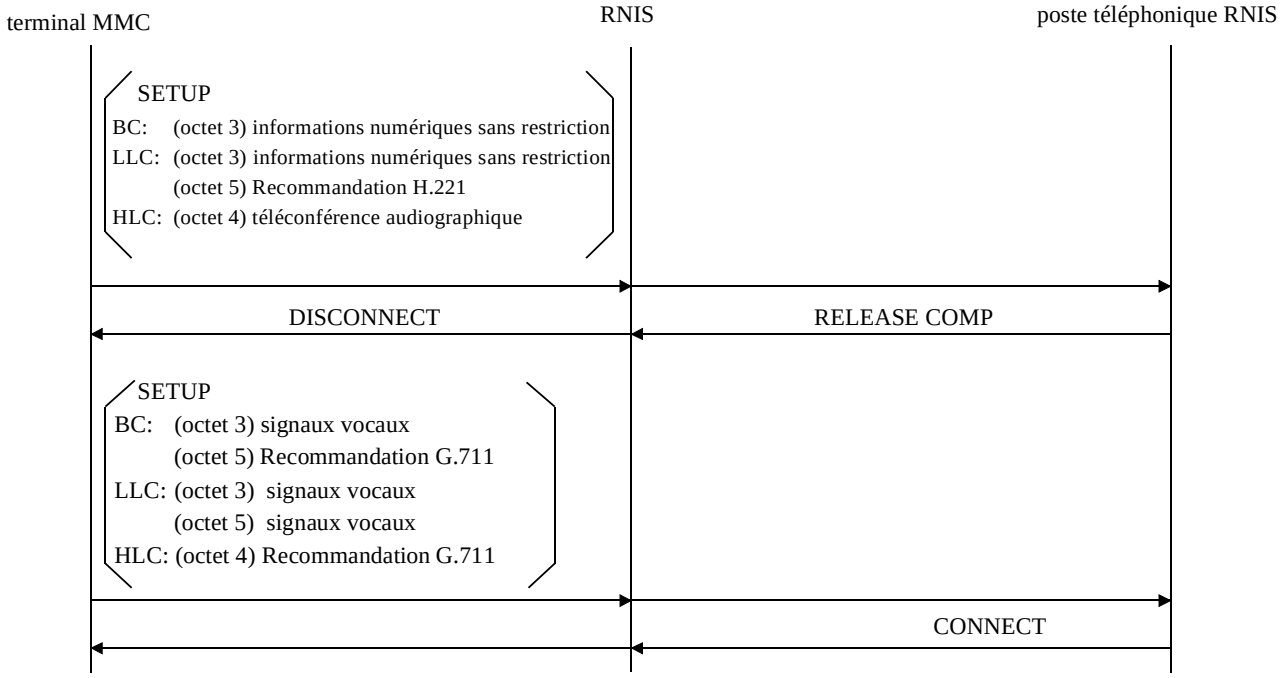


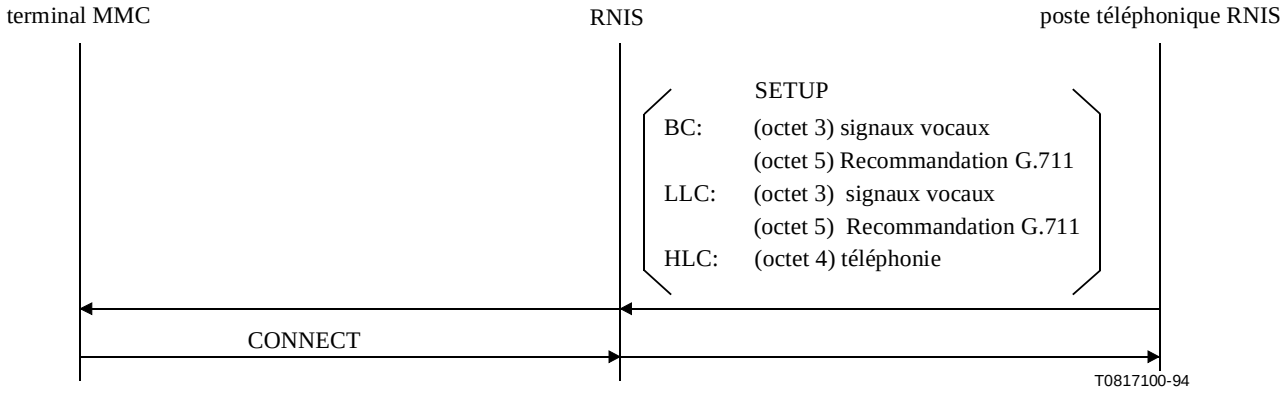
Figure I.1/T.123 – Séquence d'établissement de la communication pour terminaux MMC

1) appel d'un poste téléphonique RNIS par un terminal MMC



(communication par l'intermédiaire du service de signaux)

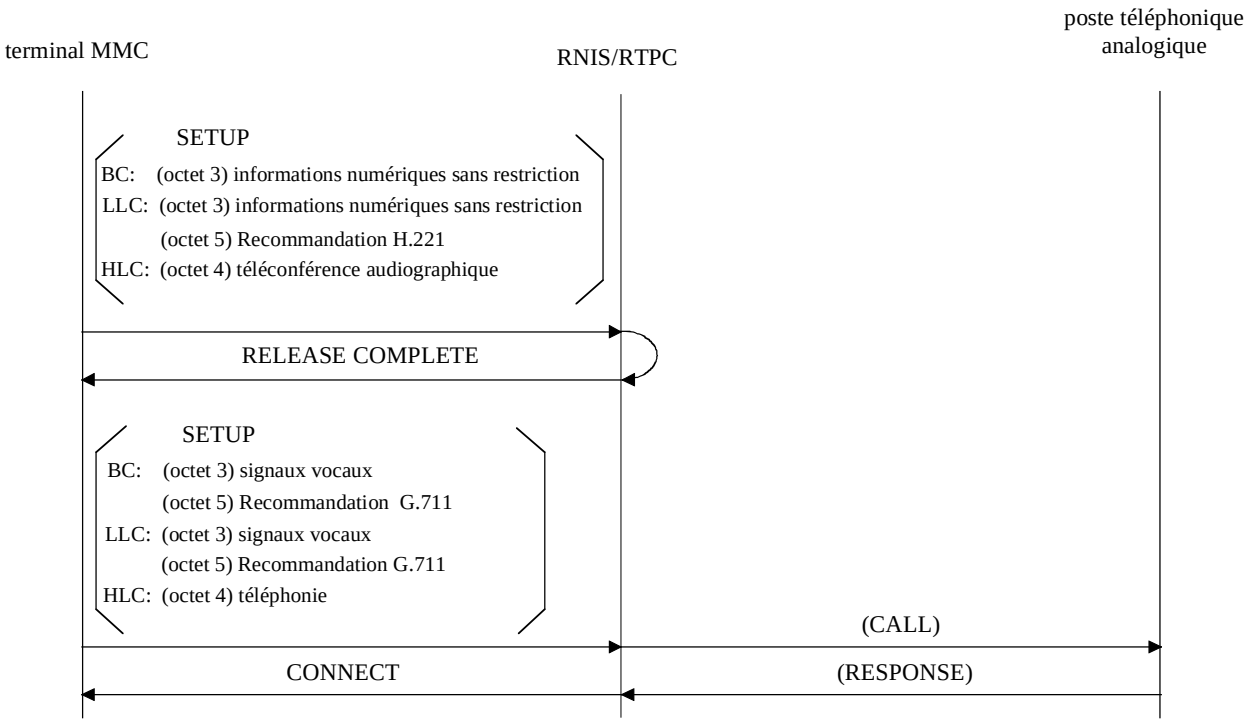
2) appel d'un terminal MMC par un poste téléphonique RNIS



(communication par l'intermédiaire du service de signaux)

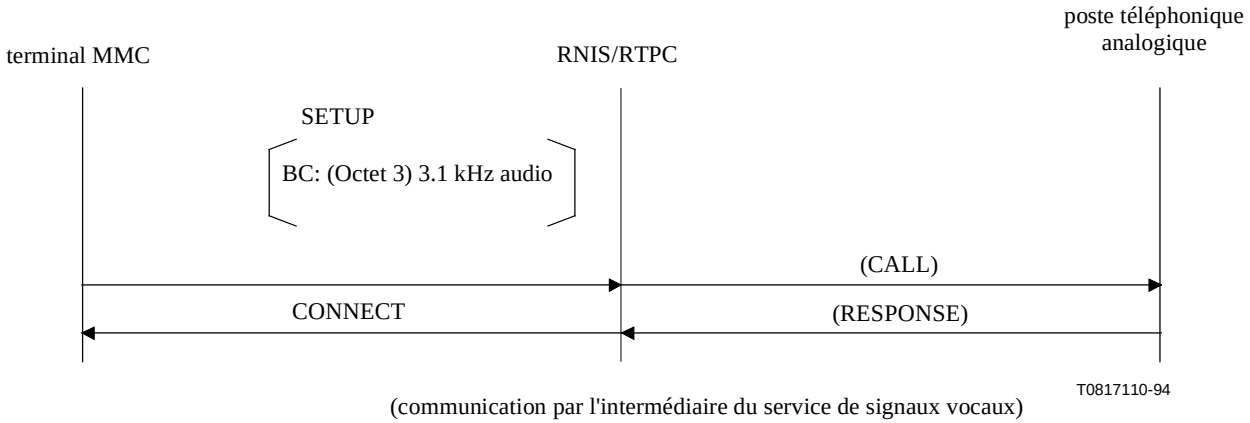
Figure I.2/T.123 – Séquences d'intercommunication entre terminal MMC et poste téléphonique RNIS

3) appel d'un poste téléphonique analogique par un terminal MMC



(communication par l'intermédiaire du service de signaux vocaux)

4) appel d'un terminal MMC par un poste téléphonique analogique



(communication par l'intermédiaire du service de signaux vocaux)

Figure I.3/T.123 – Séquences d'intercommunication entre terminal MMC et téléphones analogiques

APPENDICE II

Cadre de sécurité GSS-API

II.1 Introduction

Le présent appendice donne des détails sur le cadre de sécurité défini dans l'Annexe B sur la base du cadre de sécurité: interface de programmation d'application pour services de sécurité génériques (GSS-API, *generic security service-application programming interface*).

II.2 Technique d'authentification commune de l'IETF (CAT, *common authentication technology*)

Le présent sous-paragraphe donne des précisions sur les divers travaux relatifs à la sécurité qui sont effectués par l'IETF en rapport avec le cadre de sécurité GSS-API.

II.2.1 IETF et groupe de travail CAT

Le groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*) a regroupé ses travaux relatifs à la sécurité dans un seul cadre qui est maintenant couramment utilisé pour tous les protocoles de l'IETF. La Norme RFC 1511, intitulée "Common Authentication Technology Overview" (aperçu de la technique d'authentification commune ou CAT) présente ces travaux ainsi que leur objectif.

II.2.2 Cadre de sécurité GSS-API

Le cadre de sécurité du groupe de travail CAT est reflété par le cadre de sécurité GSS-API dans la Norme RFC 1508. Le cadre de sécurité GSS-API est une interface API qui donne un ensemble bien défini de structures de données pour la communication sur un canal fiable entre deux entités en négociation. La Norme RFC 2078, *Generic Security* fournit des explications sur le cadre de sécurité.

II.2.3 SPNEGO

La négociation du contexte de sécurité GSS-API peut poser problème. Il est possible de prendre en charge plusieurs mécanismes de sécurité au sein du cadre de sécurité GSS-API. Toutefois, il n'existe pas de moyen permettant d'identifier le mécanisme de sécurité auquel se rapporte un jeton opaque. En fait, à la réception du premier jeton, une application appelante du cadre de sécurité GSS-API doit tenter de valider le jeton pour chaque mécanisme de sécurité installé, jusqu'à ce qu'il y ait validation (ou jusqu'au dernier échec). Cette approche permet d'aboutir sans ambiguïté à la conclusion correcte, mais elle est inefficace. Pour optimiser l'utilisation du cadre de sécurité GSS-API, le groupe de travail CAT définit un mécanisme de sécurité permettant une négociation simple. Le mécanisme de négociation GSS-API simple et protégé – SPNEGO – fait l'objet de la Norme RFC 2478.

II.3 Cadre de sécurité de l'Annexe B/T.123

L'Annexe B définit implicitement un cadre de sécurité pour le protocole T.120. Dans le cas de transmissions fiables, ce cadre a les caractéristiques suivantes.

Une liste de protocoles de sécurité fiables bien connus. Cette liste est extensible, des protocoles non normalisés pouvant y être inclus (c'est-à-dire des protocoles non inclus dans la liste).

Les nœuds qui prennent en charge des connexions de transport étendues peuvent choisir et utiliser un protocole de sécurité parmi ceux qu'ils prennent en charge tous les deux, par un simple mécanisme de négociation de capacité en utilisant les modèles d'appel spécifiés au B.7.

L'appelant transmet un ensemble de protocoles de sécurité fiables qu'il prend en charge dans l'unité ConnectRequestPDU CNP.

L'appelé peut signaler si les services disponibles pour la connexion de réseau existante suffisent pour le protocole de sécurité souhaité (en utilisant une unité DisconnectRequestPDU ou ConnectConfirmPDU CNP). Dans l'un ou l'autre cas, l'appelé transmet son choix du protocole de sécurité fiable unique à utiliser (qui doit être un élément de l'ensemble indiqué par l'appelant).

Si les services suffisent, on utilise, pour la connexion T.120, la connexion de réseau existante (le protocole de transport peut être modifié par suite de négociations).

Si les services ne suffisent pas, l'appelant libère la connexion de réseau existante et crée une nouvelle connexion de réseau qui assure les services indiqués par l'appelé dans l'unité DisconnectRequestPDU CNP.

Dans tous les profils étendus définis dans l'Annexe B, la sécurité est un service qui existe implicitement au-dessous de la couche X.224 de classe 0 ou CNP. Toutefois, rien n'interdit d'utiliser un profil non normalisé pouvant être négocié à partir des services fournisseurs (y compris la sécurité) au-dessus de la couche X.224 de classe 0 ou CNP.

II.3.1 Cadre de sécurité GSS-API: acheminement de jetons GSS-API via la couche X.224 de classe 0 ou CNP

Le cadre de sécurité GSS-API implémente un processus au moyen duquel un mécanisme de sécurité crée des jetons opaques pour la communication via un mécanisme fiable (c'est-à-dire un transport) entre deux entités en négociation. Ce processus est en cours pour toute la communication entre les entités, et couvre donc la totalité d'une session. Il inclut non seulement la phase d'établissement d'un contexte de sécurité où les mécanismes de sécurité peuvent être choisis et les pouvoirs échangés mais aussi tout échange ultérieur de données cryptées.

Un exemple d'utilisation courante du cadre de sécurité GSS-API est lorsque l'application invocatrice gère la sécurité d'une session sur la base de la politique de sécurité qui peut être définie localement pour l'application. Par exemple, l'application peut déterminer les protocoles de sécurité à indiquer et les pouvoirs à choisir.

D'autres utilisations du cadre de sécurité GSS-API sont naturellement possibles. Par exemple, un service réseau de système d'exploitation peut établir son propre contexte de sécurité entre deux points d'extrémité. Du fait qu'une application invocatrice de niveau supérieur peut savoir ou ignorer que ce contexte de sécurité existe, il se peut que cette application ne sache pas si elle doit gérer la sécurité de sa session (par exemple, la sécurité IP peut être invoquée par le service réseau, mais cette invocation risque d'être transparente pour une application de niveau supérieur utilisant TCP/IP). Même si elle sait qu'un autre contexte de sécurité existe, l'application peut malgré tout souhaiter gérer sa propre sécurité pour la session.

En conséquence, l'utilisation la plus probable du cadre de sécurité GSS-API dans les Recommandations de la série T.120 est lorsqu'une application T.120 souhaite gérer directement la sécurité d'une session. Se pose alors la question de savoir dans quelle couche l'application T.120 doit décider de placer le flux de jetons GSS-API au cours de la session T.120.

Compte tenu du fait que le cadre GSS-API ne spécifie pas de mécanisme de communication pour son flux de jetons, l'Annexe B spécifie un processus qui signale le cadre de sécurité GSS-API comme étant un protocole de sécurité fiable dans la couche CNP et qui, dans un profil étendu, place le flux de jetons GSS-API dans une couche au-dessus de la composante X.224 de classe 0 de la couche 4 (ou au-dessus de la couche CNP dans le cas où la couche CNP remplace la couche X.224 de classe 0).

SERIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	**Terminaux des services télématiques**
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux pour données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication