UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T G.965

(03/2001)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE G: SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

Sections numériques et systèmes de lignes numériques – Section numérique et systèmes de transmission numériques pour l'accès usager du RNIS

Interfaces V au commutateur numérique local – Interface V5.2 (basée sur la hiérarchie à 2048 kbit/s) pour la prise en charge du réseau d'accès

Recommandation UIT-T G.965

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE G

SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

CONNEXIONS ET CIRCUITS TÉLÉPHONIQUES INTERNATIONAUX	G.100–G.199
CARACTÉRISTIQUES GÉNÉRALES COMMUNES À TOUS LES SYSTÈMES ANALOGIQUES À COURANTS PORTEURS	G.200–G.299
CARACTÉRISTIQUES INDIVIDUELLES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX À COURANTS PORTEURS SUR LIGNES MÉTALLIQUES	G.300–G.399
CARACTÉRISTIQUES GÉNÉRALES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX HERTZIENS OU À SATELLITES ET INTERCONNEXION AVEC LES SYSTÈMES SUR LIGNES MÉTALLIQUES	G.400–G.449
COORDINATION DE LA RADIOTÉLÉPHONIE ET DE LA TÉLÉPHONIE SUR LIGNES	G.450–G.499
EQUIPEMENTS DE TEST	G.500–G.599
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.600–G.699
EQUIPEMENTS TERMINAUX NUMÉRIQUES	G.700–G.799
RÉSEAUX NUMÉRIQUES	G.800–G.899
SECTIONS NUMÉRIQUES ET SYSTÈMES DE LIGNES NUMÉRIQUES	G.900–G.999
Généralités	G.900–G.909
Paramètres pour les systèmes à câbles optiques	G.910–G.919
Sections numériques à débits hiérarchisés multiples de 2048 kbit/s	G.920–G.929
Systèmes numériques de transmission par ligne à débits non hiérarchisés	G.930–G.939
Systèmes de transmission numérique par ligne à supports MRF	G.940–G.949
Systèmes numériques de transmission par ligne	G.950–G.959
Section numérique et systèmes de transmission numériques pour l'accès usager du RNIS	**G.960–G.969**
Systèmes sous-marins à câbles optiques	G.970–G.979
Systèmes de transmission par ligne optique pour les réseaux locaux et les réseaux d'accès	G.980–G.989
Réseaux d'accès	G.990–G.999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T G.965

Interfaces V au commutateur numérique local – Interface V5.2 (basée sur la hiérarchie à 2048 kbit/s) pour la prise en charge du réseau d'accès

Résumé

La présente Recommandation définit une interface de type V (V5.2) pour la connexion d'un réseau d'accès (AN, *access network*) à un commutateur local (CL) acceptant les types d'accès ci-après:

– accès téléphonique analogique;

– accès au débit de base du RNIS avec terminaison NT1 distincte du réseau d'accès ou intégrée dans celui-ci, sur la base de l'UIT-T G.960 et l'UIT-T I.430;

– accès au débit primaire du RNIS avec terminaison NT1 distincte du réseau d'accès ou intégrée dans celui-ci, sur la base de l'UIT-T G.962 et l'UIT-T I.431;

– autres accès analogiques ou numériques pour connexions semi-permanentes sans informations de signalisation associées hors bande,

avec latitude d'affectation de la voie de transfert d'information (voie support) à l'aide d'un protocole de connexion à la voie support disposant d'une fonction de concentration à l'intérieur du réseau d'accès.

La présente Recommandation se fonde sur l'UIT-T G.964 et y fait référence pour les parties qui sont communes avec elle.

Les spécifications électriques et fonctionnelles des liaisons de l'interface sont établies sur la base des parties de l'UIT-T G.703, l'UIT-T G.704 et l'UIT-T G.706 qui traitent des liaisons à 2048 kbit/s. Jusqu'à 16 liaisons peuvent fonctionner en parallèle, formant l'interface V5.2.

La signalisation issue du point d'accès utilisateur du RTPC est convertie en un protocole à stimuli comportant une partie fonctionnelle pour le trajet de signalisation, qui fait appel à un multiplexage de couche 3 pour les informations en provenance des différents accès d'utilisateur.

L'information provenant des canaux D du RNIS est traitée par répétition de trames dans le réseau d'accès (AN) au moyen des mécanismes définis dans l'UIT-T Q.933.

La présente Recommandation définit un protocole de commande qui est utilisé pour l'échange des fonctions d'état et de commande nécessaires à chaque accès pour la coordination avec les procédures de commande d'appel dans le commutateur local.

Un protocole de connexion à la voie support établit et libère sur demande les connexions supports requises identifiées par l'information de signalisation, sous contrôle du commutateur local.

Un protocole de commande de liaison est défini pour la gestion de liaisons multiples afin de gérer l'identification, le blocage et les conditions d'anomalie sur les liaisons.

Afin de coordonner les demandes de trafic dans les divers protocoles, on peut réserver jusqu'à trois voies de communication pour acheminer les différents protocoles et l'information avec répétition de trames. La couche liaison de données pour les protocoles est définie sur la base de l'UIT-T Q.920 et l'UIT-T Q.921.

Un protocole de protection, fonctionnant sur deux liaisons distinctes pour des raisons de sécurité, est défini pour gérer la commutation de protection des voies de communication en cas d'anomalies sur la liaison.

Source

La Recommandation G.965 de l'UIT-T, révisée par la Commission d'études 15 (2001-2004) de l'UIT-T, a été approuvée le 1er mars 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

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.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude 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 1 de l'AMNT.

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, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

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.

TABLE DES MATIÈRES

Introduction

Principales différences entre l'interface V5.1 et l'interface V5.2

La Recommandation spécifiant l'interface V5.1 (UIT-T G.964) est une Recommandation indépendante, alors que la présente Recommandation V5.2 renvoie à certaines parties de l'UIT-T G.964.

L'interface V5.1 n'utilise qu'une liaison à 2048 kbit/s, alors que l'interface V5.2 peut en utiliser jusqu'à seize (16) sur une seule interface.

L'interface V5.1 ne prend pas en charge la concentration, alors que l'interface V5.2 est intrinsèquement conçue pour la prendre en charge à l'aide d'un protocole spécial appelé protocole de connexion à la voie support (BCC, *bearer channel connection*).

L'interface V5.1 ne prend pas en charge les points d'accès utilisateur au débit primaire du RNIS, alors que l'interface V5.2 les accepte.

Le concept de protection de la voie de communication n'existe pas dans V5.1; au contraire, cette fonction est disponible pour l'interface V5.2 lorsqu'elle comporte plusieurs liaisons à 2048 kbit/s. Cette fonction est assortie d'un protocole spécifique, appelé protocole de protection.

Le protocole de commande pour l'interface V5.2 est légèrement modifié par rapport à celui qui est utilisé pour l'interface V5.1.

Un protocole de commande de liaison est spécifié pour l'interface V5.2 car il est nécessaire de gérer plusieurs liaisons.

Les principales modifications suivantes améliorent la présente version de l'UIT-T G.965 par rapport à la version précédente (datée de mars 1995).

- [paragraphe 4]: généralisation des exigences électriques et physiques
- [5.1.1]: la vérification de l'identificateur de liaison n'est pas nécessaire pour une interface V5.2 à liaison unique
- [5.1.2]: amélioration du blocage de liaison dans le cas d'anomalies internes du réseau d'accès
- [8.7.4]: ajout de la référence à V5.1 à propos de la nécessité d'un mécanisme de commande des flux à la couche 2
- [10.3]: ajout des pointeurs à V5.1 pour le contrôle de champ et le type de trame
- [15.4]: le verrouillage d'accès accéléré est une fonction supplémentaire qui réduit les messages sur l'interface V5 pendant les procédures de démarrage
- [16.2.1]: précisions sur les procédures de blocage et de déblocage de liaison
- [16.2.4.3.1]: blocage (et protection) immédiat de liaison sur anomalie interne du réseau d'accès
- [16.2.4.3.4]: améliorations des procédures de déblocage coordonnées
- [16.2.4.3.5]: identification simultanée de liaison (AN + CL), mais avec priorité pour CL sur la même liaison
- [17.3]: généralités sur les types de messages avec des éléments d'information facultatifs: optionnel (O) est changé en conditionnel (C)
- [Figure 22]: l'octet-1 a été changé de 0 × 40 en 0 × 44
- [17.4.2.5/6]: longueur des diagnostics dans l'élément d'information Cause d'erreur de rejet/protocole
- [Figure 24]: ajout d'une Note sur l'utilisation du domaine "extension"
- [17.5.8.1a]: ajout d'un paragraphe sur l'erreur de codification du numéro de référence BCC
- [17.5.8.4/5/6]: ajout d'une Note sur les éléments d'information obligatoires et facultatifs

- [18.1.1]: amélioration de l'introduction au protocole de protection
- [18.1.5]: amélioration du texte sur la surveillance des anomalies de liaison
- [Tableau 62]: ajout du codage pour l'erreur d'identification du canal C logique
- [18.6.6.1a]: ajout d'un paragraphe sur l'erreur d'identification du canal C logique
- [Annexe A]: ajout du paragraphe A.7 "Configuration AN/CL possible en utilisant la norme V5"
- [Annexe C]: cette annexe a été réécrite, pour s'aligner sur l'UIT-T G.964. Lorsqu'un élément est le même, il n'y a que des références à V5.1. Les procédures qui ont été modifiées sont principalement celles qui se rapportent au démarrage, au redémarrage de l'interface et aussi au blocage/déblocage de la liaison. La supervision du processus de démarrage a parfois été ajoutée.
- [Annexe E/Tableau E.2]: ajout de trois éléments d'information sur le RTPC (mesure et affaiblissement)
- [Annexe K.6]: réécriture des règles d'anomalies internes du réseau d'accès
- [Annexe K.10]: ajout d'un paragraphe sur les règles des anomalies de liaison
- [Annexe L]: ajout d'une annexe sur l'interopérabilité

Recommandation UIT-T G.965

Interfaces V au commutateur numérique local – Interface V5.2 (basée sur la hiérarchie à 2048 kbit/s) pour la prise en charge du réseau d'accès

1 Domaine d'application

La présente Recommandation spécifie les caractéristiques électriques, physiques, de procédure et de protocole de l'interface V5.2 située entre un réseau d'accès (AN) et le commutateur local (CL) pour la prise en charge des types d'accès suivants:

– accès téléphonique analogique;

– accès au débit de base RNIS avec système de transmission en ligne conforme à l'UIT-T G.960 [4] dans le cas d'une terminaison NT1 distincte du réseau d'accès;

– accès au débit de base RNIS avec interface utilisateur – réseau conforme à l'UIT-T I.430 [3] côté utilisateur du réseau d'accès (c'est-à-dire, l'interface au point de référence T);

– accès au débit primaire RNIS avec système de transmission en ligne conforme à l'UIT-T G.962 [10] dans le cas d'une terminaison NT1 distincte du réseau d'accès;

– accès au débit primaire RNIS avec interface utilisateur – réseau conforme à l'UIT-T I.431 [9] côté utilisateur du réseau d'accès (c'est-à-dire, l'interface au point de référence T);

– autres accès analogiques ou numériques pour connexions semi-permanentes sans information de signalisation associées hors bande,

avec latitude d'affectation de la voie de transfert d'information (voie support) pour chaque appel, offrant une capacité de concentration dans le réseau d'accès (AN) et au niveau de l'interface V5.2. La présente Recommandation ne spécifie pas l'implémentation des prescriptions dans le réseau d'accès et ne limite pas le choix d'implémentation, du moment que les fonctions spécifiées dans la présente Recommandation sont assurées à l'interface V5.2.

La présente Recommandation doit être utilisée conjointement avec l'UIT-T G.964 [8]. Ces deux Recommandations utilisent le même format et la présente Recommandation renvoie à certains paragraphes de l'UIT-T G.964 [8].

Une fonction de commande de liaison est assurée afin de gérer les arrangements à liaisons multiples possibles d'une interface V5.2. Voir le paragraphe 16.

Une fonction de protection est offerte afin d'assurer la continuité de fonctionnement de l'interface en cas d'anomalies sur les liaisons à 2048 kbit/s.

L'Annexe A donne une vue d'ensemble des scénarios et de l'architecture de service qui ont été pris comme base théorique pour la spécification de l'interface V5.2.

L'Annexe B définit l'utilisation des éléments d'information de protocole pour la définition des protocoles de RTPC national ainsi que les diagrammes des flux d'informations selon la spécification de protocole RTPC. L'Annexe H donne la définition de la détection des erreurs de couche 3 pour le protocole RTPC.

L'Annexe C spécifie les conditions de base des fonctions de gestion dans le réseau d'accès et dans le commutateur local afin d'assurer un fonctionnement et un contrôle corrects de la configuration.

L'Annexe D décrit l'architecture du protocole de transfert des informations de commande d'état pour les points d'accès utilisateur au RNIS et au RTPC.

L'Annexe E donne un aperçu général des formats de trame utilisés à l'interface V5.2 ainsi que les types de messages affectés par l'interface V5.2.

Les Annexes F, G, H se réfèrent aux Annexes F, H, K de l'UIT-T G.964.

L'Annexe J présente les flux d'informations et les notes explicatives pour le protocole de protection.

L'Annexe K donne des informations sur les principes d'application du protocole BCC.

L'Annexe L donne des exemples de mise en œuvre avec haut niveau d'interopérabilité.

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.

[1] UIT-T G.703 (1998), *Caractéristiques physiques et électriques des jonctions numériques hiérarchiques*.

[2] UIT-T G.704 (1998), *Structures de trame synchrone utilisées aux niveaux hiérarchiques de 1544, 6312, 2048, 8448 et 44 736 kbit/s*.

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

[4] UIT-T G.960 (1993), *Section numérique pour accès RNIS au débit de base*.

[5] UIT-T Q.920 (1993), *Couche liaison de données à l'interface usager-réseau RNIS – Aspects généraux* et UIT-T Q.921 (1998)*, Interface usager-réseau RNIS – Spécification de la couche de liaison de données*.

[6] UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface usager-réseau RNIS pour la commande de l'appel de base*.

[7] UIT-T G.823 (2000), *Régulation de la gigue et du dérapage dans les réseaux numériques fondés sur la hiérarchie à 2048 kbit/s*.

[8] UIT-T G.964 (2001), *Interfaces V au commutateur local numérique – Interface V5.1 (fondée sur la hiérarchie à 2048 kbit/s) pour le support d'un réseau d'accès*.

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

[10] UIT-T G.962 (1993), *Section numérique d'accès RNIS au débit primaire de 2048 kbit/s*.

[11] UIT-T G.706 (1991), *Procédures de verrouillage de trame et de contrôle de redondance cyclique (CRC) concernant les structures de trame de base définies dans la Recommandation G.704*.

[12] UIT-T Q.824.5 (1997), *Description d'étape 2 et d'étape 3 pour l'interface Q3 – Gestion des abonnés – Informations communes*.

[13] UIT-T Q.831 (1997), *Gestion des dérangements et de la qualité de fonctionnement des environnements à interface V5 et profils clients associés*.

3 Définitions, symboles et abréviations

3.1 Définitions

La présente Recommandation définit les termes suivants, et utilise les définitions qui figurent dans la Rec. UIT-T G.964 [8] et dans les Recommandations citées en référence.

3.1.1 voie C active: voie C physique qui est en train de transporter une voie C logique. Une voie C active devient une voie C en attente lorsqu'elle ne transporte pas de voie C logique.

3.1.2 voies supports: les voies supports sont utilisées pour fournir la capacité de transmission bidirectionnelle pour les canaux B affectés depuis les points d'accès utilisateur au débit de base, au débit primaire ou pour les voies de codage MIC en loi A à 64 kbit/s depuis les points d'accès utilisateur du RTPC. Elles peuvent être utilisées sur des voies à $n \times 64$ kbit/s pour faciliter la fourniture de certains services du RNIS.

3.1.3 protocole de connexion à la voie support (BCC, *bearer channel connection*): protocole permettant au commutateur local (CL) de donner des instructions au réseau d'accès (AN) pour affecter les voies supports à la demande, de manière simple ou groupée.

3.1.4 voie de communication (voie C): intervalle de temps associé à un débit de 64 kbit/s utilisé par une interface V5.2 profilée afin d'y insérer des trajets de communication.

3.1.5 trajet de communication (trajet C): liaison transportant un des types suivants d'information (pour plus de détails, voir le paragraphe 8.4.1):

– liaison de données de couche 2 acheminant le protocole de commande;

– liaison de données de couche 2 acheminant le protocole de commande de liaison;

– liaison de données de couche 2 acheminant la signalisation RTPC;

– chacune des liaisons de données de couche 2 acheminant le protocole de protection;

– liaison de données de couche 2 acheminant le protocole de connexion à la voie support;

– liaison acheminant toutes les données RNIS de type Ds issues d'un ou de plusieurs points d'accès utilisateur;

– liaison acheminant toutes les données RNIS de type p issues d'un ou de plusieurs points d'accès utilisateur;

– liaison acheminant toutes les données RNIS de type f issues d'un ou de plusieurs points d'accès utilisateur.

Il est à noter que cette définition couvre le cas où il existe plus d'un trajet C acheminant le même type d'information, chacun étant affecté à une voie C logique différente.

3.1.6 informations de canal D du RNIS: informations de canal D issues d'un point d'accès utilisateur au débit de base ou au débit primaire (y compris les données RNIS de type Ds, p ou f).

3.1.7 voie de communication logique (voie C logique): groupe d'un ou de plusieurs trajets de communication, chacun de type différent, mais ne comprenant pas le trajet C du protocole de protection.

3.1.8 liaison multiple: ensemble de plusieurs liaisons à 2048 kbit/s qui, ensemble, forment une interface V5.2 (bien qu'il ne soit pas nécessaire qu'une interface V5.2 ait plus d'une liaison à 2048 kbit/s).

3.1.9 intervalle de temps multiple: groupe de plusieurs voies à 64 kbit/s offrant une intégrité pour les signaux jusqu'à 8 kHz et une intégrité de l'ordre des intervalles de temps, utilisé en général dans un point d'accès utilisateur au débit de base du RNIS, afin de fournir un service à débit supérieur.

3.1.10 voie de communication physique (voie C physique): intervalle de temps de 64 kbit/s d'une interface V5.2 qui a été affecté au transport de voies C logiques. Une voie C physique ne peut pas servir à transporter des voies supports.

Les intervalles de temps 16 des liaisons primaire et secondaire (uniquement dans le cas de l'interface V5.2 avec plusieurs liaisons à 2048 kbit/s) sont toujours des voies C physiques.

3.1.11 voies supports préconnectées: toute voie support ou voie support multiple, établie à l'aide du protocole BCC de manière à fournir des services commutés dans le réseau d'accès, sur la largeur de bande réservée à cet effet dans l'interface V5.2.

3.1.12 liaison primaire: liaison à 2048 kbit/s d'une interface V5.2 à liaisons multiples dont la voie C physique de l'intervalle de temps 16 transporte un trajet C pour le protocole de protection, ou, sur initialisation de l'interface V5.2, également le trajet C pour le protocole de commande, le protocole de commande de liaison et le protocole BCC. D'autres trajets C peuvent également être transportés dans l'intervalle de temps 16.

3.1.13 groupe protégé: groupe de N voies C logiques.

3.1.14 groupe de protection: groupe de (N + K) voies C physiques, où K est le nombre de voies C physiques qui servent de voies C en attente pour les N voies C logiques.

3.1.15 liaison secondaire: liaison à 2048 kbit/s d'une interface V5.2 à liaisons multiples dont l'intervalle de temps 16 transporte un trajet C pour le protocole de protection, ou qui, sur initialisation de l'interface V5.2, sert de voie C en attente pour le protocole de commande, le protocole de commande de liaison et le protocole BCC, ou pour tout autre trajet C initialement transporté dans l'intervalle de temps 16 de la liaison primaire.

3.1.16 voie C en attente: voie C physique qui ne transporte pas de voie C logique, mais qui sert à protéger des voies C logiques. Dès qu'elle est utilisée pour transporter une voie C logique, une voie C en attente devient une voie C active.

3.1.17 point de référence T: le terme point de référence T est utilisé dans un sens général. Si un terminal ou un adaptateur de terminal RNIS est connecté à l'interface au point de référence T, alors, selon la configuration de référence du RNIS, les points de référence S et T coïncident; si une terminaison de réseau de type 2 est connectée à l'interface au point de référence T, alors il s'agit bien du point de référence T proprement dit.

3.2 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes, ainsi que celles qui figurent dans l'UIT-T G.964 [8]:

BCC	connexion de canal support (*bearer channel connection*)
dB	décibel
H0	voie à 384 kbit/s avec synchronisation associée
H12	voie à 1920 kbit/s avec synchronisation associée
LFA	perte de verrouillage de trames (*loss of frame alignment*)
M	élément de protocole obligatoire (*mandatory*)
NOF	trames de fonctionnement normales (*normal operational frame*)
O	élément de protocole facultatif (*optional*)
PRA-RNIS	accès au débit primaire du RNIS (*primary rate access)*
REQ	demande (*request*)
SN	numéro de séquence (*sequence number*)
TSSI	intégrité de séquence des intervalles de temps (*time slot sequence integrity*)

VP(R) variable d'état réception pour le protocole de protection (*receive state variable for protection protocol*)

VP(S) variable d'état émission pour le protocole de protection (*send state variable for protection protocol*)

4 Caractéristiques électriques et physiques de l'interface

L'interface V5.2 peut comporter entre une et seize liaisons à 2048 kbit/s selon les besoins.

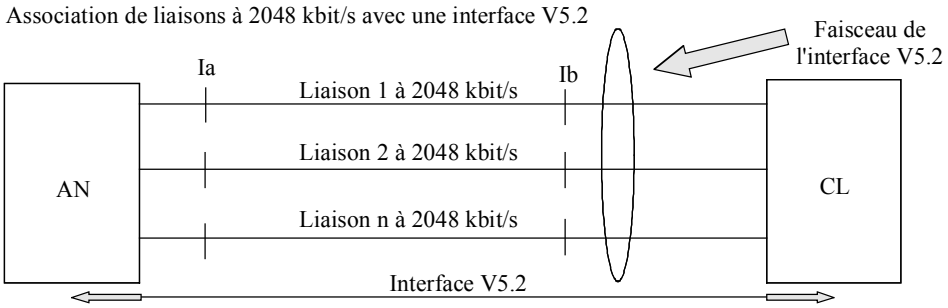
L'interface peut utiliser tout système d'émission normalisé [1] et [2] conçu pour le transport des signaux à 2048 kbit/s. L'interface doit être conforme aux exigences électriques (optiques) et de format appropriées pour la structure choisie.

NOTE – Le reste de la présente Recommandation se fonde sur les spécifications d'interface électrique à 2048 kbit/s.

Pour les cas où on utilise des interfaces électriques multiples (1 à 16) à 2048 kbit/s, les caractéristiques électriques et physiques de chacune des interfaces à 2048 kbit/s doivent être conformes à l'UIT-T G.703 [1], cas du débit à 2048 kbit/s.

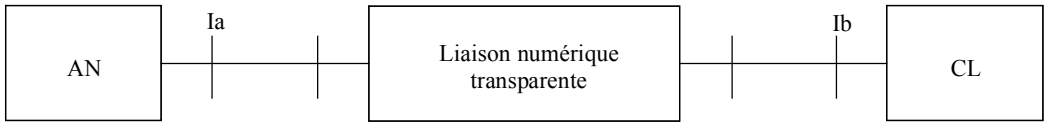
Deux types d'interface sont définis dans l'UIT-T G.703 [1]: l'interface à paire symétrique et l'interface à paire coaxiale. Conformément aux deux variantes d'interface illustrées à la Figure 1, il appartient à l'exploitant du réseau de demander la présentation d'interface nécessaire.

Les caractéristiques de gigue sont identiques à celles de l'UIT-T G.964 [8] pour chacune des liaisons à 2048 kbit/s.



NOTE – n liaisons à 2048 kbit/s sont représentées (n = 1 à 16).

L'une des liaisons à 2048 kbit/s, voire toutes, peuvent utiliser une liaison numérique transparente:



Ia point de l'interface côté AN
Ib point de l'interface côté CL

Figure 1/G.965 – Interface V5.2 avec et sans liaison numérique transparente

5 Caractéristiques fonctionnelles de l'interface et procédures associées

Les caractéristiques fonctionnelles de chacune des liaisons à 2048 kbit/s et les procédures associées sont identiques à celles de l'UIT-T G.964 [8].

5.1 Caractéristiques et procédures de commande de liaison

Comme l'interface V5.2 peut comprendre plusieurs liaisons à 2048 kbit/s, il faut effectuer une vérification d'identification de liaison et bloquer une liaison donnée. Deux procédures, définies au 16.2 pour remplir ces fonctions, sont exécutées à l'aide du protocole de commande de liaison.

5.1.1 Vérification d'identification de liaison

La vérification d'identification de liaison est une procédure symétrique qui doit être appliquée aux deux extrémités des liaisons d'interface V5.2, lorsque la machine à états finis de couche 1 (L1-FSM, *layer 1 finite state machine*) de l'interface passe à l'état "normal". Si la procédure échoue, la machine FSM vient à l'état "non opérationnel".

Cette procédure s'applique à toutes les liaisons, liaisons primaire et secondaire incluses. Elle peut aussi être effectuée lorsque la machine se trouve de façon permanente à l'état normal, par exemple, sur temporisation, ou sur demande de l'interface Q (AN/CL).

5.1.2 Blocage de liaison

Pour la maintenance de liaison, il faut disposer d'une fonction supplémentaire pour bloquer une seule liaison à 2048 kbit/s d'une interface V5.2. Le blocage de liaison est une procédure asymétrique, dans laquelle le réseau d'accès peut demander le blocage d'une liaison, mais c'est le commutateur local, en tant que maître du service qui décide. Le commutateur local libère toute connexion commutée sur la liaison demandée, selon les besoins du service et en temps voulu, rétablit des connexions semi-permanentes et préconnectées à d'autres liaisons de la même interface V5.2. Le commutateur local doit utiliser le protocole de protection pour redéployer les voies C logiques affectées, dans la mesure du possible.

Dans le cas d'anomalies internes du réseau d'accès qui empêchent la disponibilité de la liaison, l'accès réseau peut appliquer le blocage immédiat de la liaison. En même temps doit être initialisée si possible la protection de toutes voies C affectées.

Cette procédure peut s'appliquer même dans le cas d'une interface V5.2 comportant une seule liaison à 2048 kbit/s.

NOTE – Dans ce cas, le blocage met l'ensemble de l'interface hors service.

6 Aspects et caractéristiques des services et de l'architecture

Les services que l'interface V5.2 doit prendre en charge sont tous les services pris en charge par l'interface V5.1 (définis dans l'UIT-T G.964 [8]), plus l'accès au débit primaire du RNIS (PRA-RNIS). La présente Recommandation n'a cependant pas pour objet d'obliger une quelconque implémentation de réseau d'accès ou de commutateur local à assurer l'ensemble complet ou un sous-ensemble des services énumérés dans la présente Recommandation.

L'architecture de l'interface V5.2, du point de vue du service, est illustrée par la Figure 2.

6.1 Services à la demande

Les services à la demande traversent l'interface V5.2. Les trois types d'accès suivants sont pris en charge.

6.1.1 Accès au RTPC

Le contenu de ce paragraphe est identique à celui du 6.1.1/G.964 [8].

6.1.2 Accès de base au RNIS (BA-RNIS)

Le contenu de ce paragraphe est identique à celui du 6.1.2/G.964 [8].

En outre, le service support à intervalles de temps multiples à 2 × 64 kbit/s peut être assuré grâce à la fonctionnalité de voie support définie par la présente Recommandation.

6.1.3 Accès au débit primaire du RNIS (PRA-RNIS)

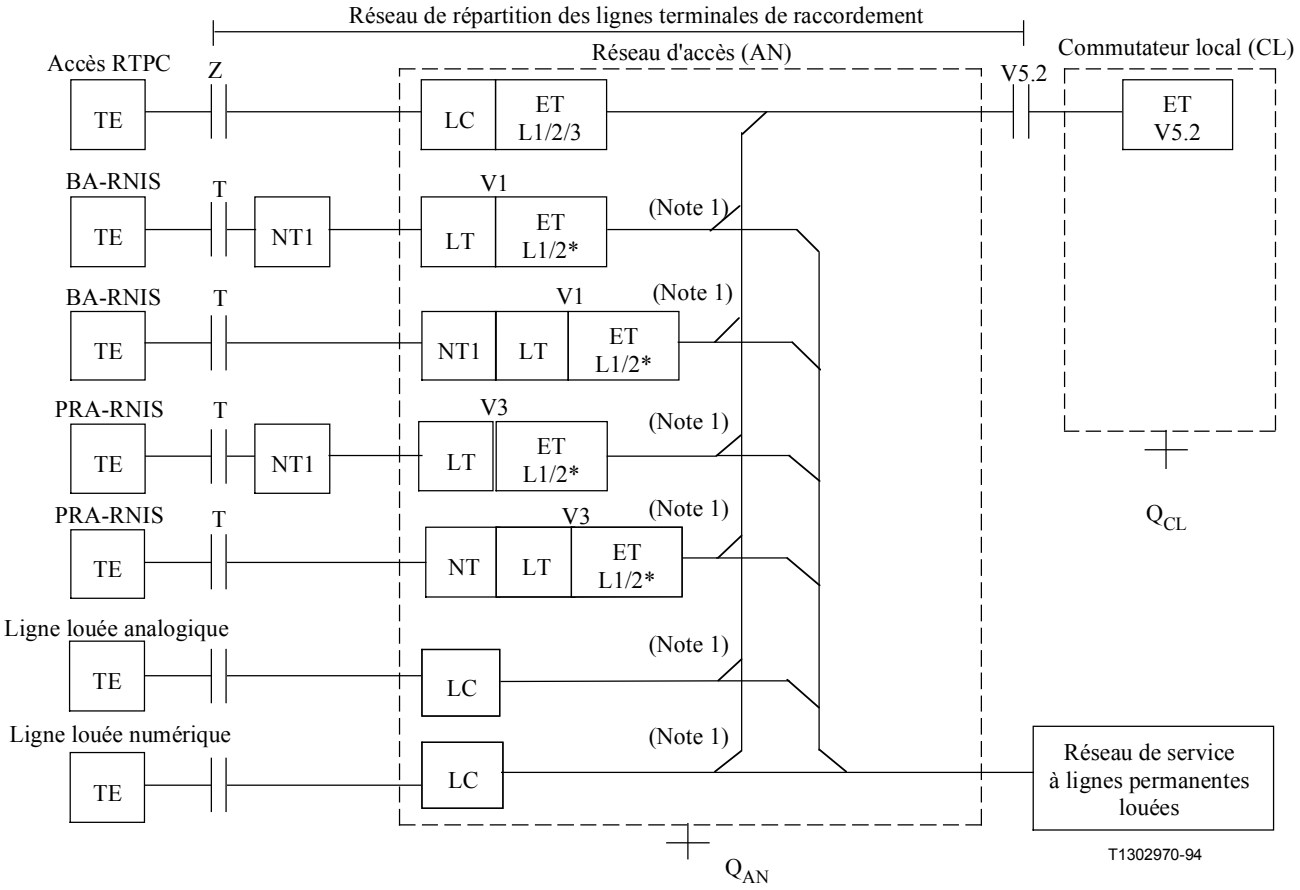
L'accès au débit primaire du RNIS est assuré avec une terminaison NT1 faisant partie intégrante du réseau d'accès ou par un équipement distinct prenant en charge les systèmes de transmission conformément à l'UIT-T G.962 [10] pour la prise en charge de la terminaison NT2 (par exemple, PABX RNIS), connectée au point de référence T.

Les débits binaires inférieurs à 64 kbit/s ne sont pas assurés directement: ils sont considérés comme des applications d'utilisateur à l'intérieur d'un canal B à 64 kbit/s dans l'accès au débit primaire.

On peut utiliser, en accès au débit primaire, un ou plusieurs canaux B pour la capacité facultative de ligne permanente ou le service de ligne semi-permanente louée.

Les services supports multidébit, qui peuvent utiliser H0, H12 ou d'autres voies à intervalles de temps multiples entre le point d'accès utilisateur et le commutateur local, sont également pris en charge par toute interface V5.2 acceptant l'accès au débit primaire du RNIS à l'aide du système approprié de signalisation du RNIS.

NOTE – Si ces services ne sont assurés ni par le commutateur local ni par le réseau d'accès, ils ne seront pas disponibles pour les utilisateurs.



BA-RNIS	accès de base RNIS
CL	commutateur local
ET	terminaison de commutateur
LC	équipement de ligne
L1/2/3	fonction de couche 1/2/3
PRA-RNIS	accès au débit primaire RNIS
Q_{CL}	interface Q dans le commutateur local
Q_{AN}	interface Q dans le réseau d'accès
TE	équipement terminal

NOTE 1 – La sélection des canaux et leur affectation au service font partie du profilage.
NOTE 2 – L'astérisque indique que la couche 2 aboutit en partie seulement dans le réseau d'accès.

Figure 2/G.965 – Architecture de l'interface V5.2 vue à partir du service

6.2 Fonction de ligne permanente (PL, *permanent line*)

Le contenu du présent paragraphe est identique à celui du 6.2/G.964 [8]. Cependant, la fonction de ligne permanente doit être fournie pour l'accès au débit primaire RNIS, comme spécifié au 15.3.

6.3 Ligne semi-permanente louée

Le contenu du présent paragraphe est identique à celui du 6.3/G.964 [8]. Cependant, les spécifications pour les lignes semi-permanentes louées doivent également être applicables à l'accès au débit primaire du RNIS.

6.4 Services de lignes permanentes louées

Le contenu du présent paragraphe est identique à celui du 6.4/G.964 [8].

7 Commande et profilage

7.1 Principes pour la commande

7.1.1 Spécifications et hypothèses générales

A partir de la Figure 3, les spécifications générales suivantes ont été définies pour le point d'accès de base RNIS et pour le point d'accès au débit primaire du RNIS. Sauf dispositions contraires, elles s'appliquent également aux points d'accès RTPC.

1) La responsabilité de la commande d'appel est confiée au commutateur local (c'est-à-dire que le réseau d'accès peut ne pas avoir connaissance de l'état de l'appel pendant le fonctionnement normal de l'interface V5.2).

2) La gestion d'accès dans le réseau d'accès et la gestion de service dans le commutateur local alimentent chacune leur machines FSM et leurs entités de protocole; elles communiquent en passant par l'interface V5.2.

   Il faut une machine FSM pour chaque point d'accès utilisateur et pour les interfaces à 2048 kbit/s; il faut également des entités de protocole pour les liaisons de couche 2, aussi bien dans le réseau d'accès que dans le commutateur local (voir la Figure 4 pour plus de précisions et le paragraphe 15 pour la définition des machines à états finis, des entités de protocole et du protocole de couche 3). Les renseignements fournis à la gestion par chaque machine FSM ou par chaque entité de protocole doivent être utilisés pour déterminer l'opération qu'il y a lieu d'effectuer vis-à-vis d'autres machines FSM et d'autres entités de protocole, de la fonction de commande d'appel et du système d'exploitation. L'Annexe C fournit de plus amples renseignements sur certaines hypothèses de base.

3) Les demandes de blocage de point d'accès, pour une maintenance non urgente d'accès via l'interface Q du réseau d'accès, ne peuvent être octroyées que par le commutateur local (c'est-à-dire qu'une demande de blocage ne doit normalement pas interférer avec des communications en cours ni avec des appels en cours d'établissement ou de libération ni avec des connexions semi-permanentes).

4) Toute demande de maintenance urgente d'accès via l'interface Q du réseau d'accès doit être signalée au commutateur local quel que soit l'état de ce dernier (c'est-à-dire qu'un message de "blocage immédiat" prend immédiatement effet alors que le nouvel état est à synchroniser avec le commutateur local).

5) Les anomalies détectées dans la couche 1 concernant des voies supports dans les liaisons à 2048 kbit/s défaillantes entraînent la libération des appels. Les anomalies détectées dans la couche 1 concernant des voies C physiques dans une liaison à 2048 kbit/s défaillante entraînent la réaffectation de ces voies C par le protocole de protection si ce dernier dispose des ressources nécessaires pour le faire. La préemption autonome des voies C physiques par le protocole de protection n'est pas autorisée. Les anomalies détectées dans la couche 1 concernant des lignes semi-permanentes louées dans une liaison à 2048 kbit/s défaillante amènent le gestionnaire des ressources du commutateur local à essayer d'établir une autre connexion support sur laquelle le service sera assuré. Il peut exister des anomalies et des défauts qui dégradent la qualité du service mais sans interrompre totalement le service, et qui n'entraînent donc pas de reconfiguration. Des anomalies et défauts de ce genre dans le service du RTPC peuvent avoir une incidence sur le protocole de ce réseau, par exemple en entraînant un accusé de réception négatif d'un message de demande; mais ils ne doivent pas affecter le fonctionnement de la machine FSM associée aux accès.

6) Les anomalies détectées et autres événements doivent être signalés au gestionnaire correspondant du réseau d'accès ou du commutateur local et consignés dans un registre.

7) Lorsqu'un point d'accès est bloqué, il n'est pas possible d'émettre des appels et les appels à l'arrivée doivent être traités par le commutateur local comme si le point d'accès était hors service, conformément au protocole national.

8) Le commutateur local doit être obligatoirement informé du niveau de qualité de la transmission en ce qui concerne les points d'accès utilisateur, au moyen de messages "d'évaluation de la qualité" envoyés par le réseau d'accès au commutateur sans modifier les machines FSM décrivant les états de ces points d'accès. Ces messages contiendront des informations relatives à la qualité de transmission qui seront enregistrées par le commutateur local. Celui-ci pourra utiliser ces renseignements pour déterminer s'il y a lieu de fournir le service demandé.

   Cette obligation n'est applicable qu'aux points d'accès RNIS dont la terminaison NT1 se trouve à l'extérieur du réseau d'accès. La qualité de transmission entre point d'accès utilisateur et interface V5.2 ne doit pas être affectée outre mesure par une diminution de la qualité due à des erreurs binaires se produisant sur des liaisons internes au réseau d'accès. Pour éviter que cela ne se produise, on effectuera une surveillance en service et les liaisons internes au réseau AN seront bloquées (mises hors service) en cas de dégradation des caractéristiques d'erreurs.

9) Les opérations de rebouclage ne seront effectuées que si le point d'accès est dans l'état bloqué. Cette fonction est pilotée par le réseau d'accès.

   Le réseau d'accès est chargé de l'exécution des opérations de localisation des anomalies survenant dans le réseau d'accès ou aux points d'accès utilisateur. Les essais actifs interférant avec le service, dont le commutateur local est responsable ne doivent pas être effectués tant que l'accès correspondant n'est pas bloqué (machine FSM à l'état bloqué) par le commutateur local.

10) Un mécanisme devra être prévu afin d'identifier chaque interface V5 ainsi que les étiquettes de leurs variantes actuelles et nouvelles de profilage. La variante de profilage est une étiquette unique d'un ensemble complet de données de profilage appliquée via les interfaces Q (voir 15.7).

11) Il doit être possible d'identifier chaque liaison à 2048 kbit/s d'une interface V5.2. Il faut effectuer une procédure (symétrique) de vérification de l'identité des liaisons à 2048 kbit/s lors de tout rétablissement du verrouillage de trame ainsi qu'après reprofilage (ce qui peut affecter ou non les liaisons de l'interface V5.2).

12) Il doit être possible de bloquer une liaison à 2048 kbit/s d'une interface V5.2. Le réseau d'accès peut émettre une demande, mais c'est le commutateur local qui décide: pour les connexions commutées, il attend que les communications se terminent, quant aux connexions semi-permanentes et réservées au réseau d'accès, elles sont rétablies sur d'autres liaisons. La gestion-systèmes du commutateur local utilise le protocole de protection pour redéployer les voies C logiques concernées avant le blocage d'une liaison à 2048 kbit/s. A l'aide d'un mécanisme légèrement différent, le réseau d'accès peut bloquer immédiatement une liaison déterminée à 2048 kbit/s.

13) Des liaisons à 2048 kbit/s d'une interface V5.2 peuvent être retirées du service à des fins de maintenance via les interfaces Q_{CL} et Q_{AN} avec la prise en charge du protocole de commande de liaison de l'interface V5.2. Elles sont remises en service à l'aide du protocole de commande de liaison V5.2.

14) Chaque voie support d'une interface V5.2 peut être interdite d'utilisation via l'interface Q_{CL}.

7.1.2 Commande du point d'accès utilisateur au débit de base du RNIS pour la fonction de ligne permanente

La commande des points d'accès utilisateur au débit de base du RNIS, en cas de fourniture de la fonction de ligne permanente, est identique à celle donnée en 7.1.2/G.964 [8].

7.1.3 Commande du point d'accès utilisateur au débit primaire du RNIS en cas de fourniture de la fonction de ligne permanente

La fourniture d'une fonction de ligne permanente ne doit pas affecter le fonctionnement d'un point d'accès utilisateur au débit primaire du RNIS.

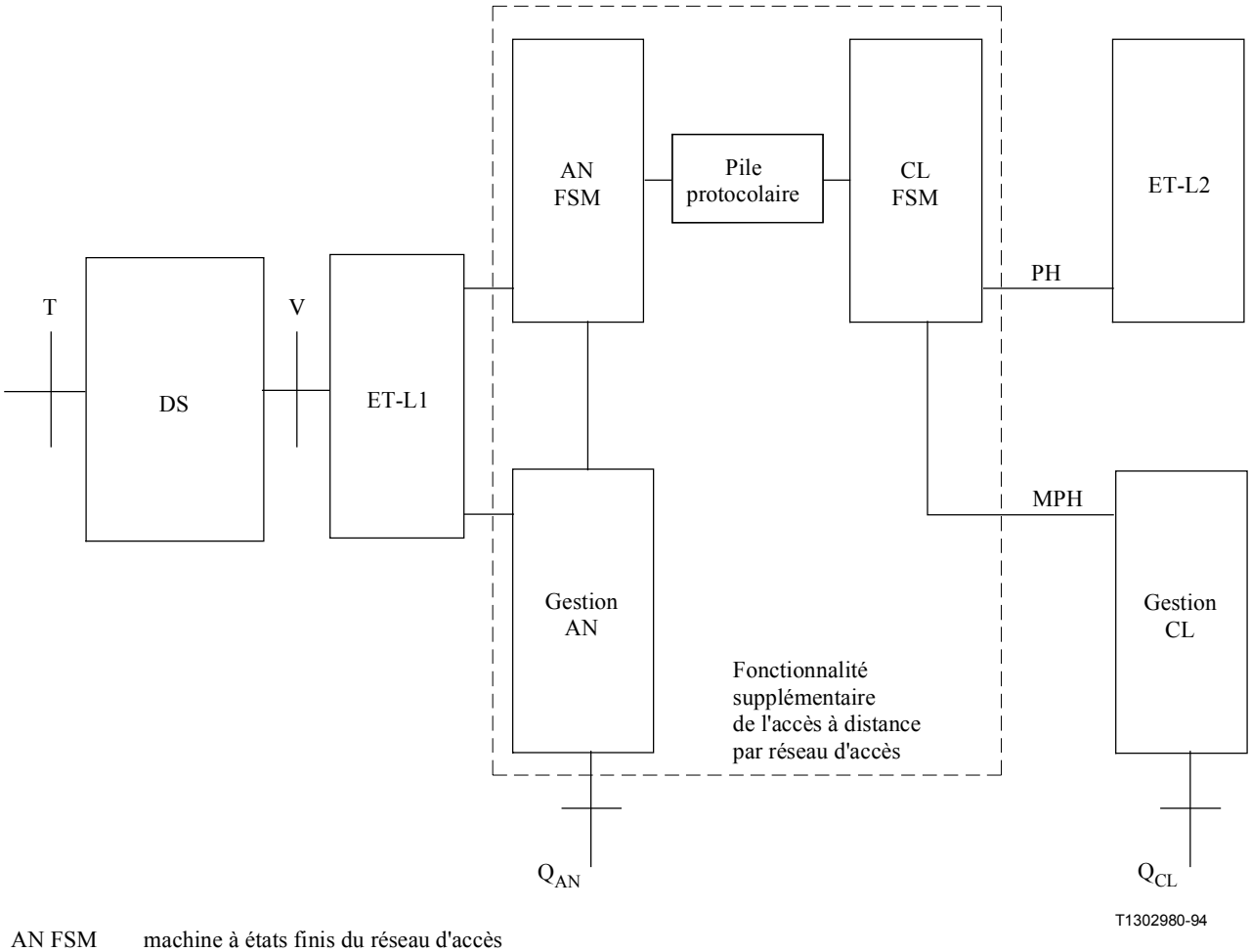
7.1.3.1 Affirmations et hypothèses

1) La fonctionnalité de ligne permanente assurée par un réseau d'accès dans la configuration d'interface V5.2 est une caractéristique supplémentaire d'interface utilisateur-réseau RNIS qui ne peut être assurée par un point d'accès raccordé directement à un commutateur local.

2) La fonctionnalité de ligne permanente peut facultativement utiliser un, voire plusieurs (tous éventuellement) canaux B d'un point d'accès utilisateur s'ils ne sont pas déjà profilés dans le réseau d'accès ou dans le commutateur local pour acheminer des services à la demande. Seules les trames normales d'exploitation (NOF, *normal operational frame*) peuvent être envoyées au point de référence V, comme le montre la Figure 3.

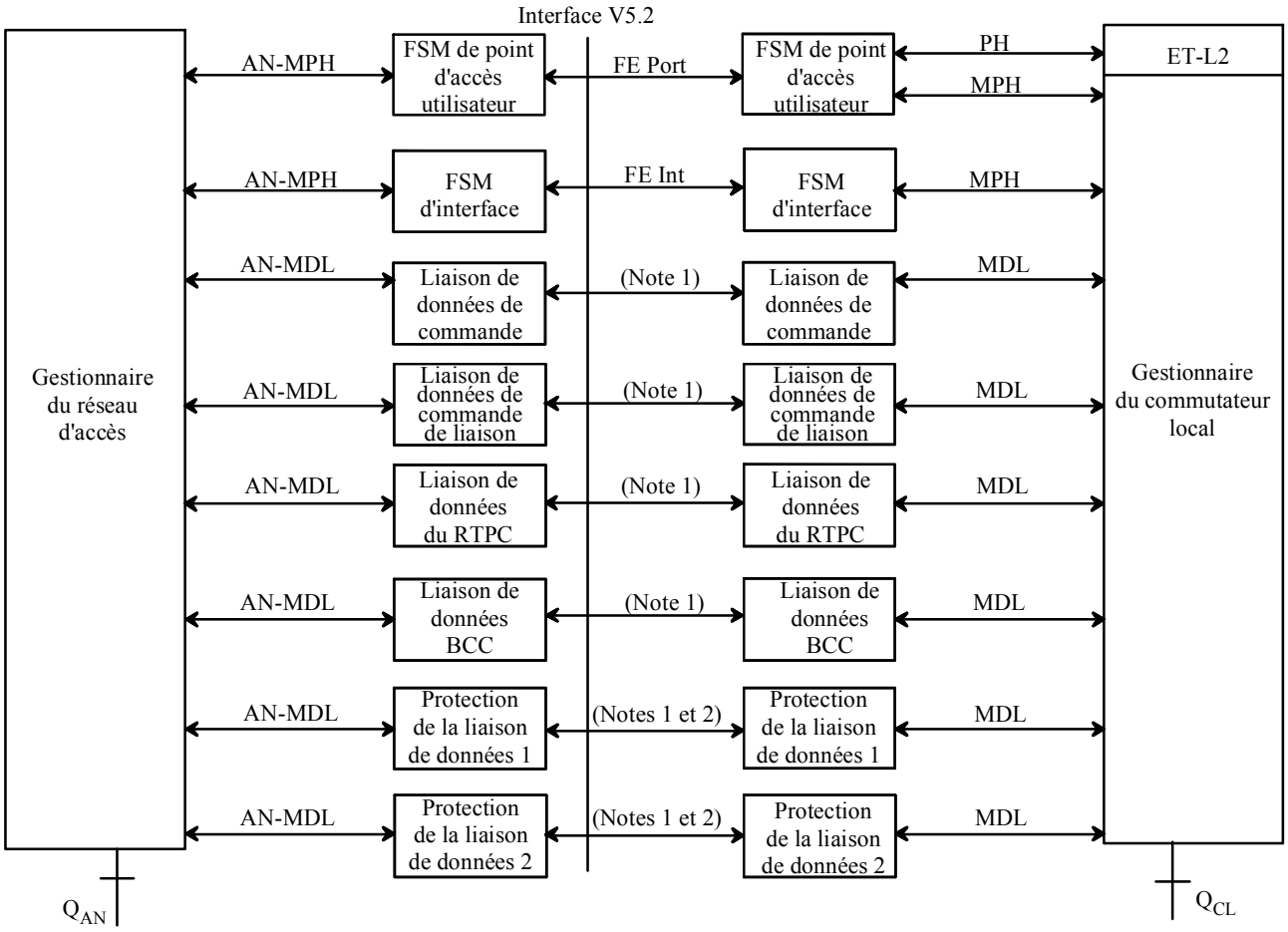
3) Le commutateur local est responsable des services à la demande.

4) Lorsque le commutateur local bloque le point d'accès utilisateur, il le place dans l'état non opérationnel pour tous les types de service; le réseau d'accès peut reprendre le contrôle pour permettre aux points d'accès utilisateur d'une fonctionnalité de ligne permanente de continuer à fonctionner.



AN FSM	machine à états finis du réseau d'accès
CL FSM	machine à états finis du commutateur local
DS	section numérique d'accès
ET-L1/2	couche 1/2 du commutateur local
Gestion AN	gestionnaire du réseau d'accès
Gestion CL	gestionnaire du commutateur local
MPH	primitive entre couche Physique et gestion de couche 2
PH	primitive entre couche Physique et couche 2

Figure 3/G.965 – Modèle fonctionnel d'accès utilisateur RNIS



AN-MPH Primitive AN entre couche Physique et gestion de couche 2
AN-MDL Primitive AN entre couche 2 et gestion de couche 3

NOTE 1 – Voir le paragraphe 10.4.
NOTE 2 – Les entités de protocole de liaison ne servent que dans le cas d'une interface V5.2 à liaisons à 2048 kbit/s multiples.

Figure 4/G.965 – Modèle fonctionnel des machines FSM de couche 1 et de couche 2

7.1.3.2 RNIS et fonction de ligne permanente

Le service de ligne permanente ne doit pas utiliser la voie D du RNIS pour les messages destinés au commutateur local. Le service d'accès au débit primaire du RNIS (PRA-RNIS) sous sa forme actuelle définie par l'UIT-T G.962 [10], fourni à un point d'accès utilisateur RNIS via un réseau d'accès, doit être identique au service fourni lorsque les connexions d'accès au commutateur local sont directes.

Pour un réseau d'accès, on ne peut accepter d'influence sur aucun service RNIS à la demande de la part d'un service (par exemple, le service de ligne permanente) utilisant un ou plusieurs canaux B à d'autres fins que les services à la demande.

7.2 Stratégie et caractéristiques de profilage

7.2.1 Généralités

Le profilage constitue l'un des nombreux aspects des fonctions de commande. Il a été distingué des autres caractéristiques de commande car, devant être exécuté par l'intermédiaire des interfaces Q du réseau d'accès et du commutateur local, il ne relève pas directement de la spécification de l'interface V5.2. Seuls sont définis les aspects de profilage qui ont une incidence au moins théorique ou indirecte sur la définition de l'interface.

7.2.2 Caractéristiques de profilage

Voir en 7.2.2/G.964 [8] une liste des éléments qui doivent être profilés, en plus des éléments mentionnés ci-dessous. Cependant, le premier élément de la liste donné en référence n'est pas valable pour l'interface V5.2, car l'association des voies supports est gérée par le protocole BCC et non de manière statique par profilage.

Caractéristiques de profilage:

1) Le nombre de liaisons à 2048 kbit/s qui sont utilisées sur une interface V5.2, ainsi que leur identification, sont affectés par profilage.
2) Les voies C physiques sont affectées aux intervalles de temps ou aux liaisons par profilage.
3) Les voies C physiques de l'intervalle de temps 16 des liaisons primaire et secondaire forment le groupe de protection 1, groupe comprenant le protocole de protection. (Ceci suppose plusieurs liaisons à 2048 kbit/s au niveau de cette interface V5.2.) Sinon, ce profilage n'est pas valable.
4) L'une des voies C physiques du groupe de protection 1 fonctionne comme voie C active. L'autre voie C physique du groupe de protection 1 fonctionne comme voie C en attente de ce groupe.
5) Par défaut, les voies C logiques sont affectées aux voies C physiques par profilage.
6) Une voie C physique sans voie C associée se comporte comme une voie C en attente. (L'affectation des trajets C aux voies C logiques se fait par profilage.)
7) L'affectation des trajets C pour les données de type Ds (ainsi que pour les données de type p ou de type f) ou pour la signalisation du RTPC est une option profilée.
8) La voie C physique active du groupe de protection 1 doit transporter au minimum les trajets C du protocole de protection, du protocole BCC, du protocole de commande et du protocole de commande de liaison.
9) L'interface Q_{CL} peut être utilisée pour supprimer l'affectation d'une voie C logique à une voie C physique.
10) L'interface Q_{CL} peut être utilisée pour affecter une voie C logique donnée à une voie C physique. Le protocole de protection peut modifier cette affectation ultérieurement.
11) Lors du profilage de voies C physiques dans une installation, il faut prendre un certain nombre de précautions lorsque le commutateur local ou le réseau d'accès sont formés de modules partageant les mêmes fonctions logicielles de terminaison pour l'interface V5.2. Il faut tenir compte des conséquences sur la distribution de la charge de l'association voie C physique-module. Il faut veiller, lors du profilage de voies C physiques pour une utilisation en attente, à ce que la future commutation de protection sur ces voies C physiques ne provoque pas d'irrégularités exagérées dans la charge de ces modules.

De même, si un commutateur local ou un réseau d'accès est modularisé afin de maintenir une certaine performance en cas d'anomalie, il faut veiller à ce que le profilage des voies C physiques en attente ou utilisées soit effectué de manière telle que la performance puisse être maintenue grâce à la commutation de protection, non seulement en présence d'anomalies de liaisons à 2048 kbit/s mais aussi en présence d'anomalies sur les modules du commutateur local ou du réseau d'accès.

7.3 Connexion de canal support (BCC)

Le protocole BCC est utilisé pour affecter les canaux supports d'une liaison à 2048 kbit/s donnée aux points d'accès utilisateur, le plus souvent pour chaque appel. On suppose que les systèmes de gestion des ressources en canaux supports sont pris en charge par le commutateur local ou par le réseau d'accès, mais la présente Recommandation ne définit que les fonctions qui ont une influence directe sur l'interface V5.2.

Les canaux supports affectés par le protocole BCC, mais qui ne sont pas affectés pour chaque appel, sont indiquées ci-dessous:

– *connexions de lignes louées semi-permanentes* – Elles utilisent un ou plusieurs canaux supports qui sont affectés aux points d'accès utilisateur à l'aide de l'interface Q_{CL} et établies par le protocole BCC;

– *canaux supports préconnectés* – Ils utilisent un ou plusieurs canaux supports qui sont affectés aux points d'accès utilisateur à l'aide de l'interface Q_{CL} et établis par le protocole BCC.

Une fonction d'audit est fournie grâce au protocole BCC afin que l'affectation des canaux supports de l'interface V5.2 et des connexions du réseau d'accès puisse être testée.

Une fonction d'anomalie interne au réseau d'accès est également fournie dans le protocole BCC afin que le réseau d'accès puisse notifier au commutateur local les anomalies internes qui affectent les connexions aux canaux supports.

7.4 Protection

Le protocole de protection est utilisé dans le cas d'interfaces à plus d'une liaison à 2048 kbit/s. Il faut que le protocole de commande de liaison, le protocole de commande et le protocole BCC aient un trajet de communication au niveau de l'interface V5.2, même en cas d'anomalie d'une liaison à 2048 kbit/s (c'est-à-dire une liaison primaire ou secondaire).

Le protocole de protection doit vérifier qu'il y a une méthode permettant aux entités du commutateur local et du réseau d'accès de communiquer aux fins de protection des voies C logiques, en cas d'anomalie d'une seule liaison et si des voies C physiques en attente sont profilées.

Si une commutation de protection est demandée pour des voies C logiques, il appartient à la fonction gestion de protection de lancer la commutation de manière contrôlée à l'aide du protocole de protection.

8 Architecture de protocole et structure de multiplexage

8.1 Description fonctionnelle

La description fonctionnelle est illustrée à la Figure 5. Les éléments de l'UIT-T G.964 [8] se rapportant à l'accès de base RNIS s'appliquent également à l'accès au débit primaire RNIS. Les caractéristiques fonctionnelles suivantes s'ajoutent à celles définies dans l'UIT-T G.964 [8]:

– un protocole BCC est utilisé pour affecter les canaux supports sous contrôle du commutateur local;

– les services nécessitant des connexions d'intervalles multiples seront fournis sur une liaison à 2048 kbit/s d'une interface V5.2. Dans ce cas, l'intégrité à 8 kHz et l'intégrité de séquence des intervalles de temps seront toujours assurées;
– un protocole de commandes de liaison est défini afin de prendre en charge les fonctions de gestion des liaisons à 2048 kbit/s de l'interface V5.2;
– un protocole de protection est défini afin de prendre en charge en tant que de besoin la commutation des voies C logiques sur les voies C physiques.

8.2 Caractéristiques de protocole pour le RTPC et pour le RNIS

La Figure 6 montre sous forme simplifiée l'architecture de protocole. Les fonctions spécifiées dans la présente Recommandation se trouvent dans les zones grisées.

Les fonctions sont définies dans les paragraphes suivants:

– sous-couche fonction enveloppe de la procédure LAPV5 (LAPV5-EF): paragraphe 9;
– sous-couche liaison de données de la procédure LAPV5 (LAPV5-DL): paragraphe 10;
– sous-couche répétition de trames du réseau d'accès (AN-FR): paragraphe11;
– communication de sous-couche à sous-couche et fonction de mappage: paragraphe 12;
– structures générales du protocole de couche 3: paragraphe 13;
– spécification du protocole de signalisation du RTPC: paragraphe 14;
– protocole de commande: paragraphe 15;
– protocole de commande de liaison: paragraphe 16;
– protocole BCC: paragraphe 17;
– protocole de protection: paragraphe 18.

Les informations du canal D du RNIS en provenance des points d'accès au débit primaire au débit de base sont multiplexées dans la couche 2 et retransmises pour répétition de trames à l'interface V5.2. Le réseau d'accès et le commutateur local assurent la fonction de séparation entre les données de type p et f et les données de signalisation de type Ds sur différentes voies de communication. Il doit cependant être possible de les transporter sur une même voie de communication, à titre d'option de profilage (voir également 8.4).

L'Annexe E donne un aperçu général des points de code de message et des formats de trame utilisés dans l'interface V5.2.

Le protocole pour les points d'accès RTPC est spécifié dans l'UIT-T G.964 [8].

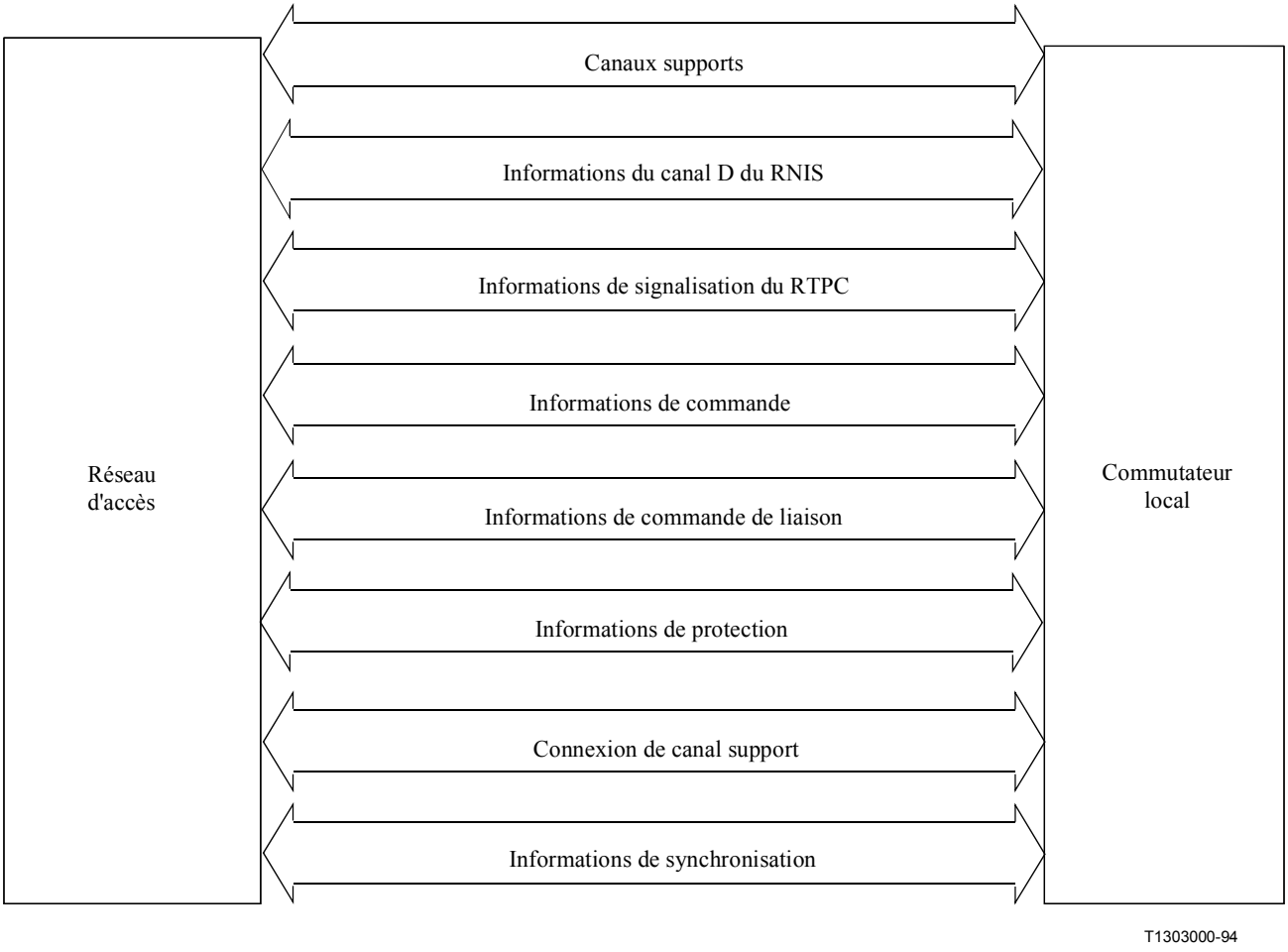


Figure 5/G.965 – Description fonctionnelle de l'interface V5.2

8.3 Intervalles de temps

Une interface V5.2 peut avoir de une à seize liaisons à 2048 kbit/s. La couche 1 de chacune d'entre elles doit respecter la structure définie dans les paragraphes 4 et 5.

Les intervalles de temps 16, 15 et 31 de chaque liaison à 2048 kbit/s peuvent être utilisés comme voies de communication physiques et sont affectés par profilage selon les besoins.

Les intervalles de temps qui ne sont pas profilés comme voies de communication physiques peuvent être utilisés comme canaux supports sous contrôle du protocole BCC.

8.4 Affectation des intervalles de temps aux voies de communication physiques

Dans le cas d'une seule liaison à 2048 kbit/s, l'affectation des intervalles de temps aux voies C physiques doit être identique à celle de l'UIT-T G.964 [8], afin d'assurer une compatibilité entière avec l'interface V5.1.

Dans le cas de plusieurs liaisons à 2048 kbit/s formant une interface V5.2, on doit utiliser le protocole de protection. Dans ce cas, l'intervalle de temps 16 de la liaison primaire contient le protocole de protection ainsi que tout trajet C qui a été profilé dans la même voie C. L'intervalle de temps 16 de la liaison secondaire contient lui aussi le protocole de protection.

D'autres voies C physiques devraient de préférence être affectées dans l'ordre suivant:

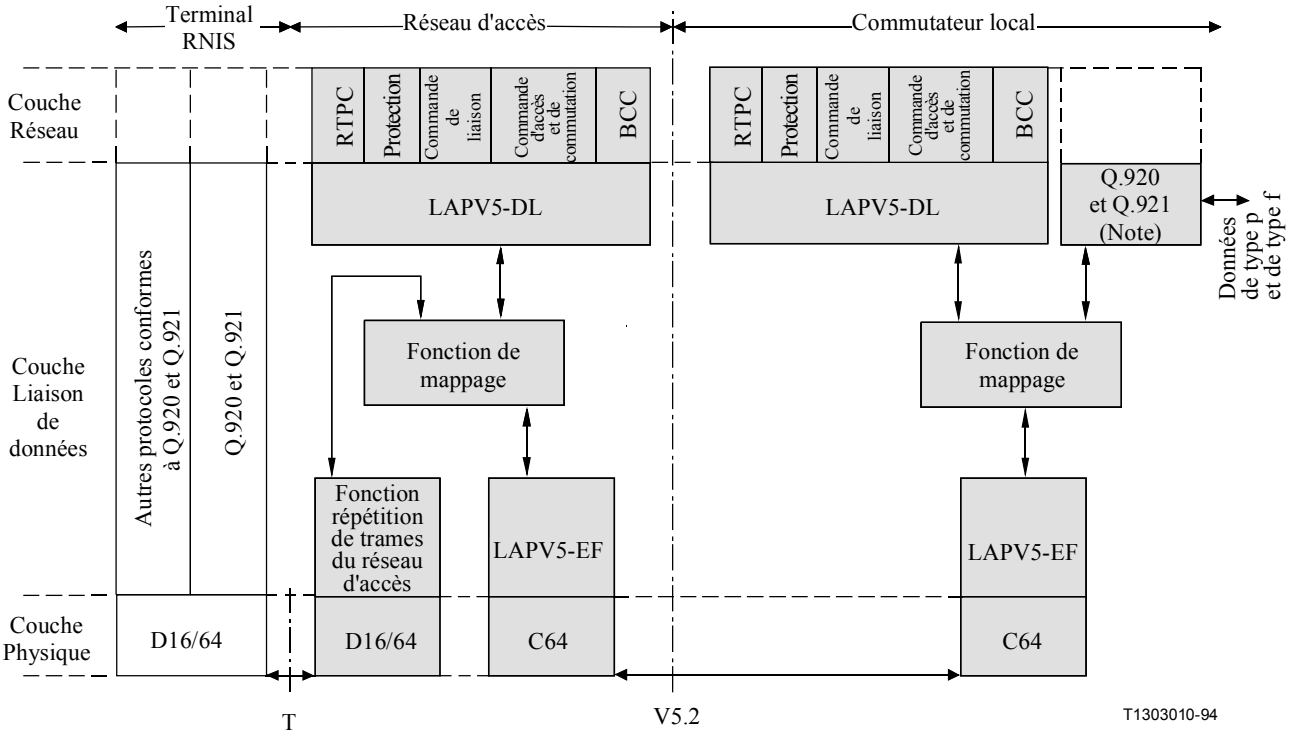
– intervalles de temps 16 des liaisons à 2048 kbit/s restantes selon les besoins. S'il en faut davantage, alors:

– intervalle de temps 15 d'une liaison à 2048 kbit/s. S'il en faut davantage, alors:

– l'intervalle de temps 31 de la même liaison à 2048 kbit/s est affecté. S'il en faut encore davantage, alors:

– poursuivre en affectant l'intervalle de temps 15 puis 31 de la liaison suivante à 2048 kbit/s comme l'indique le paragraphe précédent. Ce procédé peut être répété jusqu'à ce que tous les intervalles de temps 15 et 31 de toutes les liaisons à 2048 kbit/s aient été affectés.

Les directives ci-dessus ont été faites pour offrir une souplesse maximale d'affectation des intervalles de temps comme voies C physiques, sans pour autant imposer de limites aux futures adjonctions de services telles que les canaux H du RNIS. L'affectation indiquée ci-dessus ne doit pas nécessairement être suivie, en particulier lors du passage de l'interface V5.1 à l'interface V5.2 ou lors de l'accroissement de la capacité d'une interface V5.2; le respect scrupuleux de ces directives pourrait imposer un réarrangement total des voies C physiques à l'interface V5.2.



NOTE – Sauf les fonctions se terminant dans le mode répétition de trames du réseau d'accès.

Figure 6/G.965 – Architecture du protocole

8.4.1 Types de données pour les trajets C à l'interface V5.2

On a défini les types de données suivants qui sont transférés sur les trajets de communication de l'interface V5.2:

a) données de type p – A savoir des données de canal D du RNIS dont l'identifiant de point d'accès au service (SAPI) vaut 16;

b) données de type f – A savoir des données de canal D du RNIS dont l'identifiant de point d'accès au service (SAPI) est compris entre 32 et 62;

c) données de type Ds – A savoir des données de signalisation acheminées dans la voie D du RNIS, dont l'identifiant SAPI n'est pas égal à l'une des valeurs mentionnées ci-dessus.

NOTE – On admet que des services utilisant des identificateurs SAPI préalablement réservés pourront être proposés ultérieurement. L'attribution d'un identifiant par défaut permettra au moins aux précédentes applications de l'interface V5.2 de transporter au sein du réseau d'accès ces informations de type signalisation par canal D, bien que la future affectation des types de données puisse évoluer.

d) RTPC – Données de type information de signalisation RTPC;

e) Commande – Données de type information de commande;

f) Commande de liaison – Données de type information de commande de liaison;

g) BCC – Données de type BCC, c'est-à-dire appartenant au protocole qui affecte les voies supports sur demande;

h) Protection – Données de type protection, c'est-à-dire appartenant au protocole qui affecte les voies C logiques aux différentes voies C physiques en cas d'anomalies de liaison dans une interface V5.2.

Les trajets de communication de commande, de connexion de canal support, de commande de liaison et de protection sont toujours affectés à l'intervalle de temps 16 de la liaison primaire lors de l'initialisation. Les autres trajets de communication sont affectés aux voies C logiques, à l'exclusion de l'intervalle de temps 16 de la liaison secondaire ou des intervalles de temps fournis aux fins de protection.

8.4.2 Trajets de communication en cas d'accès au RTPC par une interface V5.2

Une seule voie C contient le protocole du RTPC.

8.4.3 Trajets de communication en cas d'accès au RNIS par une interface V5.2

Les données de type p des points d'accès utilisateur RNIS peuvent être acheminées sur une ou plusieurs voies C logiques.

Les données de type f des points d'accès utilisateur RNIS peuvent être acheminées sur une ou plusieurs voies C logiques.

Les données de type Ds des points d'accès utilisateur RNIS peuvent être acheminées sur une ou plusieurs voies C logiques.

Les trajets de communication transportant des données de type p, de type f ou de type Ds issues d'un point d'accès utilisateur RNIS, peuvent être placés sur la même voie C logique ou être répartis sur différentes voies C logiques.

Les données de type p issues d'un point d'accès utilisateur quelconque ne doivent pas être réparties sur différentes voies C logiques.

Les données de type f issues d'un quelconque point d'accès utilisateur ne doivent pas être réparties sur différentes voies C logiques.

Les données de type Ds de tout point d'accès utilisateur quelconque ne doivent pas être réparties sur différentes voies C logiques.

NOTE – Le routage des données de type p ou de type f peut également être effectué par un réseau d'accès via le réseau de service de lignes louées par profilage. Ceci n'a aucune influence sur la présente Recommandation.

8.5 Stratification de la couche 2 en sous-couches et multiplexage sur des voies de communication

Les spécifications et les procédures de protocole relatives à l'interface V5.2 découlent directement de celles du 8.5/G.964 [8].

8.6 Multiplexage dans la couche 3

En général, le multiplexage dans la couche 3 est identique à celui spécifié en 8.6/G.964 [8], avec les adjonctions suivantes propres à l'interface V5.2.

Le protocole de commande de liaison multiplexe les informations de couche 3 qui sont transportées par la liaison de données de couche 2 de la commande de liaison à l'interface V5.2. Le protocole de commande de liaison est défini au paragraphe 16.

Le protocole BCC multiplexe les informations de couche 3 qui sont transportées par la liaison de données BCC de couche 2 à l'interface V5.2. Le protocole BCC est défini au paragraphe 17.

Le protocole de protection multiplexe les informations de couche 3 qui sont transportées par deux liaisons de données de protection de couche 2, dont l'une est sur la liaison primaire, l'autre sur la liaison secondaire à 2048 kbit/s. Le protocole de protection est défini au paragraphe 18.

8.7 Gestion des encombrements

Le contenu du présent paragraphe est identique à celui du 8.7/G.964 [8].

8.7.1 Commande de flux de bout en bout

Le contenu du présent paragraphe est identique à celui du 8.7.1/G.964 [8].

8.7.2 Gestion des encombrements à l'interface V5.2

Le contenu du présent paragraphe est identique à celui du 8.7.2/G.964 [8].

8.7.3 Blocage de points d'accès utilisateur RNIS dans la couche 2

Le contenu du présent paragraphe est identique à celui du 8.7.3/G.964 [8] et porte également sur les points d'accès au débit primaire du RNIS.

8.7.4 Contrôle de flux utilisant les mécanismes de la sous-couche LAPV5-DL

Le contenu du présent paragraphe est identique à celui du 8.7.4/G.964 [8].

9 Sous-couche fonction d'enveloppement de la procédure LAPV5 (LAPV5-EF)

Le contenu du présent paragraphe est identique à celui du paragraphe 9/G.964 [8].

10 Sous-couche liaison de données de la procédure LAPV5 (LAPV5-DL)

10.1 Structure de trame pour la communication d'homologue à homologue

Le contenu du présent paragraphe est identique à celui du 10.1/G.964 [8].

10.2 Trames non valides

Le contenu du présent paragraphe est identique à celui du 10.2/G.964 [8].

10.3 Eléments des procédures et formats des champs pour la communication d'homologue à homologue dans la sous-couche liaison de données

10.3.1 Format du champ adresse de liaison

Le contenu du présent paragraphe est identique à celui du 10.3.1/G.964 [8].

10.3.2 Variables du champ adresse de liaison

10.3.2.1 Bit d'extension du champ d'adresse (bit EA)

Le contenu du présent paragraphe est identique à celui du 10.3.2.1/G.964 [8].

10.3.2.2 Bit du champ commande/réponse

Le contenu du présent paragraphe est identique à celui du 10.3.2.2/G.964 [8].

10.3.2.3 Champ d'adresse V5DLaddr

Le champ d'adresse V5DLaddr est un nombre à 13 bits. Les valeurs comprises entre 0 et 8 175 ne doivent pas être utilisées pour désigner une entité de protocole de couche 3 car cette série est réservée à l'indication des points d'accès utilisateur RNIS.

Les valeurs définies pour le champ d'adresse V5DLaddr sont indiquées dans le Tableau 1.

10.3.3 Formats du champ commande

Le contenu du présent paragraphe est identique à celui du 10.3.3/G.964 [8].

10.3.4 Paramètres du champ commande et variables d'état associées

Le contenu du présent paragraphe est identique à celui du 10.3.4/G.964 [8].

10.3.5 Types de trames

Le contenu du présent paragraphe est identique à celui du 10.3.5/G.964 [8].

10.4 Définition des procédures d'homologue à homologue de la sous-couche liaison de données

Le contenu du présent paragraphe est identique à celui du 10.4/G.964 [8].

11 Sous-couche répétition de trames dans le réseau d'accès

Le contenu du présent paragraphe est identique à celui du paragraphe 11/G.964 [8].

12 Communication de sous-couche à sous-couche et fonction de mise en correspondance

Le contenu du présent paragraphe est identique à celui du paragraphe 12/G.964 [8].

Tableau 1/G.965 – Codage des valeurs d'adresse V5DL

Bits								V5DLaddr	
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
1	1	1	1	1	1	C/R	EA	Octet 1	
								Octet 2	
1	1	1	0	0	0	0	EA	Signalisation RTPC	(8176 decimal)
1	1	1	0	0	0	1	EA	Protocole de commande	(8177 decimal)
1	1	1	0	0	1	0	EA	Protocole BCC	(8178 decimal)
1	1	1	0	0	1	1	EA	Protocole de protection	(8179 decimal)
1	1	1	0	1	0	0	EA	Protocole de commande de liaison	(8180 decimal)

13 Structures générales du protocole de couche 3

13.1 Généralités

Dans les interfaces V5.2, différents protocoles de couche 3 sont pris en charge, utilisant tous le même "discriminateur de protocole". Aussi l'ensemble des protocoles peut-il être considéré comme un protocole "V5.2" unique composé de sous-protocoles distincts:

– protocole du RTPC;

– protocole de commande (commande commune et commande de point d'accès utilisateur);

– protocole de commande de liaison;

– protocole BCC;

– protocole de protection.

Chacun de ces protocoles de couche 3 est défini comme protocole orienté message. Chaque message comporte les parties suivantes (éléments d'information). Pour chacun de ces éléments, le nombre d'octets est indiqué (entre parenthèse):

a) discriminateur de protocole (1 octet);

b) adresse de couche 3 (2 octets);

c) type de message (1 octet);

d) autres éléments d'information, selon les besoins (le nombre d'octets dépend de l'élément d'information).

Les éléments d'information a), b) et c) sont présents dans tous les messages et font office d'en-tête pour chaque message, alors que les éléments d'information d) sont propres à chaque type de message.

Cette organisation est illustrée dans l'exemple que montre la Figure 7.

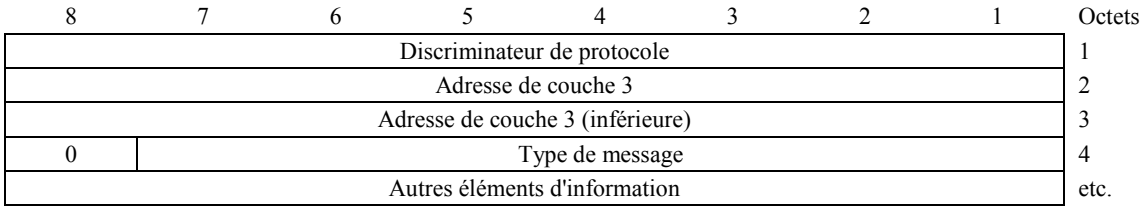


Figure 7/G.965 – Exemple d'organisation générale de message

Pour tous les protocoles V5.2 chaque élément d'information donné ne peut être présent qu'une seule fois dans un message donné.

Pour chacun des octets qui composent les éléments d'information, le bit appelé "bit 1" est transmis d'abord, suivi des bits 2, 3, 4, etc. De même, pour chaque élément d'information, l'octet appelé "octet 1" est transmis d'abord, suivi des octets 2, 3, 4, etc.

Lorsqu'un champ occupe plusieurs octets, le poids des bits décroît progressivement avec l'augmentation du numéro de l'octet. Le bit le moins significatif du champ est le bit de plus petit numéro de l'octet de numéro le plus grand.

Les bits éventuellement non utilisés dans la structure en octets d'un élément d'information particulier sont considérés comme étant "réservés" et doivent être codés comme "zéros binaires uniquement". Cependant, la réception d'un champ réservé codé par autre chose que "zéros binaires uniquement" n'est pas considérée comme une erreur de protocole.

13.2 Eléments d'information apparaissant dans tous les messages (en-tête)

Le présent paragraphe décrit les éléments d'information qui apparaissent dans chaque message (faisant office d'en-tête de message).

Ces éléments d'information ne comprennent pas de champ identifiant expressément l'élément d'information. Aussi chacun d'entre eux est identifié à partir de la position des octets dans chaque message.

13.2.1 Elément d'information Discriminateur de protocole

L'objet de l'élément d'information Discriminateur de protocole est de différencier les messages qui correspondent à l'un des protocoles V5 (protocole RTPC, protocole de commande, protocole de commande de liaison, protocole BCC ou protocole de protection) définis dans l'UIT-T G.964 [8] ou dans la présente Recommandation, des autres messages correspondant aux autres protocoles (qui ne sont pas définis dans ces Recommandations) et qui utilisent les mêmes connexions de liaisons de données d'interface V5 (en l'occurrence, V5.2).

NOTE – L'élément d'information Discriminateur de protocole est inclus dans les protocoles d'interface V5 pour conserver la compatibilité de structure avec les autres protocoles (c'est-à-dire avec l'UIT-T Q.931 [6]). Il fournit un mécanisme pour la compatibilité à l'avenir, permettant l'utilisation de la même connexion de liaison de données d'interface V5 pour d'autres protocoles de couche 3 encore non identifiés.

L'élément d'information Discriminateur de protocole forme la première partie de chaque message.

Il a une longueur d'un octet.

Sa structure et son codage sont indiqués à la Figure 8.

8	7	6	5	4	3	2	1	Octet
0	1	0	0	1	0	0	0	1

NOTE – Toutes les autres valeurs sont réservées.

Figure 8/G.965 – Elément d'information Discriminateur de protocole

13.2.2 Elément d'information Adresse de couche 3

L'objet de l'élément d'information Adresse de couche 3 est d'identifier l'entité de couche 3 dans l'interface V5.2 à laquelle le message reçu ou transmis s'applique.

L'élément d'information Adresse de couche 3 forme la seconde partie de chaque message (il vient après l'élément d'information Discriminateur de protocole).

La longueur de l'élément d'information Adresse de couche 3 doit être de 2 octets.

Sa structure dépend du protocole; pour le protocole RTPC voir 13.4.3/G.964 [8], et pour le protocole de commande voir 14.4.2.3/G.964 [8]. Pour le protocole de commande de liaison, cet élément d'information conserve la même adresse de couche 3, bien qu'elle serve à faire référence aux liaisons à 2048 kbit/s (elle est définie au 16.3.2.1). Pour le protocole BCC, cet élément d'information s'appelle "Numéro de référence BCC" et il est défini au 17.4.1. Pour le protocole de protection, cet élément d'information s'appelle "Identification de voie C logique" et il est défini au 18.5.1.

13.2.3 Elément d'information Type de message

L'élément d'information Type de message sert à identifier la fonction du message envoyé ou reçu.

L'élément d'information Type de message forme la troisième partie de chaque message (il vient après l'élément d'information Adresse de couche 3).

La longueur de l'élément d'information Type de message doit être de 1 octet.

Sa structure est indiquée à la Figure 9.

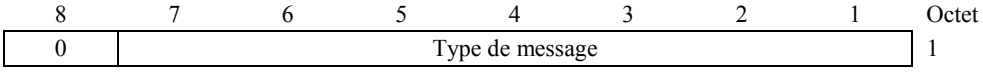


Figure 9/G.965 – Elément d'information Type de message

Son codage suit les spécifications de la présente Recommandation. Pour une liste détaillée des points de code de message, voir l'Annexe E.

La structure générale du codage du champ type de message est indiquée dans le Tableau 2.

Tableau 2/G.965 – Structures du codage du type de message pour les protocoles V5.2

Bits							Types de messages
7	6	5	4	3	2	1	
0	0	0	–	–	–	–	Types de messages de protocole RTPC
0	0	1	0	–	–	–	Types de messages de protocole de commande
0	0	1	1	–	–	–	Types de messages de protocole de protection
0	1	0	–	–	–	–	Types de messages de protocole BCC
0	1	1	0	–	–	–	Types de messages de protocole de commande de liaison
NOTE – Toutes les autres valeurs sont réservées.							

13.3 Autres éléments d'information

Ces éléments d'information peuvent apparaître dans les différents messages, soit facultativement soit obligatoirement selon la sémantique ou l'application de protocole du message.

Ces éléments d'information sont propres à chaque protocole. Pour les éléments d'information propres au protocole RTPC, voir 13.4/G.964 [8], pour les éléments d'information propres au protocole de commande, voir 14.4.4.2/G.964 [8], pour les éléments d'information propres au protocole de commande de liaison, voir 16.3.2, pour les éléments d'information propres au protocole BCC, voir 17.4, et pour les éléments d'information propres au protocole de protection, voir 18.5.

La liste complète des éléments d'information d'interface V5.2 est donnée dans l'Annexe E.

13.4 Définition fonctionnelle et contenu des informations des messages de protocole

Dans les définitions de protocole de la présente Recommandation, les différents messages sont spécifiés; l'accent est mis sur la définition fonctionnelle et le contenu informationnel de chaque message. Chaque définition comprend:

a) une brève description du message, du sens dans lequel il est envoyé et de l'utilisation qui en est faite;

b) un tableau donnant la liste de tous les éléments d'information par ordre d'apparition dans le message (même ordre relatif pour tous les types de message). Pour chaque élément d'information le tableau indique:

   1) le paragraphe de la présente Recommandation qui décrit l'élément d'information;

   2) le sens dans lequel il peut être envoyé: c'est-à-dire, dans le sens réseau d'accès vers commutateur local, commutateur local vers réseau d'accès ou dans les deux sens;

   3) s'il est obligatoire ("M") ou facultatif ("O");

   4) la longueur de l'élément d'information en octets.

13.5 Jeux de code

Le codage des éléments d'information fait appel aux règles définies en 4.5.1/Q.931 [6], sans la fonctionnalité de l'élément d'information Inversion caractère, autrement dit, le jeu de code est unique.

14 Spécification du protocole de signalisation RTPC et multiplexage de couche 3

Le contenu du présent paragraphe est identique à celui du paragraphe 13/G.964 [8].

15 Caractéristiques et protocole de commande

Le présent paragraphe définit la commande de point d'accès et les caractéristiques, protocoles et procédures communes de commande sous forme de spécifications normatives de machines à états finis (FSM, *finite state machine*) avec à l'appui la description narrative des procédures.

15.1 Indication d'état et commande de point d'accès utilisateur au débit de base RNIS

Le contenu du présent paragraphe est identique à celui du 14.1/G.964 [8].

15.2 Indication d'état et commande de point d'accès utilisateur RTPC

Le contenu du présent paragraphe est identique à celui du 14.2/G.964 [8].

15.3 Indication d'état et commande de point d'accès utilisateur au débit primaire RNIS

15.3.1 Aspects généraux

L'indication d'état des points d'accès utilisateur au débit primaire RNIS repose sur la répartition précise des responsabilités entre réseau d'accès et commutateur local. Seules les informations d'état de point d'accès utilisateur qui ont rapport à la commande d'appel auront une influence, via l'interface V5.2, sur la machine à états finis du commutateur local.

Les essais des points d'accès (par exemple, rebouclage) doivent être placés sous la responsabilité du réseau d'accès. Les essais qui interfèrent avec le service ne doivent cependant être effectués que lorsque le point d'accès utilisateur est à l'état "bloqué", soit en raison d'une anomalie, soit sur demande au commutateur local et avec son accord. Cela suppose deux catégories d'états s'appliquant de part et d'autre de l'interface V5.2:

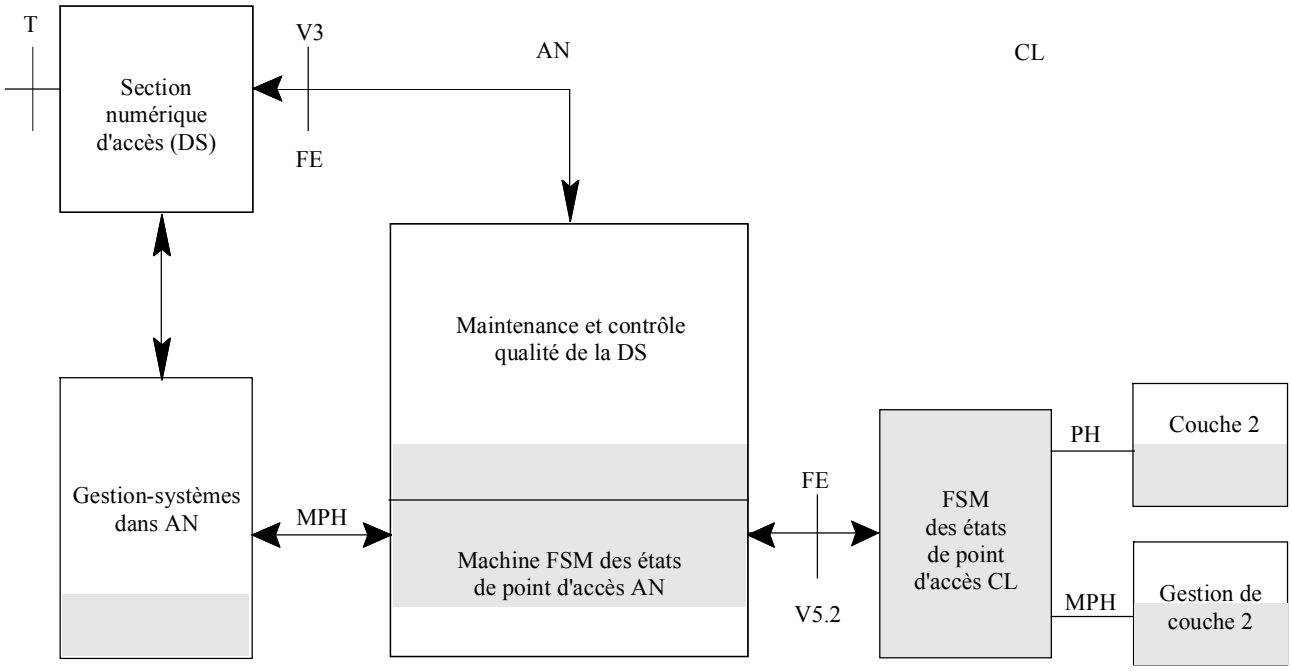
– l'état opérationnel;

– l'état non opérationnel.

Il faut disposer d'autres états dans le réseau d'accès pour la maintenance de la section numérique (DS, *digital section*) et du point d'accès utilisateur. L'accès au débit primaire RNIS est actif de manière permanente à la couche 1. Si la section numérique (DS) détecte une perte de capacité de couche 1 côté utilisateur, l'accès est considéré comme n'étant pas opérationnel du point de vue du commutateur local, alors que du point de vue du réseau d'accès, la section DS fonctionne normalement. Cette distinction est faite par la gestion du réseau d'accès et signalée au commutateur local à l'aide d'éléments de fonction (FE, *function element*) et de primitives de gestion supplémentaires.

La Figure 10 montre le modèle fonctionnel pour la commande du point d'accès utilisateur au débit primaire RNIS. Les zones grisées indiquent le domaine défini dans la présente Recommandation. La définition des autres fonctions et capacités sort du champ d'application de la présente Recommandation. On consultera l'Annexe C pour de plus amples renseignements sur les conditions de base des fonctions de gestion dans le réseau d'accès et dans le commutateur local.

Seules seront spécifiées par la suite les fonctions et procédures qui se rapportent à l'interface V5.2.



NOTE – Les éléments de fonction et les primitives indiqués dans cette figure sont définis au 15.3.2.

Figure 10/G.965 – Modèle fonctionnel de la commande des points d'accès au débit primaire

15.3.2 Evénements et éléments de fonction applicables à la commande des machines à états

Les Tableaux 3, 4, 5 et 6 présentent l'ensemble des éléments de fonction (FE) se rapportant à l'interface V5.2, les éléments de fonction définis dans l'UIT-T G.962 [10] ainsi que les primitives (PH et MPH) envoyées vers la couche 2 et la fonction de gestion implantée dans le réseau d'accès ou dans le commutateur local (voir également Figures 3/G.964 [8] et 4/G.964 [8]). La Figure 10 donne les définitions et les procédures pour les éléments de fonction et les événements qui sont utilisés dans les Tableaux 3 à 6.

Tableau 3/G.965 – Ensemble des éléments de fonctions de l'UIT-T G.962 [10] qui se rapportent à l'interface V5.2

Elément de fonction	Nom	DS ⇔ ET	Signification au terminal dans CL
FE-A	Fonctionnement normal de la section numérique	→	Non directement applicable
FE-B	Fonctionnement normal du terminal	←	Non directement applicable
FE-C	Rebouclage intempestif	Maintenance du réseau AN	Non directement applicable
FE-D	LOS ou LFA au terminal (FC2)	Maintenance du réseau AN	Non directement applicable
FE-E	LOS côté ligne du NT1 (FC3)	Maintenance du réseau AN	Non directement applicable
FE-F	LOS ou LFA au point de référence V3 du terminal (FCL)	Maintenance du réseau AN	Non directement applicable
FE-G	LOS ou LFA au point de référence T du NT1 (FC4)	Maintenance du réseau AN	Non directement applicable
FE-H	FC3 et FC4 simultanément	Maintenance du réseau AN	Non directement applicable
FE-I	Perte d'alimentation en NT1	Maintenance du réseau AN	Non directement applicable
FE-K	FE-I et FE-D simultanément	Maintenance du réseau AN	Non directement applicable
FE-L	LOS côté ligne de LT (FC1)	Maintenance du réseau AN	Non directement applicable
NOTE – Les éléments de fonction FE-M à FE-P de l'UIT-T G.962 [10] font référence à des anomalies sur une liaison numérique séparée et sont donc sans objet. Les éléments FE-Q à FE-T font référence au fonctionnement en rebouclage et sortent du domaine d'application de l'interface V5.2. Les éléments FE-U à FE-Y sont apparentés à la détection d'erreur de CRC-4 et ne se rapportent qu'au contrôle de performance (voir 15.3.4).			

Tableau 4/G.965 – Ensemble des éléments de fonction de l'interface V5.2

Elément de fonction	Nom	AN ⇔ CL	Description
FE201	Déblocage	←	Demande ou accusé de réception
FE202	Déblocage	→	Demande ou accusé de réception
FE203	Blocage	←	Commande
FE204	Blocage	→	Commande
FE205	Demande de blocage	→	Demande
FE206	Evaluation du niveau de qualité	→	Informations de performance (Note 1)
FE207	Blocage du canal D	←	Commande (Note 2)
FE208	Déblocage du canal D	←	Commande (Note 2)

Tableau 4/G.965 – Ensemble des éléments de fonction de l'interface V5.2

Elément de fonction	Nom	AN ⇔ CL	Description
FE209	TE hors service	→	Indication d'anomalie utilisateur
FE210	Anomalie interne au réseau	→	Indication d'anomalie réseau
NOTE 1 – Les informations d'évaluation de qualité peuvent être envoyées par la gestion du réseau d'accès lorsqu'elle est dans l'état AN/CL2.0 (voir également 15.3.4). NOTE 2 – Les commandes "blocage du canal D" et "déblocage du canal D" sont utilisées pour interrompre ou reprendre le fonctionnement du canal D en amont d'un point d'accès utilisateur RNIS particulier, conformément à la caractéristique du 8.7.3/G.964 [8]. Ces commandes peuvent apparaître pendant que l'entité est dans l'état AN/CL2.0, sans transition d'état.			

Les éléments de fonction sont signalés à la section numérique immédiatement après la détection d'un événement. L'effet sur la commande de point d'accès, qui concerne les procédures de commande d'appel, est retardé par une procédure appropriée d'essai de persistance. Cela sort du domaine d'application de la présente Recommandation et n'est pas répercuté sur la machine FSM du réseau d'accès (point d'accès au débit primaire RNIS). Il faut se reporter à l'UIT-T I.431 [9] qui donne un exemple de procédure d'essai de persistance.

Tableau 5/G.965 – Ensemble des primitives dans le commutateur local

Primitive	FSM ⇔ couche 2/Gestion	Description
MPH-UBR	←	Demande de déblocage
MPH-UBR	→	Demande de déblocage
MPH-UBI	→	Indication de déblocage
MPH-BI	←	Commande de blocage
MPH-BI	→	Commande de blocage
MPH-BR	→	Demande de blocage entrante
PH/MPH-AI	→	Accès activé (opérationnel)
PH/MPH-DI	→	Accès désactivé (non opérationnel)
MPH-UF	→	Indication d'anomalie utilisateur
MPH-NF	→	Indication d'anomalie réseau
MPH-GI	→	Informations d'évaluation de qualité avec paramètre (Note 1)
MPH-DB	←	Blocage du canal D au départ d'un point d'accès utilisateur (Note 2)
MPH-DU	←	Déblocage du canal D au départ d'un point d'accès utilisateur (Note 2)
NOTE 1 – Les informations d'évaluation peuvent être envoyées par la gestion du réseau d'accès pendant qu'elle est dans l'état CL2.0 (voir également 15.3.4). NOTE 2 – Les primitives "MPH-DB" et "MPH-DU" sont utilisées pour interrompre ou reprendre le fonctionnement du canal D en amont d'un point d'accès utilisateur RNIS particulier, conformément à la prescription du 8.7.3/G.964 [8]. Ces commandes peuvent apparaître pendant que l'entité est dans l'état CL2.0, sans transition d'état.		

15.3.3 Machines FSM des points d'accès utilisateur au débit primaire RNIS pour un réseau d'accès (point d'accès au RNIS) et pour un commutateur local (point d'accès au RNIS)

Les primitives, éléments de fonction et tables d'état sont donnés par la définition du comportement fonctionnel et de la coopération entre les divers blocs fonctionnels. Aucune limitation n'est imposée quant à l'implémentation de ces fonctions, du moment que cette implémentation est conforme aux fonctionnalités définies dans la présente Recommandation à l'interface V5.2 et dans la section numérique d'accès au débit primaire.

Tableau 6/G.965 –Ensemble des primitives de gestion concernant l'interface V5.2 dans le réseau d'accès

Primitive	Gestion ⇔ FSM	Description
MPH-UBR	→	Demande de déblocage
MPH-UBR	←	Demande de déblocage
MPH-UBI	←	Indication de déblocage
MPH-BI	→	Commande de blocage
MPH-BI	←	Commande de blocage
MPH-BR	→	Demande de blocage
MPH-NOF	←	Utilisateur et section numérique normaux
MPH-Eic	←	Maintenance du réseau AN
MPH-Eid	←	Maintenance du réseau AN
MPH-Eie	←	Maintenance du réseau AN
MPH-Eig	←	Maintenance du réseau AN
MPH-Eih	←	Maintenance du réseau AN
MPH-Eii	←	Maintenance du réseau AN
MPH-Eik	←	Maintenance du réseau AN
MPH-Eil	←	Maintenance du réseau AN
MPH-EIlos	←	Maintenance du réseau AN
MPH-UF	→	Indication d'anomalie utilisateur
MPH-NF	→	Indication d'anomalie réseau
MPH-GI	→	Information d'évaluation de qualité avec paramètre (Note 1)
MPH-DB	←	Blocage d'un canal D au départ d'un point d'accès utilisateur (Note 2)
MPH-DU	←	Déblocage d'un canal D au départ d'un point d'accès utilisateur (Note 2)
MPH-PAR	→	Demande de fonctionnement d'un point d'accès pour une fonction PL (Note 3)
MPH-PAI	←	Indication de fonctionnement d'un point d'accès pour une fonction de ligne permanente (Note 3)
MPH-PDR	→	Demande de non-fonctionnement d'un point d'accès pour une fonction PL (Note 3)
MPH-PDI	←	Indication de non-fonctionnement d'un point d'accès pour une fonction PL (Note 3)

Tableau 6/G.965 –Ensemble des primitives de gestion concernant l'interface V5.2 dans le réseau d'accès

Primitive	Gestion ⇔ FSM	Description
MPH-LxAR	→	Activation de rebouclage (Note 3)
MPH-AI	←	Indication d'activation de rebouclage (Note 3)
MPH-DR	→	Demande de libération de rebouclage (Note 3)
NOTE 1 – Les informations d'évaluation de qualité peuvent être envoyées par la gestion du réseau d'accès pendant qu'elle est dans l'état AN2.0, voir également 15.3.4. NOTE 2 – Les primitives de commande "MPH-DB" et "MPH-DU" sont utilisées pour interrompre ou reprendre le fonctionnement du canal D en amont d'un point d'accès utilisateur RNIS particulier, conformément à la prescription du 8.7.3/G.964 [8]. Ces commandes peuvent apparaître pendant que l'entité est dans l'état AN2.0, sans transition d'état. NOTE 3 – Les sept dernières primitives ne sont pas directement applicables à l'interface V5.2 mais elles sont données à titre d'information et pour décrire complètement la réaction de la machine FSM à la réception de ces événements, même lorsqu'elle est dans des états applicables à l'interface V5.2.		

15.3.3.1 Description des états

Les procédures d'activation et de désactivation du point d'accès utilisateur, comme elles sont spécifiées dans les machines FSM du point d'accès, tiennent compte des principes donnés en 7.1/G.964 [8].

La demande de blocage ne doit être émise par la gestion du réseau d'accès que lorsqu'elle est dans l'état opérationnel. Cette demande n'a aucune incidence sur l'état sauf si le commutateur local répond par l'élément FE203.

Une indication de blocage immédiat a un effet immédiat sur les deux machines FSM dans tout état où elle s'applique. Aucune confirmation expresse de cette indication n'est requise.

Le déblocage doit être coordonné des deux côtés. Une demande de déblocage nécessite donc l'émission d'une confirmation du côté opposé. Cette coordination est assurée pendant la durée des deux états de déblocage. Si une indication de blocage est reçue de l'autre côté alors que le point est dans l'état de déblocage local, cette situation est interprétée comme une absence de confirmation pouvant ne concerner que la gestion-systèmes.

La demande de déblocage peut également être utilisée par le système de gestion pour confirmer l'état des machines à états de la couche 1.

La machine FSM du réseau d'accès pour le point d'accès au débit primaire du RNIS assure la fonction facultative de ligne permanente, et il faut alors que la section numérique d'accès et le terminal utilisateur puissent devenir opérationnels sous contrôle du réseau d'accès alors que le commutateur local n'est pas opérationnel. Cette procédure utilise les états AN1.1 et AN3.0.

La maintenance de la section numérique (DS) et les essais de rebouclage (voir les éléments FE-Q à FE-T de l'UIT-T G.962 [10]) peuvent utiliser les états supplémentaires AN4, qui sont hors du domaine d'application de la présente Recommandation. Ces états ne sont pris qu'à partir de l'état AN1.0 ou de l'état AN1.2.

L'état AN4 ne peut être pris qu'à partir des états AN1 et ne peut revenir qu'à l'état AN1.0. L'alignement des machines FSM du réseau d'accès et du commutateur local nécessite l'envoi de l'élément FE204 au commutateur local avant que la procédure de déblocage puisse être appliquée.

15.3.3.2 Définition des états de commande de point d'accès

Les machines FSM des points d'accès utilisateur ne reflètent que les états physiques (de couche 1) des points d'accès RNIS, tels qu'ils sont vus à partir du réseau d'accès et du commutateur local. La responsabilité de la commande d'appel revient au protocole RNIS.

15.3.3.2.1 Machine FSM de point d'accès utilisateur au débit primaire RNIS – Réseau d'accès (point d'accès RNIS)

Etats non opérationnels (AN1 et AN3): le blocage du canal D a été appliqué au point d'accès. Aucune information de couche 2 ne doit donc être transmise par répétiteur de trames vers le commutateur local et le point d'accès ne peut être utilisé pour émettre ou recevoir des appels.

Etat bloqué (AN1.0): le point d'accès est dans l'état non opérationnel et aucun côté n'a lancé de déblocage. Deux sous-états sont nécessaires pour satisfaire aux spécifications de section numérique et d'interface usager-réseau.

Etat déblocage local (AN1.1): le réseau d'accès a lancé un déblocage (en envoyant un élément FE202) et attend confirmation du commutateur local. Bien que la section numérique soit en condition normale, la machine FSM du réseau d'accès doit signaler au terminal (TE) que l'accès n'est pas opérationnel, en envoyant un élément RAI.

Etat déblocage distant (AN1.2): le commutateur local a lancé un déblocage (en envoyant un élément FE201) et attend confirmation du réseau d'accès. Deux sous-états sont nécessaires pour satisfaire aux spécifications de section numérique et d'interface usager-réseau. Ils correspondent aux deux sous-états de l'état AN1.0.

NOTE – Les états AN1.1 et AN1.2 fournissent un mécanisme pour le déblocage synchronisé des points d'accès. Le réseau d'accès peut rester dans ces états pendant une durée indéterminée.

Etats PL opérationnelle (AN3): la gestion du réseau d'accès a lancé le fonctionnement du point d'accès pour la fonction de ligne permanente (PL) alors que le commutateur local ne prend pas en charge le déblocage du point d'accès (AN1.1). En cas de rapport d'anomalie de la part de la section numérique ou à la demande de la gestion du réseau d'accès, la machine FSM du point d'accès utilisateur retourne à l'état AN1.02.

Etats opérationnels (AN2.0): le point d'accès est opérationnel du point de vue du réseau d'accès et du commutateur local, les liaisons de couche 2 (et de couche 3) peuvent être établies et le point d'accès peut être utilisé afin d'émettre ou de recevoir des appels.

15.3.3.2.2 Machine FSM de point d'accès utilisateur RNIS au débit primaire RNIS – Commutateur local (point d'accès RNIS)

Etats non opérationnels (CL1): aucune information de couche 2 n'est attendue au commutateur local et le point d'accès ne peut pas être utilisé pour émettre ou recevoir des appels.

Etat bloqué (CL1.0): le point d'accès est dans l'état non opérationnel et aucun des deux côtés n'a lancé de déblocage.

Etat déblocage local (CL1.1): le commutateur local a lancé un déblocage (en envoyant un élément FE201) et attend confirmation du réseau d'accès.

Etat déblocage distant (CL1.2): le réseau d'accès a lancé un déblocage (en envoyant un élément FE202) et attend confirmation du commutateur local.

NOTE – Les états CL1.1 et CL1.2 fournissent un mécanisme pour le déblocage synchronisé des points d'accès. Le commutateur local peut rester dans ces états pendant une durée indéterminée.

Etats opérationnels (CL2.0): la couche 1 de l'accès au débit primaire est opérationnelle. Des liaisons de couche 2 (et de couche 3) peuvent être établies. Le point d'accès peut être utilisé pour émettre ou pour recevoir des appels.

15.3.3.3 Principes et procédures

15.3.3.3.1 Généralités

Les sous-paragraphes suivants décrivent le mécanisme implémenté dans les machines FSM du réseau d'accès et du commutateur local pour les points d'accès utilisateur RNIS (accès au débit primaire). Ces machines sont présentées dans les tables de transition d'état correspondantes.

Les mécanismes suivants sont décrits:

– blocage;
– demande de blocage;
– déblocage coordonné;
– indication d'anomalie réseau ou d'anomalie utilisateur;
– prise en charge de la fonction de ligne permanente.

15.3.3.3.2 Blocage

Un point d'accès utilisateur qui se trouve dans un des états opérationnels (AN2 ou CL2) peut être bloqué par l'un ou l'autre côté. Cependant, la gestion AN n'est pas informée de l'état de l'appel à ce point d'accès et ne doit donc appliquer cette procédure qu'en cas d'anomalie ou d'autre situation particulière (après que la procédure d'essai de persistance a réussi) qui justifie d'agir sur le service.

Lorsque la gestion-systèmes du réseau d'accès émet une primitive MPH-BI, la machine FSM envoie un élément FE204 (commande de blocage) au commutateur local et passe à l'état bloqué AN1.0, sous-état AN1.02 afin de signaler la situation non opérationnelle à l'équipement terminal.

La machine à états finis du réseau d'accès peut aussi bloquer le point d'accès de manière autonome en cas d'indication par la section numérique d'une situation d'anomalie. Les sous-états appropriés prennent en charge la commande de point d'accès grâce à la section numérique (DS), conformément aux Recommandations appropriées.

Lorsque la gestion-systèmes du commutateur local émet une primitive MPH-BI, la machine FSM envoie un élément FE203 (commande de blocage) au réseau d'accès et passe à l'état bloqué CL1.0.

15.3.3.3.3 Demande de blocage

Le mécanisme de demande de blocage permet un blocage non urgent des points d'accès (par exemple, pour des opérations de maintenance pouvant être différées). Dans ce cas, la gestion AN émet une primitive de demande de blocage (MPH-BR) provoquant l'envoi d'un élément FE205 au commutateur local. Cette demande doit être transmise par la machine FSM du commutateur local à la gestion CL sous la forme d'une primitive MPH-BR.

La gestion-systèmes CL, informée de l'état de l'appel, peut donner suite à la demande en émettant une primitive MPH-BI provoquant l'envoi d'un élément FE203 (commande de blocage) au réseau d'accès, avant de passer à l'état bloqué.

En cas de connexion semi-permanente, la gestion-systèmes CL ne donne pas suite à cette demande mais envoie une primitive MPH-UBR à titre de confirmation négative.

La gestion-systèmes AN peut annuler la demande de blocage en émettant une primitive MPH-UBR. La gestion-systèmes CL peut ensuite recevoir une primitive MPH-UBI et annuler la demande de blocage (c'est-à-dire ignorer la demande précédemment reçue) si le point d'accès n'a pas encore été bloqué. Si c'est le cas, le commutateur local peut lancer la procédure de déblocage en émettant une primitive MPH-UBR.

15.3.3.3.4 Déblocage coordonné

Le déblocage d'un point d'accès nécessite une coordination de part et d'autre de l'interface. Une demande de déblocage nécessite une confirmation du côté opposé. Pour assurer cette coordination, il existe deux états distincts de déblocage (déblocage local et déblocage distant) dans les deux machines FSM. Cette procédure est entièrement symétrique entre le réseau d'accès et le commutateur local. Si celui-ci a besoin d'un déblocage, il émet une primitive MPH-UBR, envoie un élément FE201 (demande de déblocage) et passe à l'état "déblocage local" (CL1.1). Le réseau d'accès passe à l'état "déblocage distant" (AN1.2), au sous-état correspondant à l'état qu'il avait dans l'état AN1.0 et envoie une primitive MPH-UBR à son entité de gestion, laquelle peut donner son accord puis répond par une primitive MPH-UBR (accusé de réception de déblocage), envoie l'élément FE202 et passe à l'état "opérationnel" (AN2.0).

Si le commutateur local est dans l'état "déblocage local" et qu'il reçoit cet accusé de réception, sa machine FSM passe à l'état "opérationnel" (CL2.0) et envoie à son entité de gestion une primitive MPH-UBI. La gestion AN peut aussi prendre l'initiative, auquel cas la même procédure s'applique.

Lorsque le réseau d'accès ou le commutateur local se trouvent dans l'état "déblocage distant" (AN1.2x, CL1.2x) et reçoivent respectivement l'élément FE204 ou l'élément FE203, l'état du point d'accès de la machine FSM est remis à "bloqué" (AN1.0, CL1.0) et une primitive MPH-BI est envoyée à l'entité de gestion. Cette opération annule une précédente demande de déblocage issue du côté opposé.

La gestion AN peut annuler la demande de blocage en envoyant une primitive MPH-UBR. La gestion CL peut alors recevoir la primitive MPH-UBI et annuler la demande de blocage (c'est-à-dire qu'elle ignore la demande précédemment reçue) si le point d'accès n'a pas auparavant été bloqué. Si c'est le cas, le commutateur local peut lancer la procédure de déblocage en émettant une primitive MPH-UBR.

Voir au C.5 les exigences de base de la gestion-systèmes.

15.3.3.3.5 Indication d'anomalie réseau ou d'anomalie utilisateur

Pour la prise en charge totale du service RNIS le commutateur local doit connaître la raison du blocage du point d'accès, c'est-à-dire si le blocage a eu lieu à cause d'une anomalie dont l'utilisateur est responsable ou d'une anomalie dont le réseau est responsable. Cette information ne peut être fournie par la gestion-systèmes AN que si la localisation de l'anomalie est connue grâce aux informations fournies par la section numérique d'accès et grâce aux capacités de détection d'anomalie interne. Les situations d'anomalie (FC) 2 et 4 (FE-G seul, FE-G et FE-K ensemble, sous certaines conditions) sont comprises comme des anomalies utilisateur, mais le réseau d'accès peut donner confirmation de ceci en appliquant la procédure de localisation d'anomalie avant d'envoyer la primitive d'indication au commutateur local. L'identification de "perte d'alimentation en NT1" (FE-I) en tant qu'anomalie réseau ou anomalie utilisateur dépend de l'arrangement de l'alimentation au niveau de la terminaison NT1.

La gestion AN est tenue d'informer la gestion CL en envoyant les informations appropriées (primitives MPH-UF ou MPH-NF) à la machine FSM du réseau d'accès (point d'accès au débit primaire du RNIS) qui envoie alors respectivement l'élément FE209 ou l'élément FE210 à la machine FSM du commutateur local (point d'accès au débit primaire). La machine FSM du commutateur local informe alors la gestion CL en conséquence.

15.3.3.3.6 Prise en charge de la fonction de ligne permanente

Comme le point d'accès utilisateur est constamment actif, il n'y a pas de caractéristiques particulières s'appliquant à la commande d'interface V5.2 de point d'accès au débit primaire hormis les procédures déjà définies. Si le commutateur local bloque un point d'accès utilisateur ou si, après correction d'une anomalie de la section numérique ou de l'équipement terminal, la procédure de déblocage n'est pas prise en charge par le commutateur local, la gestion-systèmes AN peut amener le point d'accès

utilisateur dans l'état PL opérationnelle en envoyant une primitive MPH-PAR. La machine FSM du réseau d'accès passe à l'état AN3.0 et donne confirmation par une primitive MPH-PAI. A l'aide d'une primitive MPH-PDR la gestion AN peut désactiver la fonction de ligne permanente, qui se répercute sur la machine FSM par l'état AN1.02 et par l'envoi d'une primitive MPH-PDI. Cette procédure ne s'applique pas au commutateur local.

15.3.3.4 Machine FSM de point d'accès utilisateur RNIS dans le réseau d'accès

La machine FSM de point d'accès utilisateur au débit primaire du RNIS est définie dans le Tableau 7 conformément aux hypothèses indiquées dans la Figure 10.

Tableau 7/G.965 – Machine FSM dans le réseau d'accès pour les points d'accès utilisateur au débit primaire RNIS

Etat	AN1.01	AN1.02	AN1.1	AN1.21	AN1.22	AN2.0	AN3.0
Nom de l'état / Evénement	Bloqué 1	Bloqué 2	Déblocage local	Déblocage distant 1	Déblocage distant 2	Accès opérationnel	PL opérationnelle
Signal vers V3	**NOF**	**RAI**	**RAI**	**NOF**	**RAI**	**NOF**	**NOF**
FE201	MPH-UBR 1.21	MPH-UBR 1.22	MPH-UBI 2.0	MPH-UBR –	MPH-UBR –	FE202; MPH-UBI –	MPH-UBI 2.0
FE203	–	–	MPH-BI 1.02	MPH-BI 1.01	MPH-BI 1.02	MPH-BI 1.02	MPH-BI –
MPH-UBR	MPH-BI –	FE202 1.1	FE202 –	FE204; MPH-BI 1.01	FE202; MPH-UBI 2.0	FE202; MPH-UBI –	MPH-PAI –
MPH-BI	FE204 –	FE204 –	FE204 1.02	FE204 1.01	FE204 1.02	FE204 1.02	FE204 1.02
MPH-BR	–	–	/	/	/	FE205 –	/
NOF	MPH-NOF 1.02	MPH-NOF –	–	MPH-NOF 1.22	MPH-NOF –	–	–
LOS/LFA	MPH-EIlos 1.02	MPH-Eilos –	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02
FE-C	MPH-EIc 1.02	MPH-Eic –	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-EIc 1.02
FE-D	MPH-EId –	MPH-EId 1.01	FE204; MPH-Eid 1.01	FE204; MPH-Eid 1.01	FE204; MPH-Eid 1.01	FE204; MPH-EId 1.01	FE204; MPH-EId 1.01
FE-E	MPH-EIe –	MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01
FE-G	MPH-EIg 1.02	MPH-EIg –	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02
FE-H	MPH-EIh 1.02	MPH-EIh –	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02
FE-I	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –
FE-K	MPH-EIk –	MPH-EIk 1.01	FE204; MPH–EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01

Tableau 7/G.965 – Machine FSM dans le réseau d'accès pour les points d'accès utilisateur au débit primaire RNIS

Etat	AN1.01	AN1.02	AN1.1	AN1.21	AN1.22	AN2.0	AN3.0
Nom de l'état / Evénement	Bloqué 1	Bloqué 2	Déblocage local	Déblocage distant 1	Déblocage distant 2	Accès opérationnel	PL opérationnelle
Signal vers V3	**NOF**	**RAI**	**RAI**	**NOF**	**RAI**	**NOF**	**NOF**
FE-L	MPH-EIl 1.02	MPH-EIl –	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02
MPH-LxAR	FE-Q/R 4.x	FE-Q/R 4.x	/	FE-Q/R 4.x	FE-Q/R 4.x	/	/
MPH-UF	FE209 –	FE209 –	/	FE209 –	FE209 –	/	/
MPH-PAR	/	/	MPH-PAI 3.0	/	/	/	–
MPH-PDR	/	/	/	/	/	/	MPH-PDI 1.02
MPH-NF	FE210 –	FE210 –	/	FE210 –	FE210 –	/	/
MPH-GI	/	/	/	/	/	FE206 –	/
FE207	/	/	/	/	/	MPH-DB –	/
FE208	/	/	/	/	/	MPH-DU –	/

– Un tiret indique qu'il n'y a pas de transition d'état.

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état.

NOF Indique les trames de fonctionnement normales.

LOS/FFA Indique la perte du signal ou la perte de l'alignement des trames.

NOTE 1 – Les états AN4 ne sont pas applicables à l'interface V5.2 et ne sont pas définis dans la présente Recommandation.

NOTE 2 – Si le blocage du canal D a été appliqué à un point d'accès utilisateur après réception de l'élément FE207 alors que ce point d'accès était dans l'état AN2.0 et si la machine FSM du point d'accès quitte cet état, le blocage du canal D doit être supprimé.

La machine FSM du réseau d'accès prend en charge les événements d'anomalie simple de la section numérique, sauf si des anomalies multiples sont signalées par celle-ci, c'est-à-dire en présence des éléments de fonction FE-H ou FE-K. La détection d'un événement nouveau signifie qu'une anomalie signalée auparavant a disparu.

La machine FSM du réseau d'accès donne au gestionnaire local du réseau d'accès un moyen de contrôler que la machine FSM est dans l'état opérationnel, sans qu'il soit nécessaire de suivre toute la séquence de blocage et de déblocage. Ce mécanisme est interne au réseau d'accès. Pour le mettre en œuvre, la gestion-systèmes AN envoie une primitive MPH-UBR et reçoit en retour l'information indiquant si la machine FSM est ou non dans l'état non opérationnel.

15.3.3.5 Machine FSM de point d'accès au RNIS au niveau du commutateur local

Le Tableau 8 donne la machine à états finis du commutateur local.

Tableau 8/G.965 – Machine FSM du commutateur local pour les points d'accès utilisateur RNIS de base

Etat	CL1.0	CL1.1	CL1.2	CL2.0
Nom de l'état / Evénement	Bloqué	Déblocage local	Déblocage distant	Accès opérationnel
MPH-UBR	FE201 1.1	FE201 –	PH/MPH-AI; FE201 2.0	FE201 –
MPH-BI	FE203 –	FE203 1.0	FE203 1.0	FE203 1.0
FE202	MPH-UBR 1.2	PH/MPH-AI 2.0	MPH-UBR –	MPH-UBI
FE204	–	MPH-BI 1.0	MPH-BI 1.0	MPH-BI; PH/MPH-DI 1.0
FE205	–	–	–	MPH-BR –
FE206	/	/	/	MPH-GI –
FE209	MPH-UF –	MPH-UF –	/	/
FE210	MPH-NF –	MPH-NF –	/	/
MPH-DB	/	/	/	FE207 –
MPH-DU	/	/	/	FE208 –

– Un tiret indique l'absence de transition d'état.

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état.

NOTE – Si le blocage du canal D a été appliqué à un point d'accès utilisateur dans l'état CL2.0 par envoi d'une primitive MPH-DB, la gestion-systèmes est informée du fait que le blocage du canal D dans le réseau d'accès va être supprimé après que la machine FSM du point d'accès au réseau d'accès a quitté l'état AN2.0.

La machine FSM du commutateur local offre au gestionnaire du commutateur local le moyen de vérifier, par l'envoi d'une primitive MPH-UBR, qu'elle est dans l'état opérationnel, sans avoir à passer par toute la séquence de blocage et de déblocage.

Contrairement à la situation correspondante pour le réseau d'accès, ce mécanisme n'est pas interne au commutateur local (CL) et exige la coopération de la machine FSM du réseau d'accès (AN) ainsi que la confirmation de l'alignement des deux machines FSM et de leur liaison commune.

Cette asymétrie résulte de la responsabilité du commutateur local (CL) pour la prise en charge du service.

15.3.4 Aspects relatifs à la surveillance de la qualité

C'est le réseau d'accès (AN) qui doit effectuer la surveillance de la qualité de la section numérique d'accès au débit primaire lorsque la terminaison NT1 est implémentée séparément du réseau d'accès (AN) (élément FE-U vers l'aval ou bloc CRC-4 erroné détecté dans le réseau d'accès vers l'amont). L'application de ce mécanisme doit être profilée dans le réseau d'accès (AN) et dans le commutateur local (CL) point d'accès par point d'accès.

Comme indiqué en 7.1.1/UIT-T G.964 alinéa 7 [8], le concept de travail est que l'interface V5 ne doit subir aucune influence due à une implémentation du point d'accès utilisateur. Le réseau d'accès est censé surveiller la qualité de la section numérique d'accès. Les paramètres des algorithmes de validation et les seuils spécifiques doivent être prédéfinis dans le réseau d'accès. Seul le dépassement de seuil est signalé, une fois par minute au plus (par l'élément "évaluation de qualité" avec un paramètre indiquant quelle qualité s'applique dorénavant). Le commutateur local (CL) peut utiliser ces comptes rendus pour déterminer si un service demandé doit ou non être fourni. Ce concept rend la surveillance de la qualité à l'interface V5 indépendante de l'accès et sans incidence sur la machine FSM des points d'accès.

Un taux d'erreurs binaires dont la valeur dépasse constamment 10^{-3} est considéré comme une anomalie nécessitant des opérations de maintenance (conformément aux Recommandations de la série M et à l'UIT-T G.921) et donc un blocage immédiat du point d'accès utilisateur.

L'utilisation des éléments FE-W, FE-X et FE-y pour la maintenance utilisateur distante sous contrôle du réseau d'accès est facultative et laissée à l'initiative de l'exploitant. Il n'y a donc pas d'incidence sur l'interface V5.2.

15.4 Protocole de commande

15.4.1 Définition et contenu du message Protocole de commande

Le contenu du présent paragraphe est identique à celui du 14.4.1/G.964 [8].

Tableau 9/G.965 – Codage des éléments de fonction de commande

Bits (octet 3)							Elément de fonction de commande
7	6	5	4	3	2	1	
0	0	0	0	0	0	1	FE101 (activation de l'accès)
0	0	0	0	0	1	0	FE102 (activation à l'initiative de l'utilisateur)
0	0	0	0	0	1	1	FE103 (section numérique activée)
0	0	0	0	1	0	0	FE104 (accès activé)
0	0	0	0	1	0	1	FE105 (désactivation de l'accès)
0	0	0	0	1	1	0	FE106 (accès désactivé)
0	0	1	0	0	0	1	FE201/202 (déblocage)
0	0	1	0	0	1	1	FE203/204 (blocage)
0	0	1	0	1	0	1	FE205 (demande de blocage)
0	0	1	0	1	1	0	FE206 (évaluation de performance)
0	0	1	0	1	1	1	FE207 (blocage du canal D)
0	0	1	1	0	0	0	FE208 (déblocage du canal D)
0	0	1	1	0	0	1	FE209 (équipement terminal hors service)
0	0	1	1	0	1	0	FE210 (anomalie interne au réseau)
NOTE – Toutes les autres valeurs sont réservées.							

15.4.2 Format général du message et codage de l'élément d'information

Le contenu du présent paragraphe est identique à celui du 14.4.2/G.964 [8], à l'exception du Tableau 54/G.964 [8] qui est modifié par l'adjonction de deux éléments de fonction de commande supplémentaires nécessaires pour le point d'accès au débit primaire RNIS, et à l'exception du Tableau 55/G.964 [8] qui est modifié par l'ajout de vingt identificateurs de fonction de commande pour la procédure de verrouillage accéléré. Les Tableaux 9 et 9a montrent respectivement les Tableaux 54 et 55/G.964 [8] modifiés.

Tableau 9a/G.965 – Codage d'identifiants de fonction de commande

Bits (octet 3)							Identifiant de fonction de commande	Elément d'information facultatif considéré comme obligatoire
7	6	5	4	3	2	1		
0	0	0	0	0	0	0	Vérifier le reprofilage	Variante
0	0	0	0	0	0	1	Prêt pour reprofilage	Variante
0	0	0	0	0	1	0	Pas prêt pour reprofilage	Variante, cause de refus
0	0	0	0	0	1	1	Passer à la nouvelle variante	Variante
0	0	0	0	1	0	0	Reprofilage en cours	Variante
0	0	0	0	1	0	1	Reprofilage impossible	Variante, cause de refus
0	0	0	0	1	1	0	Demande d'identification de variante et d'interface	–
0	0	0	0	1	1	1	Identification de variante et d'interface	Variante, identifiant d'interface
0	0	0	1	0	0	0	Blocage en cours	–
0	0	1	0	0	0	0	Redémarrage	–
0	0	1	0	0	0	1	Redémarrage achevé	–
0	0	1	0	0	1	0	DEMANDE DE DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC ET RNIS PERTINENTS	Note 1, Note 2
0	0	1	0	0	1	1	ACCEPTATION DU DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC ET RNIS PERTINENTS	Note 1, Note 2
0	0	1	0	1	0	0	REFUS DE DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC ET RNIS PERTINENTS	Note 1, Note 2
0	0	1	0	1	0	1	DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC ET RNIS PERTINENTS ACHEVE	Note 1, Note 2
0	0	1	0	1	1	0	DEMANDE DE DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC PERTINENTS	–
0	0	1	0	1	1	1	ACCEPTATION DU DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC PERTINENTS	–
0	0	1	1	0	0	0	REFUS DE DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC PERTINENTS	–
0	0	1	1	0	0	1	DEBLOCAGE DE TOUS LES POINTS D'ACCES RTPC PERTINENTS ACHEVE	–
0	0	1	1	0	1	0	DEMANDE DE DEBLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	Note 1
0	0	1	1	0	1	1	ACCEPTATION DU DEBLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	Note 1
0	0	1	1	1	0	0	REFUS DE DEBLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	Note 1
0	0	1	1	1	0	1	DEBLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS ACHEVE	Note 1
0	0	1	1	1	1	0	DEMANDE DE BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	–
0	0	1	1	1	1	1	ACCEPTATION DU BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	–
0	1	0	0	0	0	0	REFUS DE BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	–

Tableau 9a/G.965 – Codage d'identifiants de fonction de commande

Bits (octet 3)							Identifiant de fonction de commande	Elément d'information facultatif considéré comme obligatoire
7	6	5	4	3	2	1		
0	1	0	0	0	0	1	BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS ACHEVE	–
0	1	0	0	0	1	0	DEMANDE DE BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	Note 1
0	1	0	0	0	1	1	ACCEPTATION DU BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	Note 1
0	1	0	0	1	0	0	REFUS DE BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS	Note 1
0	1	0	0	1	0	1	BLOCAGE DE TOUS LES POINTS D'ACCES RNIS PERTINENTS ACHEVE	Note 1
– Toutes les autres valeurs sont réservées.								
NOTE 1 – "Accès RNIS" signifie points d'accès de base RNIS et points d'accès RNIS au débit primaire.								
NOTE 2 – Voir la définition du point d'accès pertinent au 3.1.								

15.4.3 Définition d'état du protocole de commande

Le contenu du présent paragraphe est identique à celui du 14.4.3/G.964 [8]

15.4.4 Procédures du protocole de commande

Le contenu du présent paragraphe est identique à celui du 14.4.4/G.964 [8]

15.4.5 Verrouillage accéléré des entités de protocole et machines FSM relatives au point d'accès

Une autre possibilité est d'aligner les états des points d'accès du réseau d'accès et du commutateur local par les commandes

a) demande de déblocage de tous les points d'accès RTPC et RNIS pertinents (Note 1);

b) demande de déblocage de tous les points d'accès RTPC pertinents;

c) demande de déblocage de tous les points d'accès RNIS pertinents (Note 1);

d) demande de blocage de tous les points d'accès RTPC;

e) demande de blocage de tous les points d'accès RNIS (Note 1);

NOTE 1 – La terminaison RNIS comprend l'accès de base RNIS et l'accès primaire RNIS.

NOTE 2 – Voir la définition du point d'accès pertinent au 3.1.

Ceci peut être accepté ou refusé.

Dans le cas des procédures de verrouillage accéléré de "demande de déblocage de tous les points d'accès pertinents" des a), b) et c):

après acceptation par l'entité homologue, tous les points d'accès pertinents sont amenés à l'état "débloqué" sur les deux côtés, sauf ceux qui sont considérés comme impropres au blocage. Après achèvement, les points d'accès considérés comme impropres au blocage sont réalignés au moyen de la procédure normale de blocage de point d'accès (en utilisant MPH-BI). Voir les détails à l'Annexe C.

Dans le cas des procédures de verrouillage accéléré de "demande de blocage de tous les points d'accès …" de d) et e):

après acceptation par l'entité homologue, tous les points d'accès pertinents sont amenés à l'état "bloqué" sur les deux côtés. Après achèvement, les entités homologues demandeuses peuvent commencer les procédures normales de déblocage de point d'accès (en utilisant MPH-UBR) pour les points d'accès considérés comme impropres au blocage. Voir les détails à l'Annexe C.

L'entité homologue qui a bloqué les points d'accès est responsable du déblocage des points d'accès affectés après la fin de la validité de la cause du blocage. Cependant, les deux côtés sont autorisés à essayer de débloquer les points d'accès.

L'implémentation des procédures de verrouillage accéléré selon a), b), c), d) ou e) est facultative [par exemple, une implémentation peut accepter seulement les procédures b) et d)]. Si l'implémentation n'accepte pas une des procédures de verrouillage accéléré, elle doit envoyer la cause de REJECT correspondante. Si la procédure demandée n'est pas implémentée, le côté qui reçoit la demande doit répondre avec le message REJECT approprié, comme défini au Tableau 9a.

Les procédures DÉBLOQUER TOUS LES ACCÈS RTPC PERTINENTS et DÉBLOQUER TOUS LES ACCÈS RNIS PERTINENTS doivent être utilisées du côté qui demande à la place de la procédure DÉBLOQUER TOUS LES ACCÈS RTPC ET RNIS PERTINENTS.

15.5 Procédures de reprofilage de l'interface V5.2

Le contenu du présent paragraphe est identique à celui du 14.5/G.964 [8].

16 Caractéristiques et protocole de commande de liaison

Le présent paragraphe définit les caractéristiques, les protocoles et les procédures de commande de liaison sous forme de spécifications normatives de machines à états finis (FSM) avec, à l'appui, des descriptions textuelles de ces procédures.

A l'interface V5.2 les fonctions et caractéristiques suivantes doivent être assurées pour chaque liaison à 2048 kbit/s:

a) état de la liaison de couche 1 à 2048 kbit/s et identification de la liaison si nécessaire (voir 16.1);

b) blocage et déblocage coordonné d'une liaison de couche 1 par la gestion-systèmes (voir 16.2);

c) vérification de la continuité de la liaison par identification de la liaison (voir 16.2);

d) coordination de ces fonctions de commande de liaison (voir 16.2);

e) protocole de commande de liaison pour la communication entre réseau d'accès et commutateur local concernant la coordination de ces fonctions des deux côtés (voir 16.3);

Toutes ces caractéristiques sont définies dans le présent paragraphe.

La Figure 11 montre le modèle fonctionnel pour la commande d'une seule liaison d'une interface V5.2. On se reportera à l'Annexe C pour obtenir de plus amples informations sur les caractéristiques de base des fonctions de gestion dans le réseau d'accès et dans le commutateur local.

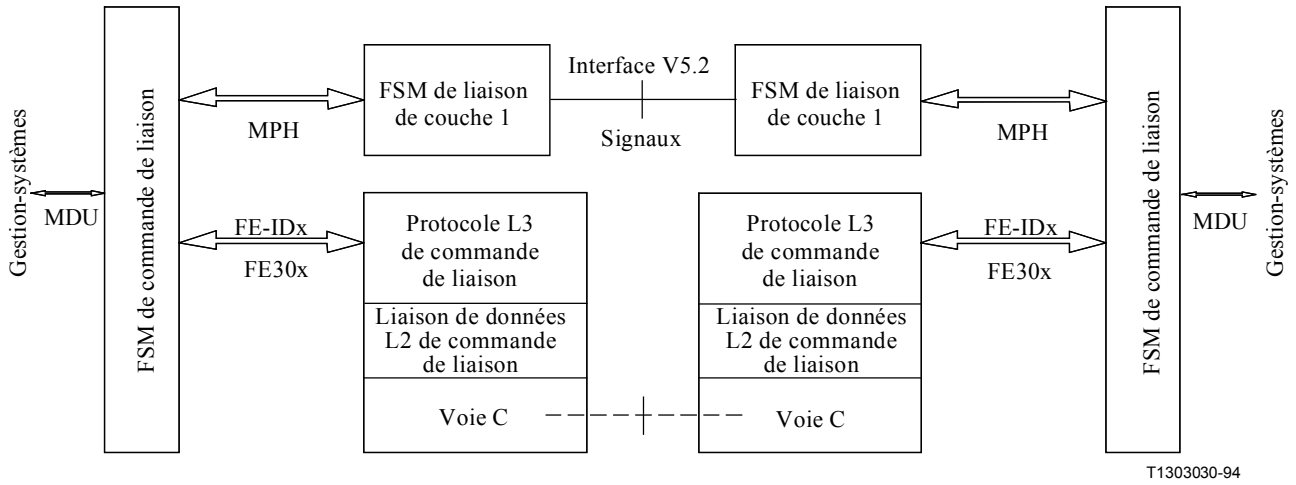


Figure 11/G.965 – Modèle fonctionnel de commande de liaison

Le modèle fonctionnel montre que la machine FSM de liaison de couche 1, qui est directement liée aux signaux d'interface, réagit de manière autonome aux fonctions et procédures de la commande de liaison. Il appartient à la commande de liaison de coordonner la liaison de couche 1 et les procédures de commande de liaison de manière que la gestion-systèmes soit toujours informée de l'état de cette liaison.

Chaque machine à états finis (FSM) de commande de liaison communique avec sa machine FSM de liaison de couche 1 grâce à des primitives de gestion (MPH), alors que la communication avec la gestion-systèmes fait appel aux unités de données de gestion (MDU, *management data unit*). Pour la communication avec la FSM de commande de liaison distante, les éléments de fonction sont transportés par un protocole de couche 3 défini au 16.3. Il existe également des unités MDU qui sont envoyées par l'entité de protocole de commande de liaison à la gestion-systèmes afin de prendre en charge les procédures de traitement des erreurs de protocole.

La FSM de liaison de couche 1 fonctionne de manière autonome sur les signaux de couche 1 et indique l'état de la liaison de couche 1 vers la machine FSM de commande de liaison grâce à des primitives MPH-DI et MPH-AI. L'état de la couche 1 sera détecté de part et d'autre de l'interface de la liaison de couche 1. Du fait que les temporisations prédéfinies d'essai de persistance peuvent avoir des valeurs différentes pour le commutateur local et pour le réseau d'accès, l'indication donnée à la machine FSM de commande de liaison peut se faire à différents moments dans le temps. Les problèmes qui peuvent en découler ont été pris en compte dans la définition de la machine FSM de commande de liaison.

Il appartient à la gestion-systèmes du commutateur local de décider si le fonctionnement de la liaison doit reprendre après correction d'une anomalie de couche 1 (la machine FSM de commande de liaison envoie une primitive MDU-LAI) sans procédure d'identification de liaison ou après réussite de l'identification de la liaison.

16.1 Caractéristiques de maintenance de liaison de couche 1 à 2048 kbit/s

16.1.1 Consignation des événements et des anomalies

Les caractéristiques et les spécifications du présent paragraphe s'appliquent à la fois au réseau d'accès et au commutateur local, à cause de la symétrie des fonctions d'interface.

Les spécifications de la liaison de couche 1 à 2048 kbit/s sont fondées sur les caractéristiques et les procédures de l'interface V5.1 de couche 1. Pour faciliter la compréhension du passage à la version supérieure de V5.1 à V5.2, les parties communes à V5.1 et V5.2 sont indiquées d'abord, puis les parties propres à l'interface V5.2. Dans le Tableau 10, l'ensemble des événements communs est montré d'abord, ceux qui sont propres à l'interface V5.2 étant montrés dans la moitié inférieure du tableau. Dans le Tableau 12, les états propres à l'interface V5.2, indiqués AN/CL5.1 et AN/CL5.2, sont séparés par des lignes doubles.

Le Tableau 10 donne les événements identifiés pour chaque liaison de couche 1 à 2048 kbit/s d'une interface V5.2.

Tableau 10/G.965 – Evénements et primitives de la machine FSM de liaison de couche 1 à l'interface

Evénement (signal)	AN/CL ⇔ Gestion	Primitive
Signal opérationnel (trame normale, pas de RAI)	→	MPH-AI
Situation non opérationnel	→	MPH-DI
Perte du signal	→	MPH-EIa
Perte de l'alignement de trame	→	MPH-Eia
Réception d'une indication d'alarme distante (RAI)	→	MPH-EIb
Réception de signal AIS (Note 1)	→	MPH-EIc
Anomalie interne	→	MPH-EId
Bloc CRC reçu par erreur	→	MPH-EIe
Information d'erreur de CRC (autrement dit, bit E mis à 0) (Note 2)	→	MPH-EIf
Demande d'arrêt avec consignation d'erreur (Note 2)	←	MPH-stop
Demande de progression avec consignation d'erreur (Note 2)	←	MPH-proceed
Indication d'identification de liaison	→	MPH-IDI
Envoi d'un signal d'identification de liaison	←	MPH-ID
Suppression d'un signal d'identification de liaison	←	MPH-NOR
Demande d'identification de liaison	←	MPH-IDR
Anomalie d'identification de liaison	→	MPH-EIg
NOTE 1 – Le signal AIS peut être généré par l'interface V5.2 dans le cas où cette dernière a détecté une anomalie interne l'empêchant de générer le signal de sortie normal. Cependant le côté récepteur de l'interface doit détecter cet événement car le choix d'une application avec une liaison numérique transparente entre signaux d'indication d'alarme (AIS) du commutateur local et du réseau d'accès peut être généré par cette liaison conformément aux Recommandations UIT-T (voir également paragraphe 4). NOTE 2 – Ces événements s'appliquent à l'interface et à la relation avec la gestion-systèmes, mais n'ont aucune influence sur la machine FSM.		

Les machines à états finis du réseau d'accès (interface) et du commutateur local peuvent être considérées comme étant conçues à partir de deux états fondamentaux: l'état opérationnel et l'état non opérationnel. La transition vers ces états est notifiée au réseau d'accès et au commutateur local respectivement par une primitive MPH-AI ou par une primitive MPH-DI à l'interface AN ou LE.

Le mécanisme de consignation disponible du côté éloigné de l'interface est la fonction réception d'une indication d'alarme distante RAI et la fonction de consignation d'erreur de CRC (bit E).

16.1.2 Algorithme de détection pour les événements et les signaux

L'algorithme de détection pour les événements et les signaux est défini au Tableau 11.

Tableau 11/G.965 – Algorithme de détection pour les signaux de couche 1

Trames normales	Les algorithmes sont conformes à ceux donnés au 4.1.2/G.706 [11] et au 4.2/G.706 [11].
Perte de verrouillage de trame	L'algorithme est conforme à celui donné au 4.1.1/G.706 [11].
Indication d'alarme distante	Une indication RAI est détectée lorsque les deux conditions suivantes sont réalisées en même temps: – condition de verrouillage de trames; – réception d'un bit A mis à 1.
Perte de signal	L'équipement implémente l'un des choix suivants, voire les deux, pour détecter la "perte de signal". La détection de cet événement ne doit pas neutraliser le fonctionnement de la procédure de verrouillage de trames. a) L'amplitude du signal entrant est, pendant au moins 1 ms, inférieur de plus de 20 dB à l'amplitude de la sortie nominale définie par l'UIT T G.703 [1]. b) L'entrée détecte plus de 10 ZEROS HDB3 consécutifs.
Signal d'indication d'alarme	Un signal AIS est détecté lorsque les deux conditions suivantes sont satisfaites simultanément: – perte de verrouillage de trames; – réception de périodes de 512 bits contenant moins de 3 ZÉROS binaires (cette condition se fonde sur le paragraphe 3.3.2/O.162.
Information d'erreur de CRC	Réception d'un bit E mis à ZÉRO.
Signal d'identification de liaison	Trames normales reçues dont 2 des 3 bits Sa7 reçus sont mis à ZÉRO.

16.1.3 Machine à états finis de la liaison de couche 1 de l'interface V5.2

La FSM dispose de trois choix d'implémentation pour signaler à la gestion-systèmes les événements détectés et pour prendre les mesures nécessaires pour la fourniture de service:

a) rapport immédiat de l'événement détecté à la gestion pour consignation (MPH-Eie) et traitement pour évaluation de l'état de l'interface en ce qui concerne les opérations ultérieures à effectuer sur le service et les autres machines FSM. Dans ce cas, la gestion effectue l'essai de persistance nécessaire des événements consignés pour identifier si l'état de l'interface est opérationnel ou non;

b) rapport immédiat de l'événement détecté à la gestion pour consignation (MPH-EIe). La couche 1 effectue le test de persistance pour évaluer l'état de l'interface, d'où l'envoi d'un rapport d'état à la gestion (par exemple, envoi d'une primitive MPH-AI, ou MPH-DI au réseau d'accès ou au commutateur local);

c) une combinaison des choix a) et b).

Le Tableau 12 présente la machine FSM de l'interface du réseau d'accès et du commutateur local en adoptant une approche symétrique. Il faut noter que cette FSM permet les trois approches pour l'implémentation de la procédure d'essai de persistance.

La ou les temporisations d'essai de persistance du réseau d'accès et du commutateur local sont prédéfinies par pas de 100 ms, de 100 ms à 25 s. Leur tolérance sera de ±50 ms pour les temporisations nominales de 100 ms à 1 s, et de ±10% au-delà de 1 s.

La machine FSM de liaison de couche 1 ne réalise aucune opération en direction de la FSM de commande de liaison concernant la procédure d'identification de liaison, car elle doit éviter toute erreur d'information en cas d'erreur binaire ou de problème de coordination. Toute opération demandée en direction de la machine FSM est contrôlée par une fonction de commande de la FSM de commande de liaison. Lorsqu'une machine FSM de liaison de couche 1 dans l'état 1, détecte un bit Sa7 à ZERO (après réussite de la procédure d'essai de persistance spécifiée), cette machine passe à l'état 5.2 pour conserver les informations disponibles tant que la procédure d'essai de persistance donne le même résultat. Si la machine FSM de commande de liaison demande des informations d'identification de liaison à l'aide d'une primitive MPH-IDR, la machine FSM de liaison de couche 1 répond par une primitive MPH-IDI, et dans le cas contraire, elle envoie une primitive MPH-EIg, qui indique une anomalie d'identification de liaison. Si la machine FSM de liaison de couche 1 est dans l'un des états non opérationnels 2 à 4, aucune identification de liaison n'est possible, aussi doit-elle répondre par une primitive MPH-DI pour informer la FSM de commande de liaison de cette situation et lui permettre de s'aligner.

Tableau 12/G.965 – FSM de la liaison de couche 1 de l'interface V5.2 – AN (interface) et CL (interface)

Numéro d'état	**AN/CL1**	**AN/CL2**	**AN/CL3**	**AN/CL4**	**AN/CL5.1**	**AN/CL5.2**
Situation	**Normale**	**Anomalie détectée localement**	**Anomalie détectée à distance**	**Anomalie interne**	**Envoi d'identifiant de liaison**	**Réception d'identifiant de liaison**
Signal envoyé côté distant	**Trames normales Sa7 = 1**	**RAI Sa7 = 1**	**Trames normales Sa7 = 1**	**AIS**	**Trames normales Sa7 = 0**	**Trames normales Sa7 = 1**
Trames normales, Sa7 = UN	–	Déclenchement de tempo.; 1	Déclenchement de tempo.; 1	–	–	1
Perte du signal ou perte de verrouillage de trames	Déclenchement de tempo.; MPH-EIa; 2	MPH-EIa; –	MPH-EIa; MPH-EIbr; 2	MPH-EIa; –	Déclenchement de tempo.; MPH-EIa; 2	Déclenchement de tempo.; MPH-EIa; 2
RAI	Déclenchement de tempo.; MPH-EIb; 3	MPH-EIdr; MPH-EIb; 3	–	–	Déclenchement de tempo.; MPH-EIb; 3	Déclenchement de tempo.; MPH-EIb; 3
AIS	Déclenchement de tempo.; MPH-EIc; 2	MPH-EIc; –	MPH-EIc; MPH-EIbr; 2	MPH-EIc; –	Déclenchement de tempo.; MPH-EIc; 2	Déclenchement de tempo.; MPH-EIc; 2
Anomalie interne	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4	–	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4
Disparition d'anomalie interne	/	/	/	MPH-EIdr; 3	/	/
Expiration de la tempori-sation d'essai de persis-tance	MPH-AI; –	MPH-DI; –	MPH-DI; –	–	/	MPH-AI; –
MPH-ID	5.1	MPH-DI; –	MPH-DI; –	MPH-DI; –	–	5.1
MPH-NOR	–	MPH-DI; –	MPH-DI; –	MPH-DI; –	1	/
Trames normales, Sa7 = ZÉRO	5.2	Déclenchement de tempo.; 5.2	Déclenchement de tempo.; 5.2	–	–	–

Tableau 12/G.965 – FSM de la liaison de couche 1 de l'interface V5.2 – AN (interface) et CL (interface)

Numéro d'état	AN/CL1	AN/CL2	AN/CL3	AN/CL4	AN/CL5.1	AN/CL5.2
Situation	**Normale**	**Anomalie détectée localement**	**Anomalie détectée à distance**	**Anomalie interne**	**Envoi d'identifiant de liaison**	**Réception d'identifiant de liaison**
Signal envoyé côté distant	**Trames normales Sa7 = 1**	**RAI Sa7 = 1**	**Trames normales Sa7 = 1**	**AIS**	**Trames normales Sa7 = 0**	**Trames normales Sa7 = 1**
MPH-IDR	MPH-EIg; –	MPH-DI;–	MPH-DI; –	MPH-DI; –	/	MPH-IDI

– Un tiret indique qu'il n'y a pas de transition d'état.

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état.

MPH-EI sert à indiquer une erreur (le paramètre r correspond à une reprise sur une situation d'erreur précédemment signalée).

NOTE 1 – Il n'est pas toujours possible d'émettre un signal d'indication d'alarme (AIS) dans toutes les situations d'anomalie interne.

NOTE 2 – Le temporisateur d'essai de persistance est lancé dès réception de l'événement approprié, comme indiqué par "déclenchement de temporisateur". Si, à cause de la réception d'un autre événement, un autre temporisateur est lancé, tout temporisateur lancé en parallèle doit être arrêté et relancé.

Les valeurs des temporisateurs, qui peuvent dépendre de chaque événement, sont prédéfinies. Pour le réseau d'accès, ces valeurs sont:

– supérieures à celles du commutateur local pour la transition à l'état non opérationnel;

– inférieures à celles du commutateur local pour la transition à l'état opérationnel.

Lorsque la machine FSM de liaison de couche 1 reçoit une primitive MPH-ID alors qu'elle se trouve dans l'état AN/CL1 ou AN/CL5.2, elle passe à l'état AN/CL5.1 et met à ZÉRO le bit Sa7 dans le train binaire d'envoi. Lorsqu'elle est dans l'état AN/CL5.1, à la réception d'une primitive MPH-NOR, la machine FSM retourne à l'état AN/CL1 (c'est-à-dire que le bit Sa7 est mis à un). Elle retourne à l'état approprié lorsqu'une situation d'anomalie est détectée et envoie le signal en fonction de la situation de l'interface de liaison de couche 1.

16.1.4 Spécifications des fonctions supplémentaires et procédures associées

Le verrouillage de multitrames de CRC-4 doit être effectué dans les états AN/CL1, AN/CL3 et AN/CL5.x et les blocs de CRC erronés détectés doivent être signalés à l'extrémité distante en mettant le bit E à ZÉRO ainsi qu'à la gestion-systèmes à l'aide d'une primitive MPH-EIe. La gestion-systèmes doit traiter l'information d'erreur de CRC selon des seuils prédéfinis et peut réagir en direction du système d'exploitation. Ceci sort du cadre de la machine à états finis de l'interface. Un taux d'erreur constamment supérieur à 10^{-3} est considéré comme non opérationnel.

Les informations d'erreur de CRC-4 peuvent être reçues dans les états AN/CL1, AN/CL3 AN/CL4 et AN/CL5.x. Les bits E mis à ZÉRO qui peuvent être reçus dans l'état AN/CL1 doivent être signalés à la gestion-systèmes au moyen d'une primitive MPH-EIf. La gestion peut traiter les informations d'erreur de CRC selon des seuils prédéfinis et peut réagir en direction du système d'exploitation. Ceci sort du domaine d'application de l'interface FSM. Un taux d'erreur constamment supérieur à 10^{-3} est considéré comme non opérationnel.

Si l'interface FSM reçoit la primitive MPH-Stop en provenance de la gestion-systèmes, la machine FSM continue de fonctionner mais n'envoie pas de primitive MPH-EI à la gestion.

Sur réception de la primitive MPH-Proceed, elle envoie l'état actuel (dernière primitive MPH-EI générée en direction de la gestion-systèmes ainsi que tout message ultérieur).

16.2 Caractéristiques et procédures de commande de liaison

16.2.1 Blocage et déblocage des liaisons

Il existe deux types distincts de demande de blocage émise par le réseau d'accès vers le commutateur local: la demande de blocage différée et la demande de blocage non différée.

Le réseau d'accès peut demander un blocage non différé d'une liaison, mais le commutateur local, en tant que maître du service, prend la décision. Si la liaison transporte une ou plusieurs voies C actives, la gestion-systèmes du commutateur local utilise le protocole de protection pour commuter la ou les voies C logiques sur des voies C physiques en attente. Ensuite, le commutateur local libère toutes les connexions commutées sur cette liaison, selon les besoins du service, mais rétablit les connexions semi-permanentes ou réservées au réseau d'accès sur d'autres liaisons de la même interface V5.2 et envoie alors une primitive "d'indication de blocage" vers le réseau d'accès. S'il s'avère cependant impossible de protéger les voies C logiques, le commutateur rejette la demande en envoyant une primitive "d'indication de déblocage" au réseau d'accès.

Le réseau d'accès peut aussi demander un blocage différé d'une liaison. Dans ce cas, le commutateur local doit empêcher toute affectation ultérieure de canal support non affecté de cette liaison et attendre que tous les canaux supports (affectés aux services à la demande) deviennent non affectés. Après cela, le commutateur local doit continuer la protection des voies C logiques et des connexions semi-permanentes ou réservées au réseau d'accès, si nécessaire, et envoyer une primitive "d'indication de blocage" au réseau d'accès. Cependant, si la protection des voies C logiques n'est pas possible, le commutateur local doit rejeter la demande en envoyant une primitive "d'indication de blocage" au réseau d'accès.

Si la demande de blocage non différée a été rejetée par le commutateur local et que le blocage de liaison est nécessaire et urgent du point de vue du réseau d'accès, ce dernier peut bloquer une seule liaison de l'interface V5.2 immédiatement. Il faut noter que ce blocage forcé d'une seule liaison par le réseau d'accès peut faire basculer toute l'interface V5.2 dans l'état non opérationnel, si la liaison primaire ou secondaire est affectée.

Dans le cas d'anomalies internes du réseau d'accès provoquant l'indisponibilité de la liaison, le réseau d'accès peut appliquer le blocage immédiat de la liaison. En parallèle, la protection de toutes les voies C affectées doit être entreprise si elle est disponible.

L'indication d'état de liaison d'une seule liaison d'une interface V5.2 repose sur un partage défini des responsabilités entre réseau d'accès et commutateur local.

Les essais qui interfèrent avec un service quelconque via cette liaison ne doivent être réalisés que lorsque la liaison est dans l'un des états non opérationnels, soit en raison d'une anomalie, soit sur demande faite au commutateur local et avec sa permission. Ceci implique l'existence de deux états principaux, s'appliquant au protocole de l'interface V5.2, des deux côtés:

– l'état opérationnel;
– l'état non opérationnel.

16.2.2 Identification de liaison

Cette procédure est utilisée pour vérifier l'identification d'une liaison donnée. Si l'extrémité opposée peut accepter cette demande (en particulier, si elle n'effectue pas déjà une procédure semblable au même moment), elle envoie un signal physique spécifique (bit Sa7 de TS 0 mis à zéro, alors qu'autrement il est à un) sur la liaison en indiquant l'adresse dans le message. Ceci permet à l'extrémité demandeuse de vérifier qu'il n'y a pas de mauvaise mise en correspondance entre les extrémités de cette ligne.

La procédure est symétrique et peut s'appliquer à partir de l'une ou l'autre extrémité de la liaison à 2048 kbit/s. En cas de collision de demandes du réseau d'accès et du commutateur local, l'identification de liaison lancée par le commutateur local a priorité sur la procédure lancée par le réseau d'accès.

Lorsque la machine FSM d'interface L1 indique à la machine FSM de commande de liaison, au moyen d'une primitive MPH-AI, qu'elle est passée à l'état normal, la gestion-systèmes peut demander qu'une procédure d'identification de liaison soit effectuée. Cette procédure s'applique à toutes les liaisons, liaisons primaire et secondaire comprises.

NOTE – La procédure d'identification de liaison peut également être effectuée par la gestion-systèmes sur une base temporisée. L'identification de liaison peut être appliquée après reprofilage. Au démarrage du système, la gestion-systèmes ou le système d'exploitation peuvent décider de ne pas appliquer la procédure d'identification de liaison.

Le principe de la procédure d'identification de liaison est indiquée par la Figure 12.

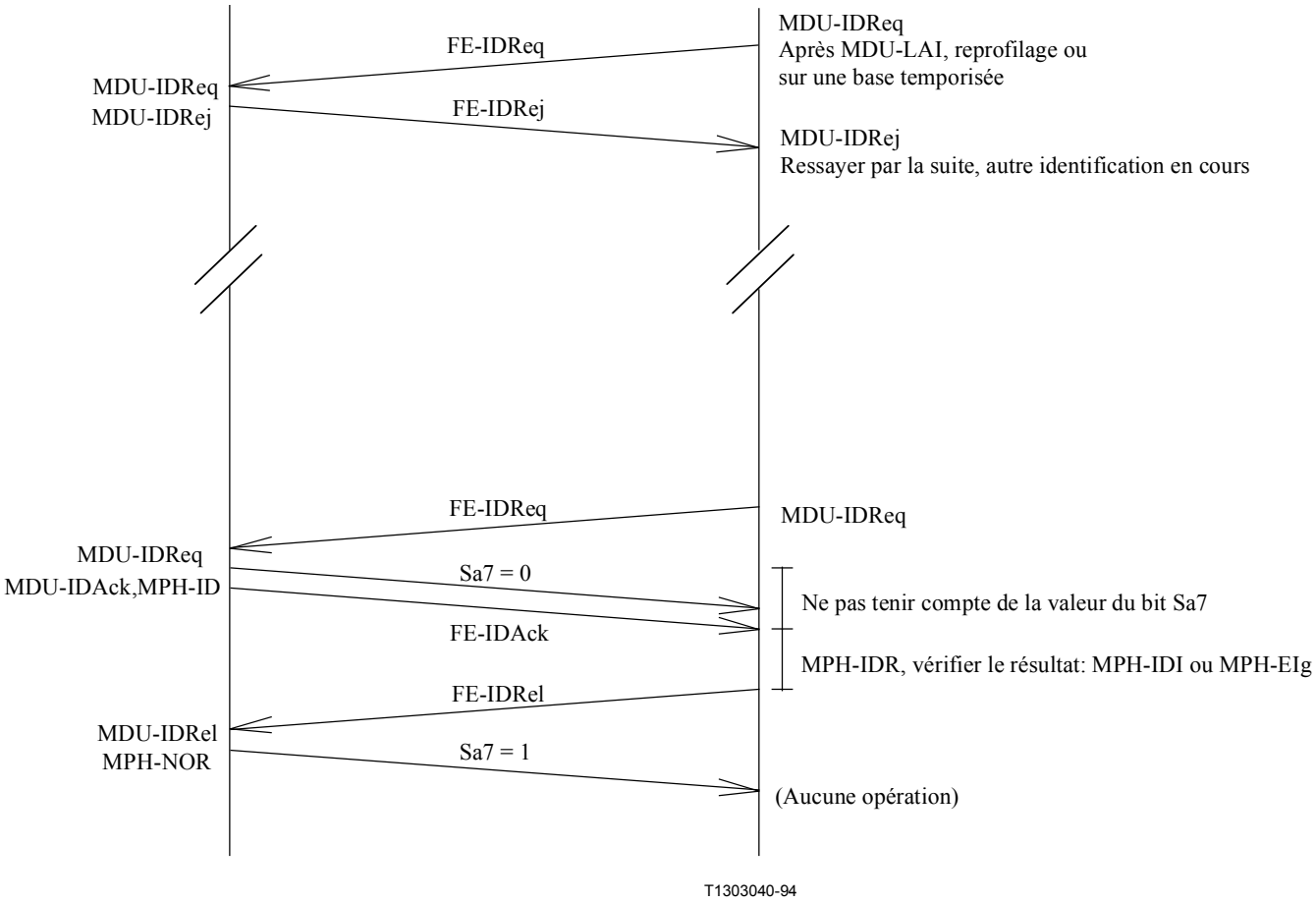


Figure 12/G.965 – Procédure fonctionnelle d'identification de liaison, diagramme fléché

16.2.3 Evénements et éléments de fonction s'appliquant à la commande des machines FSM associés aux liaisons

Les Tableaux 13, 14 et 15 donnent l'ensemble des éléments de fonction et des primitives de gestion s'appliquant aux procédures de commande de liaison de l'interface V5.2 et à la gestion, ainsi qu'aux primitives d'unités de données de gestion vers la FSM de la liaison de couche 1 et la fonction de gestion-systèmes du réseau d'accès ou du commutateur local.

Tableau 13/G.965 – Ensemble des éléments de fonction de commande de liaison

Elément de fonction	Nom	AN ⇔ CL	Description
FE-IDReq	Identification de liaison	↔	Demande
FE-IDAck	Identification de liaison	↔	Accusé de réception
FE-IDRel	Identification de liaison	↔	Demande de libération
FE-IDRej	Identification de liaison	↔	Indication de rejet
FE301	Déblocage de liaison	←	Demande ou indication
FE302	Déblocage de liaison	→	Demande ou indication
FE303	Blocage de liaison	←	Indication
FE304	Blocage de liaison	→	Indication
FE305	Blocage de liaison	→	Demande, différée
FE306	Blocage de liaison	→	Demande, non différée

Tableau 14/G.965 – Ensemble des primitives et des unités de données pour la commande de liaison dans le commutateur local

Primitive	FSM L1 ⇔ Commande de liaison	Commande de liaison ⇔ Gestion-systèmes	Description
MPH-AI	→		La liaison de couche 1 est opérationnelle
MDU-AI		→	La liaison est opérationnelle
MPH-DI	→		La liaison de couche 1 n'est pas opérationnelle
MDU-DI		→	La liaison n'est pas opérationnelle
MDU-LAI		→	Identification de liaison nécessaire
MDU-IDReq		↔	Demande d'identification de liaison
MDU-IDAck		←	Envoi d'accusé de réception d'identification de liaison
MPH-ID	←		Envoi d'identification de liaison
MPH-IDR	←		Envoi d'informations d'identification de liaison

Tableau 14/G.965 – Ensemble des primitives et des unités de données pour la commande de liaison dans le commutateur local

Primitive	FSM L1 ⇔ Commande de liaison	Commande de liaison ⇔ Gestion-systèmes	Description
MPH-IDI	→		Indication d'identification de liaison
MPH-NOR	←		Suppression d'identification de liaison
MDU-IDRel		→	Indication de libération d'identification de liaison
MDU-IDRej		↔	Demande identification de liaison rejetée
MPH-EIg	→		Anomalie d'identification de liaison
MDU-EIg		→	Indication d'anomalie d'identification de liaison
MPH-EIa-f	→		Indications d'erreur de couche 1
MDU-LUBR		↔	Demande de déblocage de liaison
MDU-LUBI			Indication de déblocage de liaison
MDU-LBI		→	Indication de blocage de liaison
MDU-LBR		↔	Demande de blocage de liaison, différée
MDU-LBRN		→	Demande de blocage de liaison, non différée

16.2.4 Machines FSM de commande de liaison, de réseau d'accès (liaison) et commutateur local (liaison)

Les primitives, unités de données, éléments de fonction et tables d'états sont donnés pour définir le comportement et la coopération fonctionnelle entre les divers blocs fonctionnels. Aucune limite n'est imposée à l'implémentation de ces fonctions, du moment que l'implémentation est conforme à la fonctionnalité définie dans la présente Recommandation au niveau de l'interface V5.2, de la machine FSM de liaison de couche 1 et de la gestion-systèmes.

16.2.4.1 Description des états

Les machines FSM de commande de liaison du réseau d'accès et du commutateur local peuvent chacune être considérées comme étant conçues à partir de deux états fondamentaux: l'état opérationnel et l'état non opérationnel.

L'état non opérationnel se subdivise en 5 sous-états:

– anomalie de liaison de couche 1 (0.1);
– anomalie de liaison de couche 1 et liaison bloquée (0.2);
– liaison bloquée (1.0);
– liaison locale débloquée (1.1);
– liaison distante débloquée (1.2).

Tableau 15/G.965 – Ensemble des primitives et des unités de données pour la commande de liaison dans le réseau d'accès

Primitive	FSM L1⇔ Commande de liaison	Commande de liaison ⇔ Gestion-systèmes	Description
MPH-AI	→		La liaison de couche 1 est opérationnelle
MDU-AI		→	La liaison est opérationnelle
MPH-DI	→		La liaison de couche 1 n'est pas opérationnelle
MDU-DI		→	La liaison n'est pas opérationnelle
MDU-LAI		→	Identification de liaison nécessaire
MDU-IDReq		↔	Identification de liaison demandée
MDU-IDAck		←	Envoi d'accusé de réception d'identification de liaison
MPH-ID	←		Envoi d'identification de liaison
MPH-IDR	←		Envoi d'informations d'identification de liaison
MPH-IDI	→		Indication d'identification de liaison
MPH-NOR	←		Suppression d'identification de liaison
MDU-IDRel		→	Indication de libération d'identification de liaison
MDU-IDRej		↔	Demande d'identification de liaison rejetée
MPH-EIg	→		Anomalie d'identification de liaison
MDU-EIg		→	Indication d'anomalie d'identification de liaison
MPH-EIa-f	→		Indications d'erreur de couche 1
MDU-LUBR		↔	Demande de déblocage de liaison
MDU-LUBI		→	Indication de déblocage de liaison
MDU-LBI		↔	Indication de blocage de liaison
MDU-LBR		←	Demande de blocage de liaison, différée
MDU-LBRN		←	Demande de blocage de liaison, non différée

Cette subdivision simplifie la coordination des deux machines FSM de commande de liaison dans la séquence de déblocage et garantit que le déblocage sera acquitté des deux côtés avant le passage à l'état opérationnel.

Les unités de données MDU-LUBI et MDU-LBI sont utilisées par les deux machines FSM de commande de liaison pour signaler à leur gestion la transition respectivement vers l'état opérationnel et hors de cet état.

Le mécanisme de déblocage de liaison est acquitté, comme l'est le mécanisme de demande de blocage de liaison côté réseau d'accès. Le mécanisme de blocage immédiat n'est pas acquitté.

L'état opérationnel se subdivise en trois sous-états:

– liaison opérationnelle (2.0);

– identification de liaison à distance (2.1);

– identification de liaison locale (2.2).

Les trois états sont considérés comme opérationnels du point de vue de la commande de liaison. Il appartient à la gestion-systèmes appropriée de lancer toute opération ultérieure requise selon l'état de liaison de la gestion-systèmes, par exemple, selon la gestion du protocole de protection et la gestion des ressources de canal support.

16.2.4.2 Définition des états de commande de liaison et des caractéristiques générales de coordination

Les machines FSM de commande de liaison reflètent uniquement le point de vue du réseau d'accès et du commutateur local sur l'état fonctionnel d'une liaison simple de l'interface V5.2.

Afin de coordonner les situations d'anomalie de liaison de couche 1 et de liaison bloquée, le sous-état 0.2 a été inséré pour couvrir la situation état combiné de la liaison. Si, durant l'anomalie de liaison de couche 1, la gestion-systèmes demande un blocage, l'entité distante en est avertie et passe au sous-état 0.2. Lorsque la liaison de couche 1 est rétablie, la machine FSM de commande de liaison passe à l'état bloqué en envoyant l'unité de donnée MBU-LBI pour inciter la gestion-systèmes à coordonner le déblocage si souhaité. Cette procédure permet aussi le rétablissement coordonné après un mauvais alignement de gestion-systèmes, par exemple, perte de la liaison de données de commande en raison d'une anomalie de liaison de couche 1 ou perte des données de l'état de la gestion-systèmes après le redémarrage.

Une demande de déblocage de liaison issue de l'un ou l'autre côté, pendant la situation d'anomalie de liaison 1 est considérée comme un mauvais alignement de gestion-systèmes et la machine FSM de commande de liaison passe au sous-état 0.2 pour déclencher le déblocage coordonné après rétablissement de la liaison de couche 1. La même opération est recommandée lorsqu'une primitive FE-IDReq est reçue alors que la machine FSM est en situation d'anomalie de liaison de couche 1.

16.2.4.2.1 Machine FSM de commande de liaison – Réseau d'accès (AN_Link)

Liaison non opérationnelle (AN0.x et AN1.x): la liaison est forcée à l'état anomalie de la liaison de couche 1 ou liaison bloquée. Aussi, les voies C physiques de cette liaison ne sont pas utilisées pour transporter de voie C logique ou pour fonctionner comme voie en attente. Aucun intervalle de temps associé à cette liaison n'est disponible comme canal support pour la commande d'appel. Une demande d'identification de liaison est rejetée.

Anomalie de liaison (AN0.1): la FSM de liaison de couche 1 indique une perte persistante de capacité de couche 1 à l'aide d'une primitive MPH-DI.

Anomalie de liaison et liaison bloquée (AN0.2): la machine FSM de liaison de couche 1 indique à l'aide d'une primitive MPH-DI une perte persistante de capacité de couche 1 alors que la liaison est bloquée, ou à la suite d'opérations demandées à la gestion-systèmes ou au côté commutateur local qui peuvent être considérées comme un mauvais alignement des machines FSM de commande de liaison nécessitant une coordination.

Liaison bloquée (AN1.0): la liaison est dans l'état non opérationnel et ni l'un ni l'autre côté n'a déclenché de déblocage.

Déblocage de liaison locale (AN1.1): le réseau d'accès a déclenché le déblocage (en envoyant l'élément FE302) et attend confirmation du commutateur local.

Déblocage de liaison distante (AN1.2): le commutateur local a déclenché le déblocage (en envoyant l'élément FE301) et attend confirmation du réseau d'accès.

NOTE – Les états AN1.1 et AN1.2 fournissent un mécanisme de déblocage synchronisé des liaisons. Le réseau d'accès peut rester dans ces états pendant une durée indéterminée.

Liaison opérationnelle (AN2.0): la liaison est considérée comme étant prête du point de vue de la couche 1 et de la commande de liaison pour assurer les capacités reprofilables. Il peut être nécessaire d'effectuer la procédure d'identification de liaison pour vérifier la continuité de la liaison.

Identification de liaison distante (AN2.1): le commutateur local a déclenché l'identification de la liaison et, sur confirmation de la gestion-systèmes, la FSM de liaison de couche 1 a reçu la demande de mise à 0 du bit d'identification de liaison Sa7. La commande de liaison du réseau d'accès attend l'élément de fonction libération d'identification de liaison.

Identification de liaison locale (AN2.2): le réseau d'accès a déclenché l'identification de la liaison et attend la primitive FE-IDAck en provenance du commutateur local, ou, s'il l'a déjà reçue, l'indication d'identification de liaison ou d'échec d'identification de liaison, en réponse à la primitive MPH-IDR. Suite à ces opérations, les informations appropriées sont envoyées à la gestion-systèmes et l'identification de liaison est libérée.

16.2.4.2.2 Machine FSM de commande de liaison – Commutateur local (LE_Link)

Liaison non opérationnelle (CL0.x et CL1.x): la liaison est forcée à l'état anomalie de liaison de couche 1 ou liaison bloquée. Aussi, les voies C physiques de cette liaison ne doivent pas être utilisées pour transporter de voie C logique ou pour fonctionner comme voie en attente. Aucun intervalle de temps de cette liaison n'est disponible comme canal support pour la commande d'appel. Une demande d'identification de liaison sera rejetée.

Anomalie de liaison (CL0.1): la FSM de la liaison de couche 1 indique une perte persistante de capacité de couche 1 à l'aide d'une primitive MPH-DI.

Anomalie de liaison et liaison bloquée (CL0.2): la machine FSM de liaison de couche 1 indique à l'aide d'une primitive MPH-DI une perte persistante de capacité de couche 1 alors que la liaison est bloquée à la suite d'opérations demandées à la gestion-systèmes ou au côté réseau d'accès qui peuvent être considérées comme un mauvais alignement des machines FSM de commande de liaison nécessitant une coordination.

Liaison bloquée (CL1.0): la liaison est dans l'état non opérationnel et ni l'un ni l'autre côté n'a déclenché de déblocage.

Déblocage de liaison locale (CL1.1): le réseau d'accès a déclenché le déblocage (en envoyant l'élément FE301) et attend confirmation du commutateur local.

Déblocage de liaison distante (CL1.2): le réseau d'accès a déclenché le déblocage (en envoyant l'élément FE302) et attend confirmation du commutateur local.

NOTE – Les états CL1.1 et CL1.2 fournissent un mécanisme de déblocage synchronisé des liaisons. Le commutateur local peut rester dans ces états pendant une durée indéterminée.

Liaison opérationnelle (CL2.0): la liaison est considérée comme étant prête du point de vue de la couche 1 et de la commande de liaison pour assurer les capacités reprofilées. Il peut être nécessaire d'effectuer la procédure d'identification de liaison pour vérifier la continuité de la liaison.

Identification de liaison distante (CL2.1): le réseau d'accès a déclenché l'identification de la liaison et, sur confirmation de la gestion-systèmes, la machine FSM de liaison de couche 1 a reçu la demande de mise à 0 du bit d'identification de liaison Sa7. La commande de liaison du commutateur local attend l'élément de fonction libération d'identification de liaison.

Identification de liaison locale (CL2.2): la gestion-systèmes du commutateur local a déclenché l'identification de liaison et attend la primitive FE-IDAck en provenance du réseau d'accès ou, s'il l'a déjà reçue, l'indication d'identification de liaison ou d'échec d'identification de liaison, en réponse à la primitive MPG-IDR. Ensuite, les informations utiles sont envoyées à la gestion-systèmes et l'identification de liaison est libérée.

16.2.4.3 Principes et procédures

16.2.4.3.1 Généralités

Le réseau d'accès peut demander le blocage d'une liaison spécifique: demande de blocage (différée ou non, avec dans les deux cas l'élément d'information identification de liaison). Le commutateur local doit accéder à cette demande (dès qu'il est en mesure de le faire) et envoie une indication de blocage (avec l'élément d'information Identification de liaison). Le réseau d'accès peut demander également le déblocage d'une liaison spécifique (bloquée): demande de déblocage (avec l'élément d'information Identification de liaison). Le commutateur local envoie une indication de déblocage (avec l'élément d'information Identification de liaison) ou une indication de blocage (avec l'élément d'information Identification de liaison). La procédure est symétrique et de ce fait, elle est aussi valable pour le commutateur local.

Si la demande de blocage non différée ne réussit pas mais qu'elle est nécessaire et urgente, le réseau d'accès peut bloquer une seule liaison de l'interface V5.2 immédiatement. Le blocage immédiat d'une seule liaison forcée par le réseau d'accès peut faire passer toute l'interface V5.2 à un état non opérationnel.

Dans le cas d'anomalies internes du réseau d'accès provoquant l'indisponibilité de la liaison, le réseau d'accès peut appliquer le blocage immédiat de la liaison. En parallèle, la protection de toutes les voies C affectées doit être entreprise si elle est disponible.

Tous les messages transportant un élément de fonction de commande de liaison d'une liaison spécifique doivent contenir l'élément d'information Identification de liaison.

Les paragraphes suivants décrivent les mécanismes implémentés par les machines FSM du réseau d'accès et du commutateur local pour les liaisons simples d'une interface V5.2, présentés dans les tables de transition d'état correspondantes.

La procédure s'appliquera même dans le cas d'une interface V5.2 à une seule liaison à 2048 kbit/s.

Les mécanismes suivants sont décrits:

– blocage de liaison;
– demande de blocage de liaison en provenance du réseau d'accès (différée ou non);
– déblocage coordonné;
– procédure d'identification de liaison.

16.2.4.3.2 Blocage d'une liaison

Une liaison simple d'une interface V5.2 peut être bloquée de part et d'autre. Le commutateur local libère toute connexion commutée sur cette liaison, de manière appropriée au service, mais rétablit les connexions semi-permanentes et les connexions préconnectées sur d'autres liaisons de la même interface V5.2. La gestion du commutateur local utilise le protocole de protection pour déplacer les voies C, si nécessaire et dans la mesure du possible.

Lorsque la gestion du commutateur local envoie l'unité de données MDU-LBI, la machine FSM envoie l'élément de fonction FE303 (indication de blocage de liaison) au réseau d'accès et passe à l'état liaison bloquée CL1.0.

Lorsque la gestion du réseau d'accès envoie l'unité de données MDU-LBI, la machine FSM envoie l'élément de fonction FE304 (indication de blocage de liaison) au commutateur local et passe à l'état liaison bloquée AN1.0.

16.2.4.3.3 Demande de blocage de liaison

Le réseau d'accès peut demander le blocage d'une liaison donnée: demande différée ou non de blocage de liaison. Le commutateur local accède à cette demande (dès qu'il est en mesure de le faire et après avoir terminé toutes les opérations que cela implique) et envoie une primitive d'indication de blocage de liaison.

Lorsque la gestion-systèmes AN envoie une unité de données MDU-LBR ou MDU-LBRN et que la liaison est dans l'état opérationnel, la machine FSM de liaison du réseau d'accès envoie l'élément de fonction FE305 ou FE306, comme approprié. Cette demande doit être transmise par la machine FSM de commande de liaison du commutateur local à la gestion-systèmes du commutateur local à l'aide d'une unité de données MDU-LBR ou MDU-LBRN.

16.2.4.3.4 Déblocage coordonné d'une liaison

Le déblocage d'une liaison simple d'une interface V5.2 doit être coordonné des deux côtés de l'interface. Une demande de déblocage de liaison nécessite confirmation du côté opposé avant que la liaison puisse être exploitée. Pour assurer cette coordination, il existe deux états distincts de déblocage de liaison (déblocage de liaison locale et déblocage de liaison distante) dans chacune des deux machines FSM. Cette procédure est entièrement symétrique entre réseau d'accès et commutateur local.

Si la gestion-systèmes du commutateur local veut débloquer la liaison, elle envoie une primitive MDU-LUBR, la machine FSM de commande de liaison envoie l'élément FE301 (demande de déblocage) et passe à l'état "blocage de liaison locale" (CL1.1). Sur réception de l'élément FE301, le réseau d'accès passe à "déblocage de liaison distante" (AN1.2) et envoie MDU-LUBR à sa gestion-systèmes. Si la gestion-systèmes du réseau d'accès l'accepte, elle répond par une primitive d'indication MDU-LUBR (demande de déblocage de liaison), la machine FSM de commande de liaison du réseau d'accès envoie un élément FE302 au commutateur local, envoie une primitive MDU-LUBI (demande de déblocage d'indication) à la gestion-systèmes et passe à l'état "liaison opérationnelle" (AN2.0). Lorsque la machine FSM de commande de liaison CL est dans l'état "déblocage de liaison locale" et reçoit cet élément FE302, elle passe à l'état "liaison opérationnelle" (CL2.0) et envoie une primitive MDU-LUBI à sa gestion-systèmes.

La gestion-systèmes du réseau d'accès peut aussi prendre l'initiative, auquel cas la même procédure s'applique. Si la gestion-systèmes n'est pas d'accord, elle doit répondre avec une primitive MDU-LBI.

La gestion-systèmes doit exécuter une séquence blocage/déblocage de liaison s'il ne reçoit pas une primitive MPH-LBI ou MPH-LUBI (indication de déblocage de liaison) dans les cinq minutes.

La gestion-systèmes du commutateur local doit envoyer à nouveau la primitive MDU-LUBR si elle ne reçoit pas une primitive MPH-LBI ou MPH-LUBI dans les cinq minutes. Ceci est nécessaire pour résoudre une mauvaise correspondance d'état de liaison qui, par exemple, pourrait survenir si une liaison est ajoutée aux données de profilage du commutateur local d'une interface opérationnelle après que le réseau d'accès a déjà essayé de débloquer cette liaison (elle reste à l'état AN1.1, liaison locale débloquée).

Lorsque les machines FSM de commande de liaison AN et CL sont dans l'état "déblocage de liaison distante" et reçoivent respectivement un élément de fonction FE304 ou FE303, l'état est remis à "liaison bloquée" et une primitive MDU-LBI est envoyée à la gestion-systèmes. Cette opération annule une demande de blocage de liaison antérieure émise par le côté opposé.

La collision d'éléments FE301/2 et FE303/4 pourrait entraîner une mauvaise coordination de déblocage par la suite. La gestion-systèmes peut détecter le problème en identifiant la séquence des primitives. Il est recommandé, dans ce cas, que la gestion-systèmes applique la procédure de vérification après déblocage pour assurer la coordination des deux côtés de l'interface. Un déblocage non coordonné peut entraîner des rejets dans la procédure d'affectation BCC ou dans la procédure de commutation de protection et l'utilisation inefficace des ressources à l'interface.

16.2.4.3.5 Identification de liaison

L'identification de liaison peut être nécessaire après correction d'une anomalie de liaison de couche 1, indiquée à la gestion-systèmes par une primitive MDU-LAI issue de la machine FSM de liaison de couche 1 et indiquée à la gestion-systèmes par une primitive MDU-LAI. Il appartient à la gestion-systèmes de déclencher ou non la procédure d'identification de liaison. Il peut exister d'autres causes de déclenchement dans la gestion-systèmes pour appeler cette procédure. Il ne doit exister, à un instant donné, qu'une seule demande de procédure d'identification de liaison de la part de la gestion-systèmes, pour toutes les interfaces V5 du réseau d'accès et du commutateur local. Il doit cependant être possible d'accomplir simultanément l'identification de liaison du réseau d'accès au commutateur local et du commutateur local au réseau d'accès, pour autant qu'aucune collision ne survient sur une liaison, comme décrit ci-dessous.

Si la liaison primaire ou la liaison secondaire a été affectée par une anomalie de couche 1, la gestion-systèmes peut ne pas invoquer cette procédure si la liaison de données de commande de liaison n'est pas (déjà) dans l'état opérationnel indiqué par la primitive d'indication MDL-establish ou de confirmation MDL-establish. L'établissement de la liaison de commande de liaison a toujours la priorité, car la procédure d'identification de liaison repose sur le fonctionnement correct de la liaison de données de commande de liaison.

Pour éviter les situations de blocage interne, les cas de collision d'identifications de liaison demandées de part et d'autre au même instant sont résolus en donnant toujours la priorité à la demande du commutateur local; cette dernière demande annule la demande du réseau d'accès à moins que le commutateur local n'en ait déjà accusé réception. La description suivante de la procédure est symétrique, sauf la résolution de collision, aussi n'est-elle décrite que pour un seul côté.

Le déclenchement d'identification de liaison à l'aide d'une primitive MDU-IDReq ne peut réussir que si la machine FSM de commande de liaison est dans l'état 2.0. Dans tous les autres cas, la gestion-systèmes répond par un rejet direct ou indirect en donnant les informations d'état de la commande de liaison. A la réception de la primitive MDU-IDReq, la machine FSM envoie une primitive FE-IDReq du côté distant, passe à l'état 2.2 et attend l'accusé de réception de la demande, donné par une primitive FE-IDAck. A la réception de cette primitive FE-IDAck, il est implicitement compris que la machine FSM de commande de liaison distante a demandé à la machine FSM de liaison de couche 1 concernée de mettre à ZÉRO le bit Sa7 (au moyen d'une primitive MPH-ID) qui est alors détecté par la machine FSM de liaison de couche 1 locale. Cette information n'est pas transmise directement à la machine FSM de commande de liaison, afin d'éviter le recouvrement des demandes d'identification de liaison.

Le côté distant recevant la primitive FE-IDReq lorsqu'il est dans l'état 2.0 informe la gestion-systèmes à l'aide d'une primitive MDU-IDReq. Si la gestion-systèmes peut accéder à cette demande, elle répond par une primitive MDU-IDAck, la FSM de commande de liaison envoie une primitive FE-IDAck et passe à l'état 2.1.

A la réception de la primitive FE-IDAck, la machine FSM de commande de liaison demande les informations d'identification de liaison en envoyant une primitive MPH-IDR à la machine FSM de liaison de couche 1 qui renvoie ensuite au moyen d'une primitive MPH-IDI ou MPH-EIg les informations appropriées qui figurent à cet instant dans la machine FSM de liaison de couche 1. La machine FSM de commande de liaison informe la gestion-systèmes par l'unité de données MDU appropriée qui est soit MDU-AI, indication de réussite d'identification de liaison, soit, si la machine FSM de liaison de couche 1 est en situation d'anomalie à cet instant, MDU-EIg ou MDU-DI, indications d'échec d'identification de liaison. Quelle que soit la réponse faite à la gestion-systèmes, la machine FSM de commande de liaison demande la libération de l'identification de liaison côté distant et passe à l'état 2.0. Cette opération est effectuée à l'aide d'une primitive FE-IDRel, qui provoque la remise à UN du bit Sa7 (par une primitive MPH-NOR de la machine FSM de commande de liaison distante à la machine FSM de liaison de couche 1).

Si la gestion-systèmes distante ne peut pas satisfaire à la demande d'identification de liaison elle envoie une primitive MDU-IDRej à la machine FSM de commande de liaison, qui doit rejeter la demande à l'aide d'une primitive FE-IDRej. Ceci appelle d'autres informations de la machine FSM de commande de liaison locale vers la gestion-systèmes par l'intermédiaire de primitives MDU-IDRej.

Il appartient à la gestion-systèmes d'effectuer les actions appropriées à la réception de toute information envoyée à la machine FSM de commande de liaison, c'est-à-dire à la réception de primitives MDU-IDRej, MDU-IDRel, MDU-AI, MDU-Elg, MDU-DI, suite à une procédure d'identification de liaison que la gestion-systèmes a demandée à la machine FSM de commande de liaison.

16.2.4.4 Machine FSM de commande de liaison au réseau d'accès

Le Tableau 16 décrit la machine FSM de commande de liaison du réseau d'accès.

La machine FSM de commande de liaison du réseau d'accès fournit à la gestion-systèmes du réseau d'accès un moyen de vérifier que la machine FSM de commande de liaison est dans l'état liaison opérationnelle, sans avoir à effectuer la séquence de blocage et déblocage. Ce mécanisme est interne au réseau d'accès: la gestion-systèmes envoie pour ce faire une primitive MDU-LUBR et reçoit les informations indiquant si la machine FSM de commande de liaison est dans un état non opérationnel.

16.2.4.5 Machine FSM de commande de liaison au commutateur local

Le Tableau 17 décrit la machine FSM de commande de liaison du commutateur local.

La machine FSM de commande de liaison de commutateur local fournit un mécanisme qui permet à la gestion-systèmes CL de vérifier que la machine FSM de commande de liaison est dans l'état liaison opérationnelle en envoyant une primitive MDU-LUBR sans avoir à passer par la séquence de blocage et de déblocage.

Au contraire de la situation correspondante dans le cas réseau d'accès, ce mécanisme n'est pas interne au commutateur local car il demande la coopération de la machine FSM de commande de liaison du réseau d'accès et confirme l'alignement des deux machines FSM de commande de liaison lorsqu'elles reçoivent la primitive MDU-LUBI.

L'asymétrie reflète ici que la prise en charge du service est de la responsabilité du commutateur local.

16.3 Protocole de commande de liaison

16.3.1 Définition et contenu des messages du protocole de commande de liaison

Le format des messages du protocole de commande de liaison correspond à la structure générique de message définie au paragraphe 13.

L'ensemble complet des messages du protocole de commande de liaison est indiqué au Tableau 18. Les paragraphes suivants donnent la structure détaillée pour chacun des messages.

16.3.1.1 Message LINK CONTROL (commande de liaison)

Ce message est envoyé par le réseau d'accès ou par le commutateur local pour acheminer les informations nécessaires aux fonctions de commande de chaque liaison à 2048 kbit/s (voir le Tableau 19).

Tableau 16/G.965 – Machine FSM de commande de liaison du réseau d'accès

Etat	AN0.1	AN0.2	AN1.0	AN1.1	AN1.2	AN2.0	AN2.1	AN2.2
Nom de l'état / Evénement	Anomalie de liaison	Anomalie de liaison et blocage	Liaison bloquée	Déblocage de liaison locale	Déblocage de liaison distante	Liaison opération-nelle	Identifi-cation de liaison distante	Identifi-cation de liaison locale
MPH-AI	MDU-LAI; 2.0	MDU-LAI; MDU-LBI; 1.0	MDU-LAI; –	–	–	–	–	–
MPH-DI	–	–	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.1	MDU-DI; MPH-NOR; 0.1	MDU-DI; FE-IDRel; 0.1
MDU-IDReq	MDU-DI; –	MDU-DI; –	MDU-LBI; –	MDU-LBI; 1.0	MDU-LUBR; MDU-IDRej: –	FE-IDReq; 2.2	MDU-IDRej; –	–
FE-IDAck	/	/	/	/	/	/	/	MPH-IDR; –
MPH-IDI	/	/	/	/	/	/	/	MDU-AI; FE-IDRel; 2.0
MPH-Eig	/	/	/	/	/	/	/	FE-IDRel; MDU-EIg; 2.0
FE-IDReq	FE304; 0.2	FE304; –	FE304; –	FE-IDRej; –	FE-IDRej; –	MDU-IDReq; –	–	MDU-IDRej; MDU-IDReq; 2.0
MDU-IDAck	/	/	/	/	/	MPH-ID; FE-IDAck; 2.1	–	/
FE-IDRel	–	/	/	–	/	/	MDU-IDRel; MPH-NOR; 2.0	/
MDU-IDRej	/	/	/	/	/	FE-IDRej; –	FE-IDRej; MPH-NOR; 2.0	/
FE-IDRej	–	/	/	–	/	/	MDU-IDRej; –	MDU-IDRej; 2.0
FE301	FE304; 0.2	FE304; –	MDU-LUBR; 1.2	MDU-LUBI; 2.0	MDU-LUBR; –	FE302; MDU-LUBI; –	FE302; MDU-LUBI; MDU-IDRel; MPU-NOR; 2.0	FE302; MDU-IDRej; 2.0
FE303	0.2	–	–	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; MPH-NOR; 1.0	MDU-LBI; 1.0

Tableau 16/G.965 – Machine FSM de commande de liaison du réseau d'accès

Etat	AN0.1	AN0.2	AN1.0	AN1.1	AN1.2	AN2.0	AN2.1	AN2.2
Nom de l'état / Evénement	Anomalie de liaison	Anomalie de liaison et blocage	Liaison bloquée	Déblocage de liaison locale	Déblocage de liaison distante	Liaison opération-nelle	Identifi-cation de liaison distante	Identifi-cation de liaison locale
MDU-LUBR	FE304; MDU-DI; 0.2	FE304; MDU-DI; –	FE302; 1.1	FE302; –	FE302; MDU-LUBI; 2.0	FE302; MDU-LUBI; –	FE-IDRej; MDU-LUBI; MPH-NOR; 2.0	FE-IDRel; MDU-LUBI; 2.0
MDU-LBI	FE304; 0.2	FE304; –	FE304; –	FE304; 1.0	FE304; 1.0	FE304; 1.0	FE304; MPH-NOR; 1.0	FE304; 1.0
MDU-LBR	FE304; MDU-LBI; 0.2	FE304; MDU-LBI; –	FE304; MDU-LBI; –	FE304; MDU-LBI; 1.0	FE304; MDU-LBI; 1.0	FE305; –	FE305; –	FE305; –
MDU-LBRN	FE304; MDU-LBI; 0.2	FE304; MDU-LBI; –	FE304; MDU-LBI; –	FE304; MDU-LBI; 1.0	FE304; MDU-LBI; 1.0	FE306; –	FE306; –	FE306; –

– Un tiret indique l'absence de transition d'état.

/ Une barre oblique indique une événement intempestif qui ne provoque pas de transition d'état.

NOTE 1 – La primitive MPH-EIa-f doit être consignée mais le rapport de ces événements depuis la FSM interface de couche 1 peut être supprimé à l'aide d'une primitive MPH-EIstop et traité à l'aide d'une primitive MPH-EIproceed.

NOTE 2 – Le premier ensemble d'événements (MPH-AI/DI) indique la disponibilité de la couche 1.

NOTE 3 – Le deuxième ensemble (MDU-IREQ... CL-IDrej) est utilisé pour la procédure d'identification de liaison.

NOTE 4 – Le troisième ensemble est utilisé pour la procédure de blocage de liaison.

Tableau 17/G.965 – Machine FSM de commande de liaison du commutateur local

Etat	CL0.1	CL0.2	CL1.0	CL1.1	CL1.2	CL2.0	CL2.1	CL2.2
Nom de l'état / Evénement	Anomalie de liaison	Anomalie de liaison et blocage	Liaison bloquée	Déblocage de liaison locale	Déblocage de liaison distante	Liaison opération-nelle	Identifi-cation de liaison distante	Identifi-cation de liaison locale
MPH-AI	MDU-LAI; 2.0	MDU-LAI; MDU-LBI; 1.0	MDU-LAI; –	–	–	–	–	–
MPH-DI	–	–	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.1	MDU-DI; MPH-NOR; 0.1	MDU-DI; FE-IDRel; 0.1
MDU-IDReq	MDU-DI; –	MDU-DI; –	MDU-LBI; –	MDU.LBI; 1.0	MDU-LUBR; MDU-IDRej; –	FE-IDReq; 2.2	MDU-IDRej; –	–
FE-IDAck	/	/	/	/	/	/	/	MPH-IDR; –
MPH-IDI	/	/	/	/	/	/	/	MDU-AI; FE-IDRel; 2.0
MPH-EIg	/	/	/	/	/	/	/	FE-IDRel; MDU-EIg; 2.0
FE-IDReq	FE303; 0.2	FE303; –	FE303; –	FE-IDRej; –	FE-IDRej; –	MDU-IDReq; –	_	FE-IDRej; –

Tableau 17/G.965 – Machine FSM de commande de liaison du commutateur local

Etat	CL0.1	CL0.2	CL1.0	CL1.1	CL1.2	CL2.0	CL2.1	CL2.2
Nom de l'état / Evénement	**Anomalie de liaison**	**Anomalie de liaison et blocage**	**Liaison bloquée**	**Déblocage de liaison locale**	**Déblocage de liaison distante**	**Liaison opération-nelle**	**Identifi-cation de liaison distante**	**Identifi-cation de liaison locale**
MDU-IDAck	/	/	/	/	/	MPH-ID; FE-IDAck; 2.1	–	/
FE-IDRel	–	/	–	–	/	/	MDU-IDRel; MPH-NOR; 2.0	/
MDU-IDRej	/	/	/	/	/	FE-IDRej; –	FE-IDRej; MPH-NOR; 2.0	/
FE-IDRej	–	/	–	–	/	/	/	MDU-IDRej; 2.0
MDU-LUBR (Note 5)	MDU-DI; FE303; 0.2	MDU-DI; FE303; –	FE301; 1.1	FE301; –	FE301; MDU-LUBI; 2.0	FE301; –	FE301; MPH-NOR; 2.0	FE301; 2.0
MDU-LBI	FE303; 0.2	FE303; –	FE303; –	FE303; 1.0	FE303; 1.0	FE303; 1.0	FE303; MPH-NOR; 1.0	FE303; 1.0
FE302 (Note 5)	FE303; 0.2	FE303; –	MDU-LUBR; 1.2	MDU-LUBI; 2.0	MDU-LUBR; –	MDU-LUBI; –	MDU-IDRel; MDU-LUBI; MPH-NOR; 2.0	MDU-IDRej; MDU-LUBI; 2.0
FE304 (Note 5)	0.2	–	–	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; MPH-NOR; 1.0	MDU-LBI; 1.0
FE305	FE303; 0.2	FE303; –	FE303; –	FE303; MDU-LBI; 1.0	FE303; MDU-LBI; 1.0	MDU-LBR; –	MDU-LBR; –	MDU-LBR; –
FE306	FE303; 0.2	FE303; –	FE303; –	FE303; MDU-LBI; 1.0	FE303; MDU-LBI; 1.0	MDU-LBRN; –	MDU-LBRN; –	MDU-LBRN; –

– Un tiret indique l'absence de transition d'état.

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état.

NOTE 1 – La primitive MPH-EIa-f doit être consignée mais le rapport de ces événements depuis la FSM interface de couche 1 peut être supprimé à l'aide d'une primitive MPH-ELstop et traité à l'aide d'une primitive MPH-EIproceed.

NOTE 2 – Le premier ensemble d'événements (MPH-AI) indique la disponibilité de la couche 1.

NOTE 3 – Le deuxième ensemble (MDU-IDreq-FE-IDrej) est utilisé pour la procédure d'identification de liaison.

NOTE 4 – Le troisième ensemble est utilisé pour la procédure de blocage de liaison.

NOTE 5 – Notification à la gestion-systèmes au sujet d'une faute de couche 1. Notification envoyée à la gestion-systèmes au sujet d'une faute de couche 1 dans l'état CL0.1.

Tableau 18/G.965 – Messages du protocole de commande de liaison d'interface V5.2

Codage dans l'élément d'information type de message							Types de message	Référence
7	6	5	4	3	2	1		
0	1	1	0	0	0	0	LINK CONTROL	16.3.1.1
0	1	1	0	0	0	1	LINK CONTROL ACK	16.3.1.2

Tableau 19/G.965 – Contenu du message LINK CONTROL

Type de message: LINK CONTROL

Sens: les deux

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	Les deux	M	1
Adresse de couche 3	16.3.2.1	Les deux	M	2
Type de message	13.2.3	Les deux	M	1
Fonction de commande de liaison	16.3.2.2	Les deux	M	3

16.3.1.2 Message LINK CONTROL ACK (accusé de réception de commande de liaison)

Ce message est envoyé par le réseau d'accès ou par le commutateur local comme accusé de réception immédiat de la réception d'un message LINK CONTROL (voir Tableau 20).

Tableau 20/G.965 – Contenu du message LINK CONTROL ACK

Type de message: LINK CONTROL ACK

Sens: les deux

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	Les deux	M	1
Adresse de couche 3	16.3.2.1	Les deux	M	2
Type de message	13.2.3	Les deux	M	1
Fonction de commande de liaison	16.3.2.2	Les deux	M	3

16.3.2 Définition, structure et codage de l'élément d'information Protocole de commande de liaison

Les éléments d'information Protocole de commande de liaison sont définis dans les sous-paragraphes suivants et résumés dans le Tableau 21, qui donne aussi le codage des bits de l'identifiant d'élément d'information. Pour chaque élément d'information le codage des différents champs est indiqué.

Tableau 21/G.965 – Codage de l'identifiant d'élément d'information

Bits								Elément d'information	Référence
8	7	6	5	4	3	2	1		
0	–	–	–	–	–	–	–	Longueur variable	
0	0	1	1	0	0	0	0	Fonction de commande de liaison	16.3.2.2

16.3.2.1 Elément d'information Adresse de couche 3

L'objet de l'élément d'information Adresse de couche 3 est d'identifier la liaison à 2048 kbit/s à laquelle fait référence le message de commande de liaison.

L'élément d'information Adresse L3 forme la deuxième partie de chaque message et il est codé comme le montre la Figure 13.

8	7	6	5	4	3	2	1	Octets
0	0	0	0	0	0	0	0	1
Champ d'adresse L3 (partie inférieure)								2

Figure 13/G.965 – Elément d'information Adresse de couche 3 pour identification de liaison à 2048 kbit/s

L'élément d'information Adresse de couche 3 est codé en binaire.

Pour une liaison donnée à 2048 kbit/s d'interface V5, le champ d'adresse L3 (partie inférieure) de l'élément d'information Adresse L3 prend la même valeur que le champ d'identifiant de la liaison à 2048 kbit/s d'interface V5 de l'élément d'information Identification d'intervalle de temps V5 qui est utilisé pour le protocole BCC.

16.3.2.2 Elément d'information Fonction de commande de liaison

Cet élément d'information identifie la fonction de commande de liaison que doit transporter le message.

La structure de l'élément d'information Fonction de commande de liaison est indiquée par la Figure 14.

8	7	6	5	4	3	2	1	Octets
0	0	1	1	0	0	0	0	1
Longueur du contenu de la fonction de commande de liaison								2
ext. 1	Fonction de commande de liaison							3

Figure 14/G.965 – Elément d'information Fonction de commande de liaison

Le codage du contenu de cet élément d'information est spécifié par le Tableau 22.

Tableau 22/G.965 – Codage de l'élément d'information Fonction de commande de liaison

Bits (octet 3)							Fonction de commande de liaison
7	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	FE-IDReq
0	0	0	0	0	0	1	FE-IDAck
0	0	0	0	0	1	0	FE-IDRel
0	0	0	0	0	1	1	FE-IDRej
0	0	0	0	1	0	0	FE301/302 (déblocage de liaison)
0	0	0	0	1	0	1	FE303/304 (blocage de liaison)
0	0	0	0	1	1	0	FE305 (demande différée de blocage de liaison)
0	0	0	0	1	1	1	FE306 (demande non différée de blocage de liaison)
NOTE – Toutes les autres valeurs sont réservées.							

16.3.3 Définition des états du protocole de commande de liaison

OUT OF SERVICE (hors service)

On passe à cet état lors du démarrage du système ou lorsqu'une primitive MDU-stop_traffic est reçue de la gestion-systèmes.

IN SERVICE (en service)

On passe à cet état lorsque l'entité de protocole de commande est dans l'état OUT OF SERVICE et reçoit une primitive MDU-start_traffic de la gestion-systèmes.

AWAIT LINK CONTROL ACK (attente d'accusé de réception de commande de liaison)

On passe à cet état lorsqu'un message LINK CONTROL (commande de liaison) a été envoyé à la sous-couche LINK CONTROL-DL.

16.3.4 Procédures associées au protocole de commande de liaison

16.3.4.1 Généralités

Le présent paragraphe spécifie les procédures associées au protocole de commande de liaison. Ce protocole est symétrique, c'est-à-dire que les procédures s'appliquent à la fois côté réseau d'accès et côté commutateur local de l'interface V5.2.

Une entité de protocole de commande de liaison propre à la liaison existe pour chaque liaison de couche 1 à 2048 kbit/s.

Outre les procédures précédentes, chaque message reçu par une entité de protocole de commande de liaison doit subir avec succès les procédures de traitement d'erreur spécifiées au 16.3.5 avant tout traitement ultérieur.

La procédure est décrite pour un événement unique (FE ou MDU-CTRL), dans le seul but d'être traité au même instant. Il faut disposer d'une mémoire pour chaque entité de protocole de commande de liaison du réseau d'accès et du commutateur local, afin d'enregistrer les événements à retransmettre par la suite dans l'ordre où ils ont été reçus de la machine FSM. L'événement suivant est transmis lorsque la machine FSM de protocole de commande de liaison pertinente passe à l'état 1.

Chaque message de protocole de commande de liaison contient une adresse de couche 3 pour identifier l'entité de protocole de commande de liaison de couche 1.

Les messages de protocole de commande de liaison sont envoyés à la liaison de données à l'aide d'une primitive de demande DL-Data; le service liaison de données est spécifié au paragraphe 10.

16.3.4.2 Indication de début du trafic

16.3.4.2.1 Fonctionnement normal

Si une entité de protocole de couche 3 de commande de liaison, dans l'état OUT OF SERVICE, reçoit de l'entité de gestion-systèmes une primitive MDU-start_traffic, elle passe à l'état IN SERVICE.

16.3.4.2.2 Procédures exceptionnelles

Si une entité de protocole de couche 3 de commande de liaison, dans l'état OUT OF SERVICE, reçoit un message LINK CONTROL ou un élément de fonction FE, une primitive d'indication MDU-error est générée. Il ne se produit pas de transition d'état.

16.3.4.3 Indication d'arrêt de trafic

16.3.4.3.1 Fonctionnement normal

Si une entité de protocole de couche 3 de commande de liaison, dans l'état IN SERVICE ou dans l'état AWAIT LINK CONTROL ACK, reçoit de l'entité de gestion-systèmes une primitive MDU-stop_traffic, elle passe à l'état OUT OF SERVICE.

16.3.4.3.2 Procédures exceptionnelles

Néant.

16.3.4.4 Procédure d'entité de protocole de couche 3 de commande de liaison

Si l'entité de protocole de couche 3 de commande de liaison, dans l'état "en service", reçoit un message LINK CONTROL, un message LINK CONTROL ACK et une primitive FE contenant la fonction de commande de liaison ainsi que l'adresse L3 sont envoyés à l'entité de gestion-systèmes.

Lorsque l'entité de protocole de couche 3 de commande de liaison est dans l'état "en service" et reçoit de l'entité de gestion de commande de liaison une primitive FE, elle envoie un message LINK CONTROL contenant la fonction de commande de liaison et l'adresse L3, lance la temporisation LCT01 et passe à l'état "attente d'accusé de réception de commande de liaison".

Si l'entité de protocole de couche 3 de commande de liaison, dans l'état "attente d'accusé de réception de commande de liaison", reçoit un message LINK CONTROL, un message LINK CONTROL ACK et une primitive FE contenant la fonction de commande de liaison et l'adresse de couche 3 sont envoyés à l'entité de gestion de commande de liaison.

A réception d'un message LINK CONTROL ACK dans l'état "attente d'accusé de réception de commande de liaison", le temporisateur LCT01 doit être arrêté et on doit passer à l'état "en service".

Si une primitive FE est reçue de l'entité de gestion de commande de liaison dans l'état "attente d'accusé de réception de commande de liaison", elle met la primitive FE en mémoire.

Si le temporisateur LCT01 arrive à expiration pour la première fois dans l'état "attente d'accusé de réception de commande de liaison", le message LINK CONTROL est retransmis et le temporisateur LCT01 est relancé. Si le temporisateur LCT01 arrive à expiration pour la seconde fois dans l'état "attente d'accusé de réception de commande de liaison", une primitive d'indication d'erreur MDU-link_control est envoyée à l'entité de gestion-systèmes et l'entité de protocole passe à l'état "en service".

16.3.5 Traitement des conditions d'erreur

Avant de donner suite à un message, l'entité réceptrice, qui est l'entité de protocole de commande de liaison d'interface V5 implantée dans le réseau d'accès (AN) ou dans le commutateur local (CL), doit appliquer les procédures spécifiées dans le présent paragraphe.

En règle générale, tous les messages doivent contenir, au moins, les éléments d'information suivants: Discriminateur de protocoles, Adresse de couche 3 et Type de message. Ces éléments d'information, qui font office d'en-tête pour tous les messages du protocole de commande de liaison, sont spécifiés au 13.2. Lorsque l'entité de protocole du réseau AN ou du commutateur CL reçoit un message comportant moins de 4 octets, elle envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

Chaque réception d'un message du protocole de commande de liaison active les essais décrits aux 16.3.5.1 à 16.3.5.7 par ordre de préséance. Aucune transition d'état n'a lieu pendant ces tests.

Les procédures de traitement d'erreur dans le réseau d'accès et le commutateur local sont symétriques.

Si le message a été testé à l'aide des procédures de traitement d'erreur qui suivent et s'il ne doit pas être ignoré, les procédures de protocole de commande de liaison (voir 16.3.4) doivent alors être exécutées.

NOTE – Dans le présent paragraphe, le terme "ignorer le message" signifie ne pas modifier son contenu.

16.3.5.1 Erreur de discriminateur de protocole

Lorsqu'une entité de protocole de commande de liaison d'interface V5 reçoit un message dont le discriminateur de protocole est codé autrement qu'il est spécifié au 13.2.1, l'entité de protocole de commande de liaison d'interface V5 envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

16.3.5.2 Erreur d'adresse de couche 3

Si l'adresse de couche 3:

a) n'est pas codée comme spécifié au 16.3.2.1;

b) a une valeur non reconnue ou ne correspondant à aucune liaison V5 à 2048 kbit/s existante, alors:

- l'entité de protocole de commande de liaison d'interface V5 envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

16.3.5.3 Erreur de type de message

Chaque fois qu'elle reçoit un message non reconnu, l'entité de protocole de commande de liaison d'interface V5 envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

16.3.5.4 Répétition d'éléments d'information

Si un élément d'information obligatoire est répété dans un message, l'entité de protocole de commande de liaison d'interface V5 qui le reçoit, envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

16.3.5.5 Absence d'un élément d'information obligatoire

Lorsque, dans un message reçu, il manque un élément d'information obligatoire, l'entité de protocole de commande de liaison d'interface V5 qui le reçoit, envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

16.3.5.6 Elément d'information non reconnu

Lorsqu'elle reçoit un message contenant un ou plusieurs éléments d'information non reconnus, l'entité de protocole de commande de liaison d'interface V5 élimine tous les éléments d'information non reconnus et poursuit le traitement du message; elle envoie également à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control.

Pour les procédures de traitement d'erreur, les éléments d'information non reconnus sont ceux qui ne sont pas définis dans la présente Recommandation.

16.3.5.7 Erreur de contenu d'élément d'information obligatoire

Si l'entité reçoit un message contenant un élément d'information obligatoire dont le contenu est erroné:

a) car la longueur n'est pas conforme au 16.3.1;

b) car le contenu n'est pas connu, alors:

- l'entité de protocole de commande de liaison d'interface V5 envoie à la gestion-systèmes une primitive d'indication d'erreur de protocole MDU-link_control et ignore le message.

NOTE – Pour les procédures de traitement des erreurs, les erreurs de contenu d'élément d'information sont des points de codes inclus dans un élément d'information donné, qui ne sont pas définis dans la présente Recommandation.

16.3.6 Temporisateurs pour le protocole de commande de liaison

Les temporisateurs pour le protocole de commande de liaison du réseau d'accès et du commutateur local sont spécifiés dans le Tableau 23. Les tolérances sur les temporisations sont de ±10%.

Tableau 23/G.965 – Temporisateurs associés au protocole de commande de liaison

Numéro de temporisateur	Durée d'expiration	Etat	Cause d'activation	Arrêt normal
LCT01	1 s	AN1 (liaison CTRL) CL1 (liaison CTRL)	Message LINK CONTROL envoyé	Message LINK CONTROL ACK reçu

16.3.7 Tableaux d'état des entités de protocole de couche 3 côté réseau d'accès et côté commutateur local

Le Tableau 24 définit la table des transitions d'état de l'entité de protocole de couche 3 de commande de liaison côté réseau d'accès de l'interface V5.2.

Le Tableau 25 définit la table des transitions d'état de l'entité de protocole de couche 3 de commande de liaison côté commutateur local de l'interface V5.2.

17 Eléments de protocole et procédures de connexion de canal support (BCC)

17.1 Généralités

Le protocole BCC d'interface V5.2 donne au commutateur local le moyen de demander au réseau d'accès l'établissement ou la libération des connexions entre des points d'accès utilisateur spécifiés et des intervalles de temps d'interface V5.2 spécifiés. Il permet aux canaux supports d'interface V5.2 d'être affectés et désaffectés grâce à des processus indépendants (appel par appel, ligne préconnectée ou ligne semi-permanente). Plusieurs processus peuvent être actifs à tout moment pour un point d'accès utilisateur donné.

Tableau 24/G.965 – Tableau des transitions d'état de l'entité de protocole L3 de commande de liaison – Réseau d'accès

Etat / Evénement	AN0 hors service	AN1 en service	AN2 attente d'accusé de réception de commande de liaison
MDU-start_traffic	AN1	–	–
MDU-stop_traffic	–	Arrêter LCT01; AN0	Arrêter LCT01; AN0
FE ou FE mémorisée	Envoyer MDU-link_control (indication d'erreur); –	Envoyer LINK CONTROL; lancer LCT01; AN2	Mémoriser les nouveaux FE reçus; –
LINK CONTROL	Envoyer MDU-link_control (indication d'erreur); –	Envoyer FE; envoyer LINK CONTROL ACK; –	Envoyer FE; Envoyer LINK CONTROL ACK; –
LINK CONTROL ACK	Envoyer MDU-link_control (indication d'erreur); –	/	Arrêter LCT01; AN1
Première expiration LCT01	/	/	Répéter LINK CONTROL; lancer LCT01; –
Seconde expiration LCT01	/	/	Envoyer MDU-link_control (indication d'erreur); AN1

Les majuscules indiquent qu'un message ou un événement est externe

Les minuscules indiquent qu'un message ou un événement est interne

– Un tiret indique l'absence de transition d'état;

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état.

Tableau 25/G.965 – Tableau des transitions d'état de l'entité de protocole L3 de commande de liaison – Commutateur local

Etat / Evénement	CL0 hors service	CL1 en service	CL2 attente d'accusé de réception de commande de liaison
MDU-start_traffic	CL1	–	–
MDU-stop_traffic	–	Arrêter LCT01; CL0	Arrêter LCT01; CL0
FE ou FE mémorisée	Envoyer MDU-link_control (indication d'erreur); –	Envoyer LINK CONTROL; Lancer LCT01; CL2	Mémoriser le nouvel FE reçu; –
LINK CONTROL	Envoyer MDU-link_control (indication d'erreur); –	Envoyer FE; Envoyer LINK CONTROL ACK; –	Envoyer FE; Envoyer LINK CONTROL ACK; –
LINK CONTROL ACK	Envoyer MDU-link_control (indication d'erreur); –	/	Arrêter LCT01; LE1
Première expiration LCT01	/	/	Répéter LINK CONTROL; Lancer LCT01; –
Seconde expiration LCT01	/	/	Envoyer MDU-link_control (indication d'erreur); CL1

Les majuscules indiquent qu'un message ou un événement est externe

Les minuscules indiquent qu'un message ou un événement est interne

– Un tiret indique l'absence de transition d'état;

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état.

Les processus suivants ont été définis pour être pris en charge par le protocole BCC:

Processus d'affectation

Procédure utilisée par le protocole BCC, qui définit les interactions entre réseau d'accès et commutateur local, afin d'affecter un nombre défini de canaux supports à un point d'accès particulier à l'interface V5.2. Le processus a une durée de vie finie et se termine:

a) lorsque le protocole BCC rapporte à la gestion des ressources CL que la gestion des ressources AN lui a donné confirmation que les canaux proposés ont été affectés;

b) lorsque l'affectation n'a pas réussi.

Dans le second cas, toutes les informations appropriées sont renvoyées au gestionnaire des ressources du commutateur local.

Processus de désaffectation

Procédure utilisée par le protocole BCC, qui définit les interactions entre réseau d'accès et commutateur local, afin de désaffecter un nombre défini de canaux supports d'un point d'accès particulier à l'interface V5.2. Le processus a une durée de vie finie et se termine:

a) lorsque le protocole BCC rapporte à la gestion des ressources CL que la gestion de ressources AN lui a donné confirmation que les canaux proposés ont été désaffectés;

b) lorsque la désaffectation n'a pas réussi.

Dans le second cas, toutes les informations appropriées sont renvoyées à la gestion des ressources du commutateur local.

Processus d'analyse

Procédure utilisée par le protocole BCC, qui définit les interactions entre réseau d'accès et commutateur local, afin de vérifier le routage d'un canal support à l'interface V5.2 puis sa connexion à un point d'accès utilisateur. On ne peut pas supposer que tout routage entre les deux est entièrement vérifié (en règle générale). On considère le processus terminé lorsque la réponse à la procédure d'audit est envoyée à la gestion des ressources.

Pour identifier un processus, un numéro de référence BCC lui est affecté.

Les interfaces V5.2 ont la capacité de prendre en charge les trois types suivants de connexion support:

a) les connexions commutées appel par appel dans le commutateur local et à l'interface V5.2, qui permettent d'assurer les services commutés du RTPC et du RNIS avec concentration du trafic dans le réseau d'accès;

b) les connexions commutées appel par appel dans le commutateur local mais préconnectées à l'interface V5.2 et dans le réseau d'accès, qui permettent d'assurer les services commutés du RTPC et du RNIS (sans concentration du trafic dans le réseau d'accès), pour les lignes à fort trafic (par exemple les lignes d'autocommutateurs privés) et les situations dans lesquelles le blocage d'appel dans le réseau d'accès ou à l'interface V5 n'est pas acceptable (par exemple, lignes de service d'urgence);

c) les connexions semi-permanentes dans le commutateur local et dans le réseau d'accès, qui permettent d'assurer les services de lignes louées semi-permanentes (sans voies C logique ou physique de signalisation associée).

Pour les connexions de type a), la procédure BCC est appliquée au début et à la fin de chaque appel sous contrôle de la commande d'appel RTPC ou RNIS du commutateur local.

Pour les connexions de type b) et c), la procédure BCC est appliquée sous contrôle de la gestion-systèmes CL (c'est-à-dire de l'interface Q_{CL}), selon les besoins de profilage ou de cessation de service de ligne commutée ou louée. La gestion du commutateur local ne spécifie pas d'intervalle de temps d'interface V5 ni de liaison à 2048 kbit/s particulière mais elle est informée de l'intervalle de temps et de la liaison sélectionnée.

Pour les connexions de type b) et de type c), la gestion CL spécifie le point d'accès utilisateur et l'intervalle de temps du point d'accès.

Les interfaces V5.2 ont la capacité d'établir et de libérer des connexions à intervalles multiples à n × 64 kbit/s où n est compris entre 1 et 30, pour assurer les services H0, H12 et les futurs services multidébits. De telles connexions peuvent être de type a), b) ou c).

Les types de voies du système de signalisation DSS1 ne sont pas visibles à l'interface V5 mais sont traitées de manière transparente comme des connexions à n × 64 kbit/s. Les appels multimédias ne sont pas visibles à l'interface V5 mais sont traités de manière transparente comme plusieurs connexions indépendantes.

Seules les connexions entre les points d'accès utilisateur du réseau d'accès et l'interface V5.2 sont assurées par le protocole BCC. La commutation interne (c'est-à-dire la connexion entre points d'accès utilisateur) n'est pas assurée par le protocole. Ceci n'empêche pas la commutation interne sous contrôle entier du réseau d'accès, par exemple lorsqu'un réseau d'accès est isolé de son commutateur local de rattachement à cause d'une anomalie à l'interface V5.

NOTE – L'Annexe K donne de plus amples informations sur la manière dont le commutateur local et le réseau d'accès utilisent le protocole BCC.

La Figure 15 illustre le modèle fonctionnel du protocole BCC.

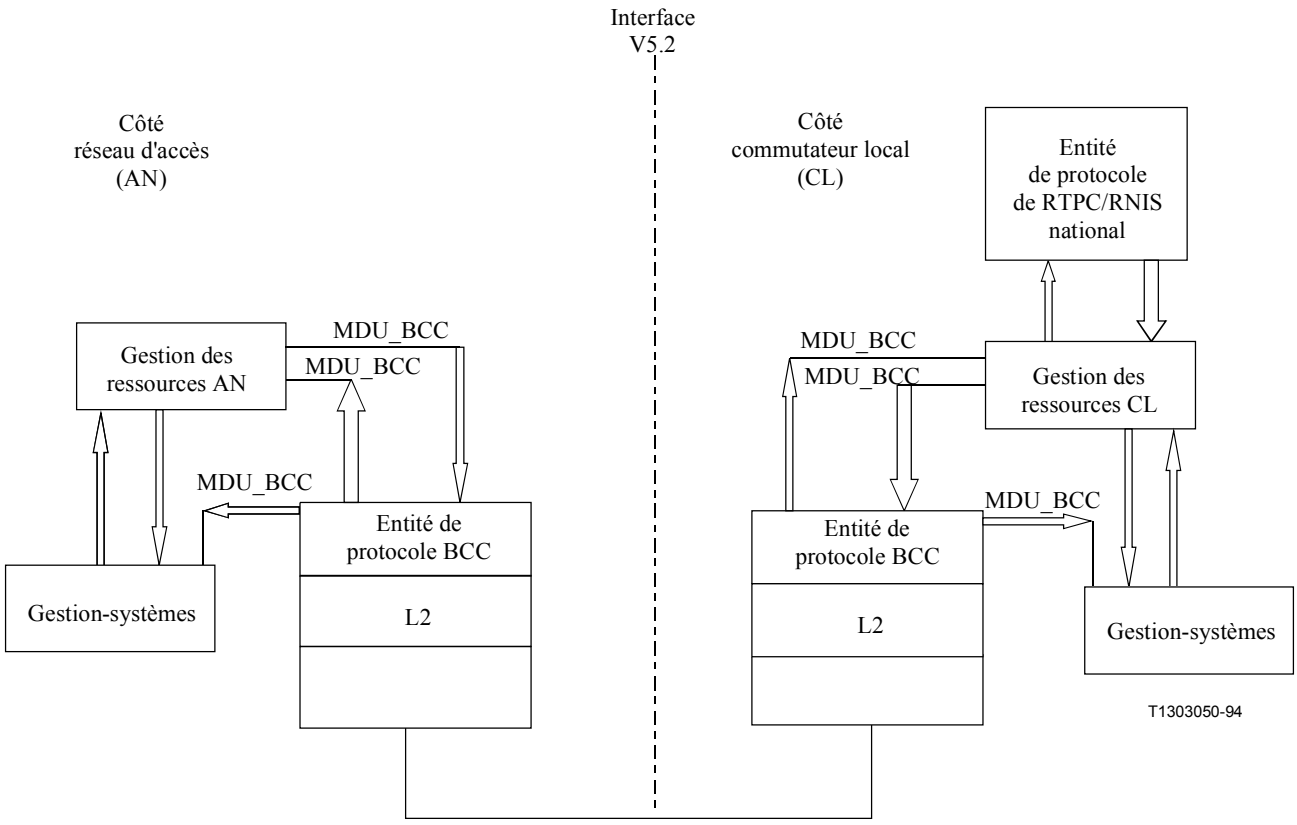


Figure 15/G.965 – Modèle fonctionnel du protocole BCC

17.2 Définition de l'entité de protocole de connexion de canal support (BCC)

17.2.1 Définition des états de protocole BCC

17.2.1.1 Etats de connexion BCC dans le réseau d'accès

Etat BCC opérationnelle (ANBcc0)

L'entité de protocole BCC du réseau d'accès est asservie au commutateur local pour les processus de protocole BCC lancés par le commutateur local (processus d'affectation, de désaffectation et d'audit). Pour tous ces processus, il est défini un seul état opérationnel (l'état "Bcc opérationnelle") de l'entité de protocole BCC du réseau d'accès.

Etat rapport d'anomalie BCC/interne au réseau d'accès (ANBcc1)

L'entité de protocole BCC du réseau d'accès considère qu'un processus est dans cet état lorsqu'un message AN FAULT (anomalie interne au réseau d'accès) a été envoyé. Le réseau d'accès s'attend à recevoir un message AN FAULT ACKNOWLEDGE (accusé de réception d'anomalie interne au réseau d'accès) avant expiration de le temporisateur Tbcc5.

17.2.1.2 Etats de connexion BCC dans le commutateur local

Etat BCC zéro (LEBcc0)

L'entité de protocole BCC du commutateur local considère qu'un processus est dans cet état lorsqu'il n'a pas encore participé à une procédure d'affectation ou de désaffectation.

Etat BCC en attente d'affectation (LEBcc1)

L'entité de protocole BCC du commutateur local considère qu'un processus est dans cet état lorsqu'un message d'affectation ALLOCATION a été envoyé. Le commutateur local s'attend à recevoir un message de désaffectation achevée ALLOCATION COMPLETE ou un message de rejet d'affectation ALLOCATION REJECT, avant expiration du temporisateur Tbcc1.

Quand le commutateur est dans cet état, il se peut également qu'il reçoive une demande interne de lancement de désaffectation (interruption d'affectation).

Etat interruption d'affectation BCC (LEBcc2)

L'entité de protocole BCC du commutateur local considère qu'un processus est dans cet état lorsqu'un message de désaffectation DE-ALLOCATION a été envoyé alors que l'entité est dans l'état BCC en attente d'affectation. Le commutateur local s'attend à recevoir un message de désaffectation achevée DE-ALLOCATION COMPLETE ou un message de rejet de désaffectation DE-ALLOCATION REJECT avant expiration du temporisateur Tbcc2.

Etat BCC en attente de désaffectation (LEBcc3)

L'entité de protocole BCC du commutateur local considère qu'un processus est dans cet état lorsqu'un message de désaffectation DE-ALLOCATION a été envoyé pendant qu'il se trouvait dans l'état BCC en attente d'affectation. Le commutateur local s'attend à recevoir un message de désaffectation achevée DE-ALLOCATION COMPLETE ou un message de rejet de désaffectation DE-ALLOCATION REJECT avant expiration du temporisateur Tbcc3.

Etat BCC en attente d'analyse (LEBcc4)

L'entité de protocole BCC du commutateur local considère qu'un processus est dans cet état lorsqu'un message AUDIT a été envoyé. Le commutateur local s'attend alors à recevoir un message AUDIT COMPLETE avant expiration du temporisateur Tbcc4.

17.2.2 Définition des primitives, messages et temporisateurs du protocole BCC

Le Tableau 26 définit les primitives, messages et temporisateurs de protocole BCC côté commutateur local de l'interface V5.2. Ces événements de protocole sont utilisés dans la table des transitions d'état du commutateur local indiquée au Tableau 46.

Le Tableau 27 définit les primitives, messages et temporisateurs de protocole BCC côté réseau d'accès de l'interface V5.2. Ces événements de protocole sont utilisés dans la table des transitions d'état du commutateur local donnée dans le Tableau 47.

17.3 Définition et contenu de messages du protocole de connexion de canal support (BCC)

Le format des messages du protocole BCC correspond à la structure générique de message définie au paragraphe 13.

L'ensemble complet des messages de protocole BCC est donné dans le Tableau 28. Les sous-paragraphes suivants donnent la structure détaillée du message de chacun de ces messages.

17.3.1 Message ALLOCATION (affectation)

Ce message est utilisé par le commutateur local pour demander au réseau d'accès l'affectation d'un canal support simple ou multiple à un point d'accès donné par identification et utilisation d'un certain intervalle de temps V5 de l'interface V5.2 (voir Tableau 29).

Tableau 26/G.965 – Primitives, messages et temporisateurs associés au protocole BCC côté CL

	Sens	Description
MDU-BCC (demande d'affectation)	RM → BCC_PE	Lancement d'un processus d'affectation de canal support
MDU-BCC (confirmation d'affectation)	RM ← BCC_PE	Fin d'un processus d'affectation de canal support
MDU-BCC (indication de rejet d'affectation)	RM ← BCC_PE	Fin d'un processus d'affectation de canal support impossible
MDU-BCC (indication d'erreur d'affectation)	RM ← BCC_PE	Après les retransmissions du message ALLOCATION aucune réponse n'est reçue du côté réseau d'accès
MDU-BCC (demande de désaffectation)	RM → BCC_PE	Lancement d'un processus de désaffectation de canal support
MDU-BCC (confirmation de désaffectation)	RM ← BCC_PE	Achèvement d'un processus de désaffectation de canal support
MDU-BCC (indication de rejet de désaffectation)	RM ← BCC_PE	Fin d'un processus de désaffectation de canal support impossible
MDU-BCC (indication d'erreur de désaffectation)	RM ← BCC_PE	Après les retransmissions du message DE-ALLOCATION aucune réponse n'est reçue du côté réseau d'accès
MDU-BCC (demande d'audit)	RM → BCC_PE	Lancement d'un processus de procédure d'analyse
MDU-BCC (confirmation d'audit)	RM ←BCC_PE	Fin d'un processus de procédure d'analyse
MDU-BCC (indication d'erreur d'audit)	RM ← BCC_PE	Après les retransmissions du message AUDIT aucune réponse n'est reçue en provenance du côté réseau d'accès

Tableau 26/G.965 – Primitives, messages et temporisateurs associés au protocole BCC côté CL

	Sens	Description
MDU-BCC (indication d'anomalie AN)	RM ← BCC_PE	Lancement d'un processus de procédure d'anomalie interne AN
MDU-BCC (indication d'erreur de protocole)	SYS ← BCC_PE	Erreur de protocole détectée par la vérification du traitement d'erreur
ALLOCATION	CL → AN	Message initial d'un processus d'affectation de canal support
ALLOCATION COMPLETE	CL ← AN	Message final d'un processus d'affectation de canal support ayant réussi
ALLOCATION REJECT	CL ← AN	Message final d'un processus d'affectation de canal support n'ayant pas réussi
DE-ALLOCATION	CL → AN	Message initial d'un processus de désaffectation de canal support
DE-ALLOCATION COMPLETE	CL ← AN	Message final d'un processus de désaffectation de canal support ayant réussi
DE-ALLOCATION REJECT	CL ← AN	Message final d'un processus de désaffectation de canal support n'ayant pas réussi
AUDIT	CL → AN	Message initial d'un processus de procédure d'analyse
AUDIT COMPLETE	CL ← AN	Message final d'un processus de procédure d'analyse ayant réussi
AN FAULT	CL ← AN	Message initial d'un processus de notification d'anomalie interne AN
AN FAULT ACKNOWLEDGE	CL → AN	Message final d'un processus de notification d'anomalie interne AN ayant réussi
PROTOCOL ERROR	CL ← AN	Notification d'une erreur de protocole BCC
Expiration du temporisateur Tbcc1	LE_BCC interne	Etat Bcc en attente d'affectation et aucun message approprié reçu
Expiration du temporisateur Tbcc2	LE_BCC interne	Etat abandon d'affectation de Bcc et aucun message approprié reçu
Expiration du temporisateur Tbcc3	LE_BCC interne	Etat Bcc en attente de désaffectation et aucun message approprié reçu
Expiration du temporisateur Tbcc4	LE_BCC interne	Etat Bcc en attente d'analyse et aucun message approprié reçu
RM	Entité de gestion des ressources du commutateur local	
BCC_PE	Entité de protocole BCC du commutateur local	
LE_BCC interne	Interne à l'entité de protocole BCC du commutateur local	
SYS	Gestion-systèmes du commutateur	

Tableau 27/G.965 – Primitives, messages et temporisateurs associés au protocole BCC côté AN

	Sens	Description
MDU-BCC (indication d'affectation)	RM ← BCC_PE	Lancement d'un processus d'affectation de canal support
MDU-BCC [réponse d'affectation (achevée)]	RM → BCC_PE	Achèvement d'un processus d'affectation de canal support
MDU-BCC [réponse d'affectation (rejet)]	RM → BCC_PE	Achèvement d'un processus d'affectation de canal support impossible
MDU-BCC (indication de désaffectation)	RM ← BCC_PE	Lancement d'un processus de désaffectation de canal support
MDU-BCC [réponse de désaffectation (achevée)]	RM → BCC_PE	Achèvement d'un processus de désaffectation de canal support
MDU-BCC [réponse de désaffectation (rejet)]	RM → BCC_PE	Achèvement d'un processus de désaffectation de canal support impossible
MDU-BCC (Indication d'audit)	RM ← BCC_PE	Lancement d'un processus de procédure d'analyse
MDU-BCC (réponse d'analyse)	RM → BCC_PE	Achèvement d'un processus de procédure d'analyse
MDU-BCC (demande d'anomalie AN)	RM → BCC_PE	Lancement d'un processus de procédure d'anomalie interne au réseau d'accès
MDU-BCC (confirmation d'anomalie AN)	RM ← BCC_PE	Fin d'un processus de procédure d'anomalie interne au réseau d'accès
MDU-BCC (indication d'erreur d'anomalie AN)	RM ← BCC_PE	Après les retransmissions du message AN FAULT aucune réponse n'est reçue en provenance du côté commutateur local
MDU-BCC (indication d'erreur de protocole)	SYS ← BCC_PE	Erreur de protocole détectée par la vérification du traitement d'erreur
ALLOCATION	CL → AN	Message initial d'un processus d'affectation de canal support
ALLOCATION COMPLETE	CL ← AN	Message final d'un processus d'affectation de canal support réussi
ALLOCATION REJECT	CL ← AN	Message final d'un processus d'affectation de canal support n'ayant pas réussi
DE-ALLOCATION	CL → AN	Message initial d'un processus de désaffectation de canal support
DE-ALLOCATION COMPLETE	CL ← AN	Message final d'un processus de désaffectation de canal support réussi
DE-ALLOCATION REJECT	CL ← AN	Message final d'un processus de désaffectation de canal support n'ayant pas réussi
AUDIT	CL → AN	Message initial d'un processus de procédure d'analyse
AUDIT COMPLETE	CL ← AN	Message final d'un processus de procédure d'analyse réussi
AN FAULT	CL ← AN	Message initial d'un processus de notification d'anomalie interne au réseau d'accès

Tableau 27/G.965 – Primitives, messages et temporisateurs associés au protocole BCC côté AN

	Sens	Description
AN FAULT ACKNOWLEDGE	CL → AN	Message final d'un processus de notification d'anomalie interne au réseau d'accès réussi
PROTOCOL ERROR	CL ← AN	Notification d'une erreur de protocole BCC
Expiration du temporisateur Tbcc5	AN_BCC interne	Etat rapport d'erreur de connexion Bcc et aucun message approprié reçu
RM	Entité de gestion des ressources du réseau d'accès	
BCC_PE	Entité de protocole BCC du réseau d'accès	
AN_BCC interne	Interne à l'entité de protocole BCC du réseau d'accès	
SYS	Gestion-systèmes du réseau d'accès	

Tableau 28/G.965 – Ensemble des messages associés au protocole BCC

Codage dans l'élément d'information Type de message							Messages de protocole BCC	Référence
7	**6**	**5**	**4**	**3**	**2**	**1**		
0	1	0	0	0	0	0	ALLOCATION (Affectation)	17.3.1
0	1	0	0	0	0	1	ALLOCATION COMPLETE (Affectation achevée)	17.3.2
0	1	0	0	0	1	0	ALLOCATION REJECT (Rejet d'affectation)	17.3.3
0	1	0	0	0	1	1	DE-ALLOCATION (Désaffectation)	17.3.4
0	1	0	0	1	0	0	DE-ALLOCATION COMPLETE (Désaffectation achevée)	17.3.5
0	1	0	0	1	0	1	DE-ALLOCATION REJECT (Rejet de désaffectation)	17.3.6
0	1	0	0	1	1	0	AUDIT (Analyse)	17.3.7
0	1	0	0	1	1	1	AUDIT COMPLETE (Fin d'analyse)	17.3.8
0	1	0	1	0	0	0	AN FAULT (Anomalie interne au réseau d'accès)	17.3.9
0	1	0	1	0	0	1	AN FAULT ACKNOWLEDGE (Accusé de réception d'anomalie interne au réseau d'accès)	17.3.10
0	1	0	1	0	1	0	PROTOCOL ERROR (Erreur de protocole)	17.3.11

Tableau 29/G.965 – Contenu du message ALLOCATION

Type de message: ALLOCATION
Sens: CL vers AN

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	CL vers AN	M	1
Numéro de référence BCC	17.4.1	CL vers AN	M	2
Type de message	17.3	CL vers AN	M	1
Identification de point d'accès utilisateur	17.4.2.1	CL vers AN	M	4
Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2	CL vers AN	C (Note 1)	3
Identification d'intervalle de temps d'interface V5	17.4.2.3	CL vers AN	C (Note 2)	4
Mappage d'intervalles de temps multiples	17.4.2.4	CL vers AN	C (Note 3)	11
Fonction de transfert d'informations	17.4.2.8	CL vers AN	C (Note 4)	3

NOTE 1 – L'élément d'information Identification de la voie d'accès au RNIS doit être inclus lors de l'affectation d'un intervalle de temps simple afin d'assurer un canal support lié à un point d'accès au RNIS. Cet élément d'information spécifie l'intervalle de temps de point d'accès utilisateur de l'interface utilisateur-réseau du RNIS (accès au débit de base ou au débit primaire) auquel le canal support doit être connecté.

NOTE 2 – L'élément d'information Identification d'intervalle de temps doit être inclus lors de l'affectation d'un intervalle de temps simple, afin d'identifier l'intervalle de temps correspondant de l'interface V5.2.

NOTE 3 – L'élément d'information mappage d'intervalles de temps multiples doit être inclus lors de l'affectation d'intervalles de temps multiples, afin d'assurer les services supports multidébit du RNIS (n × 64 kbit/s). Cet élément d'information spécifie également les intervalles de temps de point d'accès utilisateur à l'interface utilisateur-réseau du RNIS (accès au débit de base ou au débit primaire), auxquels le canal support doit être connecté.

NOTE 4 – La fonction de transfert d'informations doit être incluse lorsque l'élément d'information Identification de la voie d'accès au RNIS identifie un point d'accès RNIS.

Dans le cas d'affectations de canal support à un point d'accès du RNIS à des fins de connexions, le commutateur local indique aussi l'intervalle de temps du point d'accès utilisateur qui doit être utilisé à l'interface avec le RNIS.

Ce message permet aussi l'affectation en bloc de canaux supports multidébit (intervalles de temps V5 multiples) afin d'assurer les services multidébits (n × 64 kbit/s).

17.3.2 Message ALLOCATION COMPLETE (affectation achevée)

Ce message est utilisé par le commutateur local pour indiquer au commutateur local que l'affectation du ou des canaux supports à un point d'accès utilisateur particulier a réussi (voir Tableau 30).

Tableau 30/G.965 – Contenu du message ALLOCATION COMPLETE

Type de message: ALLOCATION COMPLETE
Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1

17.3.3 Message ALLOCATION REJECT (rejet d'affectation)

Ce message est utilisé par le réseau d'accès pour indiquer au commutateur local que l'affectation de du ou des canaux supports demandés à un point d'accès utilisateur particulier n'a pas été achevée (voir Tableau 31).

Tableau 31/G.965 – Contenu du message ALLOCATION REJECT

Type de message: ALLOCATION REJECT

Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1
Cause de rejet	17.4.2.5	AN vers CL	M	3 à 14

17.3.4 Message DE-ALLOCATION (désaffectation)

Ce message est utilisé par le commutateur local pour demander au réseau d'accès la désaffectation d'un canal support simple ou multiple d'un point d'accès donné. L'intervalle de temps V5 de l'interface V5.2 concerné est explicitement identifié (voir Tableau 32).

Ce message permet aussi la désaffectation *en bloc* de canaux supports multiples (intervalles de temps V5 multiples) afin d'assurer les services multidébit (n × 64 kbit/s).

Tableau 32/G.965 – Contenu du message DE-ALLOCATION

Type de message: DE-ALLOCATION

Sens: CL vers AN

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	CL vers AN	M	1
Numéro de référence BCC	17.4.1	CL vers AN	M	2
Type de message	17.3	CL vers AN	M	1
Identification de point d'accès utilisateur	17.4.2.1	CL vers AN	M	4
Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2	CL vers AN	C (Note 1)	3
Identification d'intervalle de temps V5	17.4.2.3	CL vers AN	C (Note 2)	4
Mappage d'intervalles de temps multiples	17.4.2.4	CL vers AN	C (Note 3)	11

NOTE 1 – L'élément d'information Identification de la voie d'accès au RNIS doit être inclus lors de la désaffectation d'un intervalle de temps simple afin de disposer d'un canal support lié à un point d'accès au RNIS. Cet élément d'information spécifie l'intervalle de temps de point d'accès utilisateur de l'interface utilisateur-réseau du RNIS (accès au débit de base ou au débit primaire) duquel le canal support doit être déconnecté.

NOTE 2 – L'élément d'information Identification d'intervalle de temps doit être inclus lors de la désaffectation d'un intervalle de temps simple afin d'identifier l'intervalle de temps correspondant de l'interface V5.2.

NOTE 3 – L'élément d'information Mappage d'intervalles de temps multiples doit être inclus lors de la désaffectation d'intervalles de temps multiples, afin d'assurer les services supports multidébit du RNIS (n × 64 kbit/s). Cet élément d'information doit également spécifier les intervalles de temps de point d'accès utilisateur à l'interface utilisateur-réseau du RNIS (accès au débit de base ou au débit primaire), desquels le canal support doit être déconnecté.

17.3.5 Message DE-ALLOCATION COMPLETE (désaffectation achevée)

Ce message est utilisé par le réseau d'accès pour indiquer au commutateur local que la désaffectation du ou des canaux supports demandés d'un point d'accès utilisateur particulier a été achevée avec succès (voir Tableau 33).

Tableau 33/G.965 – Contenu du message DE-ALLOCATION COMPLETE

Type de message: DE-ALLOCATION COMPLETE

Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1

17.3.6 Message DE-ALLOCATION REJECT (rejet de désaffectation)

Ce message est utilisé par le réseau d'accès pour indiquer au commutateur local que la désaffectation du ou des canaux supports demandés d'un point d'accès utilisateur particulier n'a pas réussi (voir Tableau 34).

Tableau 34/G.965 – Contenu du message DE-ALLOCATION REJECT

Type de message: DE-ALLOCATION REJECT

Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1
Cause de rejet	17.4.2.5	AN vers CL	M	3 à 14

17.3.7 Message AUDIT

Ce message est utilisé par le commutateur local pour demander au réseau d'accès qu'il fournisse les informations complètes identifiant la connexion de canal support à 64 kbit/s (voir Tableau 35).

Ce message permet au commutateur local de demander des informations de connexion de canal support sur la base des informations partielles disponibles dans certaines circonstances telles qu'identification de point d'accès utilisateur ainsi qu'identification de voie d'accès au RNIS, le cas échéant, ou identification d'intervalle de temps V5.

Tableau 35/G.965 – Contenu du message AUDIT

Type de message: AUDIT

Sens: CL vers AN

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	CL vers AN	M	1
Numéro de référence BCC	17.4.1	CL vers AN	M	2
Type de message	17.3	CL vers AN	M	1
Identification de point d'accès utilisateur	17.4.2.1	CL vers AN	O (Note 1)	4
Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2	CL vers AN	O (Note 2)	3
Identification d'intervalle de temps V5	17.4.2.3	CL vers AN	O (Note 3)	4
NOTE 1 – Lors d'une analyse sur la base du point d'accès utilisateur, cet élément d'information permet d'identifier le point d'accès utilisateur qui se trouve à l'extrémité de la connexion de canal support sur laquelle l'analyse doit être réalisée. NOTE 2 – Lors d'une analyse sur la base du point d'accès utilisateur qui est un point d'accès utilisateur au RNIS, cet élément d'information identifie l'intervalle de temps de point d'accès utilisateur qui se trouve à l'extrémité de la connexion de canal support sur laquelle l'analyse doit être réalisée. Cet élément d'information apparaît avec l'élément d'information Identification de point d'accès utilisateur. NOTE 3 – Lors d'une analyse sur la base de l'intervalle de temps V5, cet élément d'information identifie l'intervalle de temps V5 de l'interface V5.2 assurant la connexion de canal sur laquelle l'analyse doit être réalisée. Le message AUDIT doit toujours inclure l'élément d'information Identification du point d'accès utilisateur ou l'élément d'information Intervalle de temps V5, mais pas les deux. Lorsqu'il est inclus, l'élément d'information doit être traité comme un élément d'information obligatoire.				

17.3.8 Message AUDIT COMPLETE (analyse achevée)

Ce message est utilisé par le réseau d'accès pour donner au commutateur local le résultat de l'audit demandé, en fournissant les informations identifiant la connexion de canal support ou en indiquant qu'aucune connexion n'est disponible à la référence fournie (voir Tableau 36).

Tableau 36/G.965 – Contenu du message AUDIT COMPLETE

Type de message: AUDIT COMPLETE

Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1
Identification de point d'accès utilisateur	17.4.2.1	AN vers CL	O (Note 1)	4
Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2	AN vers CL	O (Note 1)	3
Identification d'intervalle de temps V5	17.4.2.3	AN vers CL	O (Note 1)	4
Connexion non achevée	17.4.2.7	AN vers CL	O (Note 2)	3

Tableau 36/G.965 – Contenu du message AUDIT COMPLETE

NOTE 1 – L'élément d'information Identification du point d'accès utilisateur doit être inclus, ainsi que le cas échéant, l'élément d'information Identification de voie d'accès au RNIS, et l'élément d'information Identification d'intervalle de temps V5 si le résultat du processus d'analyse indique la présence d'une connexion existante achevée. NOTE 2 – Cet élément d'information doit être inclus lorsqu'un processus d'analyse n'a pas réussi en raison de l'absence de connexion associée aux informations de référence fournies par le processus d'analyse. NOTE 3 – Le message AUDIT COMPLETE doit toujours inclure soit l'élément d'information Identification du point d'accès utilisateur et l'élément d'information Identification de l'intervalle de temps V5 et le cas échéant l'élément d'information Identification de la voie d'accès RNIS, soit l'élément d'information Connexion non achevée. Lorsqu'ils sont inclus, ces éléments d'information doivent être traités comme éléments d'information obligatoires.

17.3.9 Message AN FAULT (anomalie interne au réseau d'accès)

Ce message est utilisé par le réseau d'accès pour signaler au commutateur local qu'une connexion de canal support simple à 64 kbit/s a été perdue dans le réseau d'accès en raison d'une anomalie interne (voir Tableau 37).

Lorsqu'il signale une anomalie interne, le réseau d'accès doit fournir les informations nécessaires pour permettre au commutateur local d'identifier toutes les données qui se rapportent à cette connexion.

Tableau 37/G.965 – Contenu du message AN FAULT

Type de message: AN FAULT

Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1
Identification de point d'accès utilisateur	17.4.2.1	AN vers CL	O (Note 1)	4
Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2	AN vers CL	O (Note 2)	3
Identification d'intervalle de temps V5	17.4.2.3	AN vers CL	O (Note 3)	4
NOTE 1 – Lorsqu'une connexion interne au réseau d'accès échoue, cet élément d'information est inclus s'il est disponible, avec l'élément d'information Identification de la voie d'accès au RNIS, le cas échéant, afin de notifier au commutateur local le point d'accès utilisateur qui est touché par l'anomalie du réseau d'accès. NOTE 2 – Lorsqu'une connexion interne au réseau d'accès échoue, cet élément d'information est utilisé lorsque la notification d'anomalie fait référence à un point d'accès utilisateur au RNIS identifié par l'élément d'information Identification de point d'accès utilisateur. NOTE 3 – Lorsqu'une connexion interne au réseau d'accès échoue, cet élément d'information est inclus s'il est disponible, afin d'informer le commutateur local de l'intervalle de temps V5 de l'interface V5.2 qui est touché par l'anomalie du réseau d'accès.				

17.3.10 Message AN FAULT ACKNOWLEDGE (accusé de réception d'anomalie interne au réseau d'accès)

Ce message est utilisé par le commutateur local pour accuser réception d'un message AN FAULT envoyé par le réseau d'accès (voir Tableau 38).

NOTE – L'envoi de ce message est un accusé de réception du message AN FAULT reçu et non une notification d'exécution des opérations appropriées.

Tableau 38/G.965 – Contenu du message AN FAULT ACKNOWLEDGE

Type de message: AN FAULT ACKNOWLEDGE

Sens: CL vers AN

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	CL vers AN	M	1
Numéro de référence BCC	17.4.1	CL vers AN	M	2
Type de message	17.3	CL vers AN	M	1

17.3.11 Message PROTOCOL ERROR (erreur de protocole)

Ce message est utilisé par le réseau d'accès pour indiquer au commutateur local qu'une erreur de protocole a été détectée dans un message reçu (voir Tableau 39).

Tableau 39/G.965 – Contenu du message PROTOCOL ERROR

Type de message: PROTOCOL ERROR

Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Numéro de référence de BCC	17.4.1	AN vers CL	M	2
Type de message	17.3	AN vers CL	M	1
Cause d'erreur de protocole	17.4.2.6	AN vers CL	M	3 à 5

17.4 Définition, structure et codage de l'élément d'information BCC

Le présent paragraphe définit le codage des éléments d'information qui sont propres au protocole de connexion de canal support (BCC), utilisés dans les messages propres au protocole BCC. Pour chacun de ces éléments, on donne le codage de leurs divers champs d'information.

La liste des éléments d'information propres au protocole BCC figure au Tableau 40, qui donne également le codage de l'identifiant d'élément d'information.

Tableau 40/G.965 – Eléments d'information propres au protocole BCC

Bits								Elément d'information	Référence
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
0	–	–	–	–	–	–	–	Eléments d'information de longueur variable	
0	1	0	0	0	0	0	0	Identification de point d'accès utilisateur	17.4.2.1
0	1	0	0	0	0	0	1	Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2
0	1	0	0	0	0	1	0	Identification d'intervalle de temps V5	17.4.2.3
0	1	0	0	0	0	1	1	Mappage d'intervalles de temps multiples	17.4.2.4
0	1	0	0	0	1	0	0	Cause de rejet	17.4.2.5
0	1	0	0	0	1	0	1	Cause d'erreur de protocole	17.4.2.6
0	1	0	0	0	1	1	0	Connexion non achevée	17.4.2.7
0	1	0	0	0	1	1	1	Fonction de transfert d'informations	17.4.2.8
NOTE – Toutes les autres valeurs sont réservées.									

17.4.1 Elément d'information numéro de référence BCC

Cet élément d'information est propre au protocole de connexion BCC et utilise l'emplacement de l'élément d'information Adresse de couche 3 dans la structure générale du message telle que la définit le paragraphe 13.

L'objet de l'élément d'information Numéro de référence BCC est d'identifier le processus de protocole BCC, au niveau de l'interface V5.2, auquel s'applique le message transmis ou reçu.

La valeur du numéro de référence BCC est un nombre aléatoire généré par l'entité (réseau d'accès ou commutateur local) créant le nouveau processus de protocole BCC (cette valeur aléatoire peut être implémentée comme une génération séquentielle de valeurs). Il est important que les valeurs ne soient pas répétées dans les messages pour lesquels un autre processus de connexion de canal support est nécessaire (dans le même sens), jusqu'à ce que l'ancien processus BCC soit terminé et que le numéro ait été supprimé. L'élément d'information Numéro de référence BCC, en tant que partie de l'en-tête de message, forme la seconde partie de chaque message (il se situe après l'élément d'information Discriminateur de protocole). En cas de processus donnant lieu à des indications d'erreurs, le numéro de référence BCC ne doit pas être réutilisé avant un laps de temps suffisant pour permettre l'arrivée en retard de messages contenant le même numéro de référence BCC.

La longueur de l'élément d'information Numéro de référence BCC est de 2 octets.

La Figure 16 indique la structure de l'élément d'information Numéro de référence BCC.

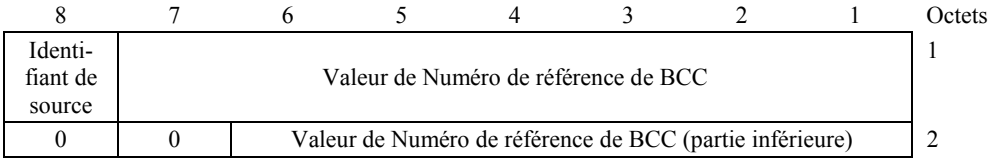


Figure 16/G.965 – Elément d'information numéro de référence de BCC

L'identification de source est un champ occupant un bit spécifiant l'entité (commutateur local ou réseau d'accès) qui a généré le numéro de référence (c'est-à-dire l'entité qui a créé le processus de protocole BCC). Le codage de ce champ doit être "zéro" pour un processus créé par le commutateur local, et "un" pour un processus créé par le réseau d'accès.

Le champ numéro de référence BCC comprend 13 bits et est utilisé pour fournir le codage binaire qui identifie le processus BCC.

17.4.2 Autres éléments d'information

Le présent paragraphe décrit les éléments d'information qui peuvent apparaître dans les différents messages.

Ces éléments peuvent être soit facultatifs ou obligatoires, selon la sémantique du message ou l'utilisation du message par le processus.

17.4.2.1 Elément d'information Identification de point d'accès utilisateur

L'objet de l'élément d'information Identification de point d'accès utilisateur est d'identifier via l'interface V5.2 le point d'accès RTPC ou RNIS auquel s'applique le message du processus de protocole BCC.

La longueur de l'élément d'information Identification de point d'accès utilisateur est de 4 octets.

Sa structure est illustrée par les Figures 17 et 18.

L'élément d'information Identification de point d'accès utilisateur est codé en binaire. Pour le codage de cet élément, deux structures ont été définies, l'une pour les applications de point d'accès RTPC (voir Figure 17), l'autre pour les applications de point d'accès RNIS (voir Figure 18).

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	0	0	0	1
Longueur du contenu de l'élément d'information								2
Valeur de Identification de point d'accès utilisateur							1	3
Valeur de Identification de point d'accès utilisateur (partie inférieure)								4

Figure 17/G.965 – Elément d'information Identification de point d'accès utilisateur (application au point d'accès RTPC)

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	0	0	0	1
Longueur du contenu de l'élément d'information								2
Valeur de Identification de point d'accès utilisateur						0	0	3
Valeur de Identification de point d'accès utilisateur (partie inférieure)							1	4

Figure 18/G.965 – Elément d'information Identification de point d'accès utilisateur (application au point d'accès au RNIS)

Dans le cas des applications de point d'accès au RTPC, la valeur de l'identification de point d'accès utilisateur (15 bits) doit être la même que celle de l'élément d'information Adresse de couche 3 contenu dans les messages du protocole RTPC concernant le point d'accès utilisateur RTPC auquel s'applique le message associé au processus.

Dans le cas des applications de point d'accès RNIS, la valeur de l'identification de point d'accès utilisateur (13 bits) doit être la même que celle de l'élément d'information Adresse d'enveloppe contenu dans les trames de fonction d'enveloppe utilisées pour la répétition des messages du système de signalisation DSS1 concernant ce point d'accès utilisateur RNIS auquel s'applique le message associé au processus.

17.4.2.2 Elément d'information Identification d'intervalle de temps de point d'accès RNIS

L'objet de l'élément d'information Identification d'intervalle de temps de point d'accès RNIS est d'indiquer, uniquement dans le cas d'un protocole BCC d'intervalle de temps V5 simple concernant un point d'accès utilisateur du RNIS, l'intervalle de temps de point d'accès utilisateur de l'interface utilisateur-réseau du RNIS (accès de base ou accès au débit primaire) auquel l'intervalle de temps V5 de la liaison à 2048 kbit/s de l'interface V5.2 doit être connecté ou dont il doit être déconnecté.

La longueur de l'élément d'information Identification d'intervalle de temps de point d'accès au RNIS est de 3 octets.

Sa structure doit être conforme à ce qui est indiqué par la Figure 19.

Le numéro d'intervalle de temps de point d'accès utilisateur RNIS est un champ codé sur 5 bits précisant le code binaire qui identifie l'intervalle de temps du point d'accès utilisateur RNIS. Dans le cas de point d'accès utilisateur au débit primaire du RNIS (PRA-RNIS), les canaux B1 à B31 sont appelés intervalles de temps de point d'accès utilisateur RNIS numéro 1 (00001) à 31 (11111). Dans le cas de point d'accès utilisateur au débit de base du RNIS, la voie B1 est appelé intervalle de temps de point d'accès utilisateur RNIS numéro 1 (00001) et la voie B2, intervalle de temps de point d'accès utilisateur RNIS numéro 2 (00010).

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	0	0	1	1
Longueur du contenu de l'élément d'information								2
1	0	0	Numéro d'intervalle de temps de point d'accès utilisateur RNIS					3

Figure 19/G.965 – Elément d'information Identification d'intervalle de temps de point d'accès RNIS

17.4.2.3 Elément d'information Identification d'intervalle de temps V5

L'objet de l'élément d'information Identification d'intervalle de temps V5 est d'identifier, dans le cas d'un processus de protocole BCC d'intervalle de temps V5 simple, l'intervalle de temps V5 d'une liaison à 2048 kbit/s particulière auquel s'applique le processus.

La longueur de l'élément d'information Identification d'intervalle de temps V5 est de 4 octets.

Sa structure doit être conforme à ce qui est indiqué par la Figure 20.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	0	1	0	1
Longueur du contenu de l'élément d'information								2
Identifiant de liaison d'interface V5 à 2048 kbit/s								3
0	0	Prise de contrôle	Numéro d'intervalle de temps V5					4

Figure 20/G.965 – Elément d'information Identification d'intervalle de temps V5

L'identifiant de liaison V5 à 2048 kbit/s est un champ à 8 bits qui est utilisé pour fournir le codage binaire identifiant une liaison particulière à 2048 kbit/s où se trouve l'intervalle de temps V5 sélectionné pour être utilisé comme canal support, parmi celles qui forment l'interface V5.2. Un maximum de 256 liaisons (à 2048 kbit/s) peuvent être identifiées explicitement.

Le numéro d'intervalle de temps V5 est un champ de 5 bits qui est utilisé pour fournir le codage binaire identifiant l'intervalle de temps V5 ou le premier intervalle de temps V5 d'un bloc d'intervalles de temps V5 (dans la liaison à 2048 kbit/s identifiée par l'octet précédent), qui est utilisé ou qui doit être utilisé comme canal support.

Le bit de prise de contrôle spécifie la demande du commutateur local de prise de contrôle de la connexion de canal support existante sur l'intervalle de temps V5 identifié, lors de l'établissement de la connexion de canal support demandée. Ce champ doit être codé par un zéro pour "prise de contrôle non demandée" et un "un" pour "prise de contrôle demandée".

17.4.2.4 Elément d'information Mappage d'intervalles de temps multiples

L'objet de l'élément d'information Mappage d'intervalles de temps multiples est d'identifier, en cas d'affectation ou de désaffectation *en bloc* d'intervalles de temps multiples, tous les intervalles de temps V5 d'une liaison V5 à 2048 kbit/s auxquels s'applique le processus d'affectation ou de désaffectation.

Cet élément d'information identifie également les intervalles de temps de point d'accès utilisateur de l'interface utilisateur-réseau du RNIS auxquels les intervalles de temps V5 identifiés doivent être connectés ou dont ils doivent être déconnectés.

La relation entre intervalles de temps V5 identifiés et intervalle de temps de point d'accès utilisateur se fait de façon biunivoque dans le même ordre d'apparition indiqué dans chaque correspondance de codage respectif.

NOTE – Lorsque plusieurs intervalles de temps V5 ont été affectés *en bloc*, on peut les désaffecter *en bloc* ou non.

Le nombre d'intervalles de temps V5 concernés par un processus de désaffectation est déterminé par le système de gestion des ressources sur la base du service RNIS fourni.

Dans certaines circonstances (par exemple, redémarrage de l'interface RNIS), un processus de désaffectation concernant plusieurs intervalles de temps V5 peut être demandé par le système de gestion des ressources, même si ces intervalles de temps V5 ont été attribués individuellement.

La longueur de l'élément d'information Mappage d'intervalles de temps multiples est de 11 octets.

Sa structure doit être conforme à ce qui est indiqué par la Figure 21.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	0	1	1	1
Longueur du contenu de l'élément d'information								2
Identifiant de liaison V5 à 2048 kbit/s								3
V5TS31	V5TS30	V5TS29	V5TS28	V5TS27	V5TS26	V5TS25	V5TS24	4
V5TS23	V5TS22	V5TS21	V5TS20	V5TS19	V5TS18	V5TS17	V5TS16	5
V5TS15	V5TS14	V5TS13	V5TS12	V5TS11	V5TS10	V5TS9	V5TS8	6
V5TS7	V5TS6	V5TS5	V5TS4	V5TS3	V5TS2	V5TS1	0	7
UPTS31	UPTS30	UPTS29	UPTS28	UPTS27	UPTS26	UPTS25	UPTS24	8
UPTS23	UPTS22	UPTS21	UPTS20	UPTS19	UPTS18	UPTS17	UPTS16	9
UPTS15	UPTS14	UPTS13	UPTS12	UPTS11	UPTS10	UPTS9	UPTS8	10
UPTS7	UPTS6	UPTS5	UPTS4	UPTS3	UPTS2	UPTS1	0	11

Figure 21/G.965 – Elément d'information Mappage d'intervalles de temps multiples

L'identifiant de liaison V5 à 2048 kbit/s est un champ codé binaire à 8 bits identifiant la liaison particulière à 2048 kbit/s (parmi celles qui peuvent fermer l'interface V5.2) où se trouve l'intervalle de temps sélectionné pour être utilisé comme canal support. Un maximum de 256 liaisons (à 2048 kbit/s) peuvent être identifiées explicitement.

Les octets 4 à 7 identifient des intervalles de temps multiples de l'interface V5.2 qui sont affectés ou désaffectés *en bloc*. Les bits correspondants aux intervalles de temps V5 sur lesquels le processus agit sont codés comme des "1" binaires, les bits correspondants aux intervalles de temps sur lesquels le processus n'agit pas, comme des "0" binaires.

Les octets 8 à 11 identifient des intervalles de temps multiples du point d'accès utilisateur au RNIS (accès de base ou primaire) auxquels les intervalles de temps V5 spécifiés par les octets 4 à 7 doivent être connectés ou dont ils doivent être déconnectés. La relation entre intervalles de temps V5 et intervalles de temps de point d'accès utilisateur se fait un à un dans l'ordre de numérotation spécifié. Les bits correspondants aux intervalles de temps sur lesquels le processus agit sont codés comme des "1" binaires, les bits correspondants aux intervalles de temps sur lesquels le processus n'agit pas, comme des "0" binaires.

Dans le cas d'un point d'accès utilisateur au débit de base du RNIS, les deux canaux B sont appelés intervalles de temps de point d'accès utilisateur UPTS1 et UPTS2 dans le mappage, UPTS3 à UPTS31 ne sont jamais activés dans ce cas.

17.4.2.5 Elément d'information Cause de rejet

L'objet de l'élément d'information Cause de rejet est d'indiquer du réseau d'accès au commutateur local la raison de l'échec de l'affectation ou de la désaffectation du canal ou des canaux supports demandés.

Cet élément comprend, pour certaines causes de rejet, un champ diagnostic permettant de fournir des informations supplémentaires concernant ces causes. Ce champ diagnostic lorsqu'il existe, est toujours constitué par une copie de l'élément d'information reçu qui contenait les informations qui ont déclenché l'envoi du message de rejet.

La longueur de l'élément d'information Identification d'intervalle de temps de point d'accès au RNIS est comprise entre 3 et 14 octets. Pour les types de cause de rejet qui ne comprennent pas les informations de diagnostic, la longueur de l'élément d'information est de 3 octets. Pour les types de cause de rejet qui les comprennent, la longueur de l'élément d'information varie entre 6 et 14 octets (les valeurs autorisées étant 6, 7 et 14).

La structure de cet élément doit être conforme à ce qui est indiqué par la Figure 22.

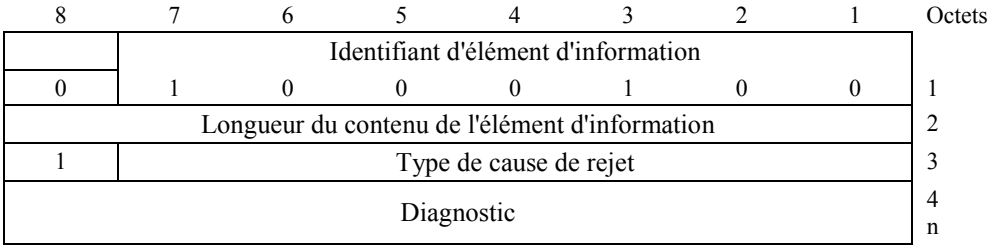


Figure 22/G.965 – Elément d'information Cause de rejet

Le Tableau 41 spécifie le codage du champ type de cause de rejet.

Tableau 41/G.965 – Codage du type de cause de rejet

7	6	5	4	3	2	1	Cause de rejet
0	0	0	0	0	0	0	Non spécifié
0	0	0	0	0	0	1	Anomalie du réseau d'accès
0	0	0	0	0	1	0	Blocage du réseau d'accès (interne)
0	0	0	0	0	1	1	Connexion existant déjà au point d'accès utilisateur RTPC vers un autre intervalle de temps V5
0	0	0	0	1	0	0	Connexion existant déjà aux intervalles de temps V5 vers un autre point d'accès ou un autre intervalle de temps de point d'accès utilisateur
0	0	0	0	1	0	1	Connexion existant déjà aux intervalles de temps de point d'accès utilisateur RNIS vers d'autres intervalles de temps V5
0	0	0	0	1	1	0	Point d'accès utilisateur non disponible (bloqué)
0	0	0	0	1	1	1	La désaffectation ne peut être réalisée en raison d'une incompatibilité de contenu de données
0	0	0	1	0	0	0	La désaffectation ne peut être réalisée en raison d'une incompatibilité de données d'intervalles de temps V5
0	0	0	1	0	0	1	La désaffectation ne peut être réalisée en raison d'une incompatibilité de données de point d'accès
0	0	0	1	0	1	0	La désaffectation ne peut être réalisée en raison d'une incompatibilité de données d'intervalles de temps de point d'accès utilisateur
0	0	0	1	0	1	1	Point d'accès utilisateur non profilé
0	0	0	1	1	0	0	Identifications d'intervalles de temps V5 non valides
0	0	0	1	1	0	1	Identification de liaison V5 à 2048 kbit/s non valide
0	0	0	1	1	1	0	Identifications d'intervalles de temps de point d'accès utilisateur non valides
0	0	0	1	1	1	1	Intervalles de temps V5 utilisés comme voies C physiques
0	0	1	0	0	0	0	Liaison V5 non disponible (bloquée)
NOTE – Toutes les autres valeurs sont réservées.							

Le Tableau K.1 contient de plus amples informations sur la manière d'utiliser les différents types de cause de rejet dans les procédures de protocole de connexion de canal support (BCC).

Le champ diagnostic est un champ à plusieurs octets (dont le nombre dépend de la valeur de cause), qui fournit un diagnostic approprié pour chaque type de cause de rejet, conformément au Tableau 42.

Tableau 42/G.965 – Diagnostic pour les types de cause de rejet

Cause	Diagnostic	Longueur
Non spécifié	Absent	0
Anomalie interne au réseau d'accès	Absent	0
Blocage du réseau d'accès (interne)	Absent	0
Connexion existant déjà au point d'accès utilisateur RTPC vers un autre intervalle de temps V5	Elément d'information Identification de point d'accès utilisateur	4
Connexion existant déjà aux intervalles de temps V5 de l'interface V5.2 vers un autre point d'accès ou un autre intervalle de temps de point d'accès utilisateur RNIS	Identification d'intervalle de temps V5 ou élément d'information Mappage d'intervalles de temps multiples	4 ou 11
Connexion existant déjà aux points d'accès utilisateur du RNIS vers d'autres intervalles de temps V5	Identification de voie d'accès au RNIS ou élément d'information Mappage d'intervalles de temps multiples	3 ou 11
Point d'accès utilisateur non disponible (bloqué)	Elément d'information Identification de point d'accès utilisateur	4
La désaffectation ne peut être réalisée en raison d'un contenu de données incompatible	Absent	0
La désaffectation ne peut être réalisée en raison d'une incompatibilité de données d'intervalles de temps V5	Identification d'intervalle de temps V5 ou élément d'information Mappage d'intervalles de temps multiples	4 ou 11
La désaffectation ne peut être réalisée en raison d'une incompatibilité de données de point d'accès utilisateur	Elément d'information Identification de point d'accès utilisateur	4
La désaffectation ne peut être réalisée en raison d'une incompatibilité de données d'intervalles de temps de point d'accès	Identification de voie d'accès au RNIS ou élément d'information Mappage d'intervalles de temps multiples	3 ou 11
Point d'accès non profilé	Elément d'information Identification de point d'accès utilisateur	4
Identifications d'intervalles de temps V5 non valides	Identification d'intervalle de temps V5 ou élément d'information Mappage d'intervalles de temps multiples	4 ou 11
Identification de liaison V5 à 2048 kbit/s non valide	Identification d'intervalle de temps V5 ou élément d'information Mappage d'intervalles de temps multiples	4 ou 11
Identifications d'intervalles de temps de point d'accès utilisateur non valides	Identification de voie d'accès au RNIS ou élément d'information Mappage d'intervalles de temps multiples	3 ou 11
Intervalles de temps V5 utilisés comme voies C physiques	Identification d'intervalle de temps V5 ou élément d'information Mappage d'intervalles de temps multiples	4 ou 11
Liaison V5 non disponible (bloquée)	Identification d'intervalle de temps V5 ou élément d'information Mappage d'intervalles de temps multiples	4 ou 11

Si la longueur des diagnostics dans l'élément d'information Cause de rejet n'est pas correcte (c'est-à-dire n'est pas conforme à la valeur donnée au Tableau 42), l'élément d'information doit réagir conformément au 17.5.8.7.

17.4.2.6 Elément d'information Cause d'erreur de protocole

L'objet de l'élément d'information Cause d'erreur de protocole est d'indiquer du réseau d'accès au commutateur local le type d'erreur de protocole détectée dans un processus de protocole BCC donné.

Cet élément doit comporter, pour certains types de cause d'erreur de protocole, un champ diagnostic permettant de fournir des informations supplémentaires concernant ces types de cause d'erreur de protocole. Ce champ diagnostic, d'un ou deux octets, lorsqu'il existe, est une copie de l'identifiant de type de message reçu qui a déclenché l'envoi du message contenant l'élément d'information Cause d'erreur de protocole et si nécessaire l'identifiant d'élément d'information approprié de ce message.

La longueur de l'élément d'information Cause d'erreur de protocole peut être de 3 à 5 octets. Pour les types de cause d'erreur de protocole qui ne comprennent pas les informations de diagnostic, la longueur de l'élément d'information est de 3 octets. Pour les types de cause d'erreur de protocole qui les comprennent, la longueur de l'élément d'information est de 4 ou 5 octets.

La structure de cet élément doit être conforme à ce qui est indiqué par la Figure 23.

8	7	6	5	4	3	2	1	Octets
Identifiant d'élément d'information								
0	1	0	0	0	1	0	1	1
Longueur du contenu de l'élément d'information								2
1	Type de cause d'erreur de protocole							3
0	Diagnostic (identifiant de type de message)							4
Diagnostic (identifiant d'élément d'information)								5

Figure 23/G.965 – Elément d'information Cause d'erreur de protocole

Le Tableau 43 spécifie le codage du champ type de cause d'erreur de protocole.

Tableau 43/G.965 – Type de cause d'erreur de protocole

7	6	5	4	3	2	1	Cause d'erreur de protocole
0	0	0	0	0	0	1	Erreur de discriminateur de protocole
0	0	0	0	1	0	0	Type de message non reconnu
0	0	0	0	1	0	1	Elément d'information hors séquence
0	0	0	0	1	1	0	Elément d'information facultatif répété
0	0	0	0	1	1	1	Elément d'information obligatoire manquant
0	0	0	1	0	0	0	Elément d'information non reconnu
0	0	0	1	0	0	1	Erreur de contenu d'élément d'information obligatoire
0	0	0	1	0	1	0	Erreur de contenu d'élément d'information facultatif
0	0	0	1	0	1	1	Message incompatible avec l'état du protocole BCC
0	0	0	1	1	0	0	Elément d'information obligatoire répété
0	0	0	1	1	0	1	Eléments d'information trop nombreux
0	0	0	1	1	1	1	Erreur de codage du numéro de référence BCC
NOTE – Toutes les autres valeurs sont réservées.							

Le paragraphe 17.5.8 spécifie la manière d'utiliser les différentes valeurs de types de cause d'erreur de protocole.

Le champ diagnostic, qui est codé sur plusieurs octets (le nombre des octets dépendant de la valeur de cause), donne le diagnostic approprié pour chaque valeur de cause d'erreur de protocole conformément au Tableau 44.

Tableau 44/G.965 – Diagnostic pour les types d'erreur de protocole

Cause	Diagnostic	Longueur
Erreur de discriminateur de protocole	Absent	0
Erreur de codage du numéro de référence BCC	Absent	0
Type de message non reconnu	Identifiant de type de message	1
Elément d'information hors séquence	Identifiant d'élément d'information Identifiant de type de message	2
Elément d'information facultatif répété	Identifiant d'élément d'information Identifiant de type de message	2
Elément d'information obligatoire manquant	Identifiant d'élément d'information Identifiant de type de message	2
Elément d'information non reconnu	Identifiant d'élément d'information Identifiant de type de message	2
Erreur de contenu d'élément d'information obligatoire	Identifiant d'élément d'information Identifiant de type de message	2
Erreur de contenu d'élément d'information facultatif	Identifiant d'élément d'information Identifiant de type de message	2
Message incompatible avec l'état du protocole BCC	Identifiant de type de message	1
Elément d'information obligatoire répété	Identifiant d'élément d'information Identifiant de type de message	2
Eléments d'information trop nombreux	Identifiant de type de message	1

Si la longueur des diagnostics dans l'élément d'information Cause d'erreur de protocole n'est pas correcte (c'est-à-dire n'est pas conforme à la valeur donnée au Tableau 44), le commutateur local doit réagir conformément au 17.5.8.7.

17.4.2.7 Elément d'information Connexion incomplète

L'objet de l'élément d'information Connexion incomplète est d'indiquer du réseau d'accès au commutateur local que le résultat d'un processus d'analyse est négatif en raison de l'absence de connexion au réseau d'accès.

Dans le champ de cause, cet élément d'information donne la cause pour lequel la connexion n'a pas été établie.

La longueur de l'élément d'information Connexion incomplète est de 3 octets.

La structure de cet élément doit être conforme à ce qui est indiqué par la Figure 24.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	1	1	0	1
Longueur du contenu de l'élément d'information								2
ext. 1	Cause							3
NOTE – Le bit 8 est marqué "1 ext." parce qu'il s'agit du dernier octet du domaine d'extension. Des octets supplémentaires pourront être définis ultérieurement ("1 ext." deviendra "0/1 ext.") et les équipement devront être prêts à recevoir de tels octets supplémentaires bien qu'il ne soit pas nécessaire qu'ils puissent les interpréter ou agir sur le contenu de ces octets.								

Figure 24/G.965 – Elément d'information Connexion incomplète

Le Tableau 45 spécifie le codage du champ raison de l'élément d'information Connexion incomplète.

Tableau 45/G.965 – Codage du champ cause

7	6	5	4	3	2	1	Cause
0	0	0	0	0	0	0	Incomplet normal
0	0	0	0	0	0	1	Anomalie interne au réseau d'accès
0	0	0	0	0	1	0	Point d'accès utilisateur non profilé
0	0	0	0	0	1	1	Identification d'intervalle de temps V5 non valide
0	0	0	0	1	0	0	Identification de liaison V5 à 2048 kbit/s non valide
0	0	0	0	1	0	1	Intervalle de temps V5 utilisé comme voie C physique
NOTE – Toutes les autres valeurs sont réservées.							

17.4.2.8 Elément d'information Fonction de transfert d'informations

L'objet de l'élément d'information Fonction de transfert d'informations est d'indiquer au réseau d'accès la fonction de transfert d'informations nécessaire pour un canal support RNIS donné sur un accès utilisateur RNIS donné.

Le commutateur local doit avoir la possibilité de permettre ou d'empêcher l'utilisation de cet élément d'information au moyen du profilage.

Le contenu de cet élément d'information est un sous-ensemble de l'élément d'information Capacité support présent dans le système DSS1.

La longueur de l'élément d'information Fonction de transfert d'informations est de 3 octets.

La structure de cet élément doit être conforme à ce qui est indiqué par la Figure 24a.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	0	0	1	1	1	1
Longueur du contenu de l'élément d'information								2
1	0	0	Fonction de transfert d'informations					3

Figure 24a/G.965 – Elément d'information Fonction de transfert d'informations

Le codage de l'octet 3 est identique au codage de l'octet 3 de l'élément d'information Capacité support dans les messages du système DSS1.

17.5 Description du protocole et des procédures de connexion de canal support (BCC)

L'Annexe K donne de plus amples détails sur l'interaction entre les appels commutés et le protocole de connexion BCC.

17.5.1 Généralités

Comme le réseau d'accès et l'interface V5.2 sont transparents aux protocoles de commande d'appel du RNIS et du RTPC, la procédure appropriée de ce protocole BCC doit être déclenchée à partir de l'entité de gestion des ressources du commutateur local, suite à l'analyse des procédures de commande d'appel du réseau RNIS ou RTPC.

Du point de vue de la connexion de canal support (BCC), chaque affectation ou désaffectation d'intervalle de temps V5 est considérée comme un processus indépendant qui se conclut par la réussite ou l'abandon de l'affectation de l'intervalle de temps V5.

Chaque processus doit être identifié par un numéro de référence BCC différent des autres. L'entité de protocole BCC et l'entité de gestion des ressources permettent à plusieurs processus BCC de fonctionner en parallèle.

NOTE – Pour le protocole BCC (procédures de commande de canal support), on suppose qu'une machine FSM individuelle doit être implémentée pour chaque demande d'affectation ou de désaffectation concernant un ou plusieurs des intervalles de temps V5.2 disponibles pour être utilisés comme canal support.

Les procédures qui forment le protocole de connexion de canal support, décrites dans les paragraphes suivants, sont les suivantes:

– affectation de canal support: procédure normale;
– affectation de canal support: procédures exceptionnelles;
– désaffectation de canal support: procédure normale; doit être conforme à ce qui est indiqué
– désaffectation de canal support: procédures exceptionnelles;
– procédure d'analyse;
– procédure de notification d'anomalie interne au réseau d'accès;
– traitement des situations d'erreur.

17.5.2 Affectation de canal support – Procédure normale

Si l'entité de protocole BCC du commutateur local est dans l'état "Bcc zéro" et reçoit une primitive MDU-BCC (demande d'affectation), elle lance l'affectation de canal support en envoyant au réseau d'accès un message ALLOCATION (affectation) indiquant le ou les intervalles de temps V5 de l'interface V5.2 à utiliser. Dans le cas d'affectations concernant les points d'accès RNIS, le commutateur local indique également le ou les intervalles de temps de point d'accès utilisateur RNIS à l'interface utilisateur-réseau du RNIS qui doivent être connectés à l'intervalle de temps V5 sélectionné.

Avec l'envoi du message ALLOCATION, le commutateur local doit lancer le temporisateur Tbcc1 et passer à l'état "Bcc en attente d'affectation".

Lorsque l'entité de protocole BCC du réseau d'accès reçoit le message ALLOCATION, elle signale l'événement à l'entité de gestion des ressources à l'aide de la primitive MDU-BCC (indication d'affectation). Lorsque c'est possible, le réseau d'accès affecte le ou les intervalles de temps V5 spécifiés au point d'accès spécifié. Après réception de la primitive de réponse MDU-BCC [réponse d'affectation (achevée)], l'entité de protocole BCC du réseau d'accès envoie au commutateur local le message ALLOCATION COMPLETE (affectation achevée).

A réception d'un message ALLOCATION COMPLETE que, par analyse de l'élément d'information Numéro de référence BCC, le commutateur local considère comme étant la réponse à un message ALLOCATION envoyé auparavant, il arrête le temporisateur Tbcc1, avertit l'entité de gestion des ressources grâce à la primitive de confirmation MDU-BCC (affectation) et passe à l'état "Bcc zéro".

Si le temporisateur Tbcc1 expire une première fois avant réception du message ALLOCATION COMPLETE ou du message ALLOCATION REJECT (rejet d'affectation), le commutateur local retransmet le message ALLOCATION, relance le temporisateur Tbcc1 et reste dans l'état "Bcc en attente d'affectation".

Si le temporisateur Tbcc1 expire une seconde fois avant réception du message ALLOCATION COMPLETE ou du message ALLOCATION REJECT, le processus doit s'achever en passant à l'état "Bcc zéro". L'événement est signalé également à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication d'erreur d'affectation), afin que les opérations de maintenance appropriées soient exécutées.

17.5.3 Affectation de canal support – Procédures exceptionnelles

17.5.3.1 Affectation de canal support

Si l'entité de protocole BCC du commutateur local est dans l'état ZÉRO et reçoit un message ALLOCATION COMPLETE (affectation achevée), elle informe la gestion des ressources en envoyant une primitive MDU-BCC (confirmation d'affectation) et reste dans l'état ZÉRO. Cette situation peut se produire à la suite de la perte de messages ou d'une expiration de temporisation de couche 3 mais avec retransmission du message par la couche 2. Il appartient à la gestion des ressources d'effectuer les opérations nécessaires.

17.5.3.2 Rejet d'affectation de canal support

Si l'entité de commande du réseau d'accès reçoit le message ALLOCATION et si la gestion des ressources du réseau d'accès s'aperçoit que le ou les intervalles de temps V5 ne peuvent pas être affectés au point d'accès identifié (ni à l'intervalle de temps de point d'accès utilisateur le cas échéant) dans les conditions demandées, l'entité de gestion des ressources génère une primitive MDU-BCC [réponse (rejet) d'affectation] et le réseau d'accès signale l'événement en envoyant au commutateur local le message ALLOCATION REJECT spécifiant dans l'élément d'information Cause de rejet la raison du rejet.

A la réception d'un message ALLOCATION REJECT que, par analyse de l'élément d'information Numéro de référence BCC, le commutateur local considère comme étant la réponse à un message ALLOCATION envoyé auparavant, il met fin au processus d'affectation de canal support, arrête le temporisateur Tbcc1, avertit l'entité de gestion des ressources grâce à la primitive d'indication MDU-BCC (rejet d'affectation) et passe à l'état "Bcc zéro".

Si l'entité de protocole BCC du commutateur local est dans l'état ZÉRO et reçoit un message ALLOCATION REJECT (rejet d'affectation), elle informe la gestion des ressources en envoyant une primitive MDU-BCC (indication de rejet d'affectation) et reste dans l'état ZÉRO. Cette situation peut se produire suite à la perte de messages ou d'expiration des temporisations de couche 3 mais de retransmission du message par la couche 2. Il appartient à la gestion des ressources d'effectuer les opérations nécessaires.

17.5.3.3 Abandon d'affectation de canal support

Si l'entité de protocole BCC du commutateur local est en attente de réception d'un message ALLOCATION COMPLETE (affectation achevée) ou ALLOCATION REJECT (rejet d'affectation) et si cette entité reçoit une primitive MDU-BCC (demande de désaffectation) demandant la libération du canal support en cours d'établissement (par exemple, à la suite d'une libération d'appel prématurée), le commutateur local poursuit la désaffectation de canal support, arrête le temporisateur Tbcc1, envoie le message DE-ALLOCATION (désaffectation), lance le temporisateur Tbcc2 et passe à l'état "abandon d'affectation Bcc".

Lorsqu'il est dans l'état "abandon d'affectation Bcc", le commutateur local ignore tout message ALLOCATION COMPLETE ou ALLOCATION REJECT reçu.

Si l'entité de protocole BCC du réseau d'accès reçoit le message DE-ALLOCATION, l'événement est signalé à l'entité de gestion des ressources à l'aide d'une primitive MDU-BCC (indication de désaffectation), puis le réseau d'accès désaffecte le ou les intervalles de temps V5 spécifiés du point d'accès approprié et envoie au commutateur local le message DE-ALLOCATION COMPLETE (désaffectation achevée).

A la réception d'un message DE-ALLOCATION COMPLETE que, par analyse de l'élément d'information Numéro de référence BCC, l'entité de commande BCC du commutateur local considère comme étant la réponse à un message DE-ALLOCATION envoyé auparavant, elle signale l'événement à l'entité de gestion des ressources du commutateur local à l'aide d'une primitive MDU-BCC (confirmation de désaffectation), puis arrête le temporisateur Tbcc2 et passe à l'état "Bcc zéro".

Si le temporisateur Tbcc2 expire une première fois avant réception du message DE-ALLOCATION COMPLETE (désaffectation achevée) ou du message DE-ALLOCATION REJECT (rejet de désaffectation), le commutateur local retransmet le message DE-ALLOCATION, relance le temporisateur Tbcc2 et reste dans l'état "abandon d'affectation Bcc".

Si le temporisateur Tbcc2 expire une seconde fois avant réception du message DE-ALLOCATION COMPLETE ou du message DE-ALLOCATION REJECT, la procédure doit s'achever en passant à l'état "Bcc zéro". L'événement est signalé également à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication d'erreur de désaffectation), afin que les opérations de maintenance appropriées soient effectuées.

17.5.3.4 Demande d'affectation de canal support reçue pour une connexion préexistante

Si l'entité de gestion des ressources du réseau d'accès reçoit un message ALLOCATION demandant une affectation de canal support déjà établie, le réseau d'accès envoie un message ALLOCATION COMPLETE (affectation achevée).

17.5.3.5 Affectation de canal support, suppression de connexion demandée

Dans certaines conditions de service, (comme par exemple, à la suite d'une négociation d'intervalle de temps de point d'accès utilisateur avec le système DSS1 à l'interface utilisateur-réseau du RNIS appelée), le commutateur local lance un processus d'affectation de canal support BCC sur l'intervalle de temps V5 de l'interface V5.2 qui participe déjà à une connexion au même point d'accès utilisateur. Le commutateur local signale la demande au moyen d'un champ indicateur de suppression contenant l'élément d'information Identification d'intervalle de temps V5 du message ALLOCATION (affectation) envoyé.

A la réception d'un message ALLOCATION contenant une demande de suppression, le réseau d'accès achève l'établissement du canal support en supprimant la connexion précédente et en envoyant un message ALLOCATION COMPLETE conformément à la procédure normale d'affectation du canal support décrite au 17.5.2. Dans le cas où le commutateur local demande la suppression d'une connexion incomplète au point d'accès utilisateur spécifié dans le message ALLOCATION, le réseau d'accès rejette la procédure en envoyant un message ALLOCATION REJECT conformément à la procédure de rejet d'affectation de canal support décrite au 17.5.3.2.

17.5.4 Désaffectation de canal support – Procédure normale

L'entité de gestion des ressources du commutateur local signale qu'il est nécessaire de désaffecter un canal support à l'aide d'un primitive MDU-BCC (demande de désaffectation). Puis l'entité de protocole BCC du commutateur local, qui est dans l'état "Bcc zéro", lance la désaffectation de canal support en envoyant au réseau d'accès un message DE-ALLOCATION (désaffectation) indiquant le ou les intervalles de temps V5 de l'interface V5.2 qui doivent être libérés.

A l'envoi du message DE-ALLOCATION, le commutateur local lance le temporisateur Tbcc3 et passe à l'état "Bcc en attente de désaffectation".

Lorsque l'entité de protocole BCC du réseau d'accès reçoit le message DE-ALLOCATION, elle signale l'événement à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication de désaffectation). Le réseau d'accès désaffecte ensuite le ou les intervalles de temps V5 spécifiés du point d'accès approprié et envoie au commutateur local le message DE-ALLOCATION COMPLETE (désaffectation achevée).

A la réception d'un message DE-ALLOCATION COMPLETE que, par analyse de l'élément d'information Numéro de référence BCC, l'entité de protocole BCC du commutateur local considère comme étant la réponse à un message DE-ALLOCATION (désaffectation) envoyé auparavant, l'événement est signalé à l'aide d'une primitive MDU-BCC (confirmation de désaffectation) puis le commutateur local arrête le temporisateur Tbcc3 et passe à l'état "Bcc zéro".

Si le temporisateur Tbcc3 expire une première fois avant réception du message DE-ALLOCATION COMPLETE (désaffectation achevée) ou du message DE-ALLOCATION REJECT, le commutateur local retransmet le message DE-ALLOCATION, relance le temporisateur Tbcc3 et reste dans l'état "Bcc en attente de désaffectation".

Si le temporisateur Tbcc3 expire une seconde fois avant réception du message DE-ALLOCATION COMPLETE ou du message DE-ALLOCATION REJECT, la procédure est abandonnée et le système passe à l'état "Bcc zéro". L'événement est signalé également à l'entité de gestion des ressources grâce à une primitive MDU-BCC (erreur de désaffectation), afin que les opérations de maintenance appropriées soient effectuées.

17.5.5 Désaffectation de canal support – Procédures exceptionnelles

17.5.5.1 Désaffectation de canal support

Si l'entité de protocole BCC du commutateur local est dans l'état ZÉRO et qu'elle reçoit un message DE-ALLOCATION COMPLETE, elle informe la gestion des ressources en envoyant une primitive MDU-BCC (confirmation de désaffectation) et reste dans l'état ZÉRO. Cette situation peut se produire à la suite de la perte de messages d'expiration de temporisations de couche 3 mais retransmission du message par la couche 2. Il appartient à la gestion des ressources d'effectuer les opérations nécessaires.

17.5.5.2 Rejet de désaffectation de canal support

A la réception d'un message DE-ALLOCATION, si l'entité de gestion des ressources du réseau d'accès s'aperçoit que le ou les intervalles de temps V5 demandés ne peuvent être désaffectés du point d'accès identifié (ni de l'intervalle de temps de point d'accès utilisateur le cas échéant) ou ne peuvent pas l'être dans les conditions demandées par le commutateur local, elle génère une primitive MDU-BCC [réponse (rejet) de désaffectation] et le réseau d'accès signale l'événement en envoyant au commutateur local un message DE-ALLOCATION REJECT spécifiant dans l'élément d'information Cause de rejet la raison de ce rejet.

A la réception d'un message DE-ALLOCATION REJECT que, par analyse de l'élément d'information Numéro de référence BCC, l'entité de protocole BCC du commutateur local considère comme étant la réponse à un message DE-ALLOCATION envoyé auparavant, le commutateur local met fin à la procédure de désaffectation de canal support, arrête le temporisateur Tbcc3, avertit l'entité de gestion des ressources grâce à la primitive MDU-BCC (indication de rejet de désaffectation) et passe à l'état "Bcc zéro".

Si l'entité de protocole BCC du commutateur local est dans l'état ZERO et qu'elle reçoit un message DE-ALLOCATION REJECT, elle informe la gestion des ressources en envoyant une primitive MDU-BCC (indication de rejet de désaffectation) et reste dans l'état ZERO. Cette situation peut se produire suite à la perte de messages ou à l'expiration de temporisations de couche 3 mais retransmission du message par la couche 2. Il appartient à la gestion des ressources d'effectuer les opérations nécessaires.

17.5.5.3 Message manquant de processus de désaffectation de canal support

Si l'entité de gestion des ressources du réseau d'accès reçoit un message DE-ALLOCATION concernant un intervalle de temps V5 et un point d'accès (et un intervalle de temps de point d'accès le cas échéant) considéré comme étant libre, le réseau d'accès envoie un message DE-ALLOCATION COMPLETE.

17.5.6 Procédure d'analyse (audit)

Si l'entité de protocole BCC du commutateur local est dans l'état "Bcc zéro" et reçoit une primitive MDU-BCC (demande d'analyse), elle lance la procédure d'analyse en envoyant au réseau d'accès un message AUDIT indiquant l'intervalle de temps V5 simple à 64 kbit/s ou le cas échéant, le point d'accès et l'intervalle de temps de point d'accès sur lequel l'analyse doit être réalisée.

A l'envoi du message AUDIT, le commutateur local lance le temporisateur Tbcc4 et passe à l'état "Bcc en attente d'analyse".

Lorsque l'entité de protocole BCC du réseau d'accès reçoit le message AUDIT, elle signale l'événement à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication d'analyse). Le gestionnaire des ressources du réseau d'accès doit ensuite mettre en regard les informations reçues avec ses propres informations concernant les connexions de canaux supports établies dans le réseau d'accès. Après cette vérification, le réseau d'accès informe le commutateur local de l'existence de la connexion support correspondant aux informations fournies par ce dernier ou de l'absence de cette connexion. Après réception de la primitive MDU-BCC (réponse d'analyse), l'entité de protocole BCC du réseau d'accès envoie au commutateur local le message AUDIT COMPLETE (analyse terminée).

A la réception d'un message AUDIT COMPLETE que, par analyse de l'élément d'information Numéro de référence BCC, le commutateur local considère comme étant la réponse à un message AUDIT envoyé auparavant, il arrête le temporisateur Tbcc4, avertit l'entité de gestion des ressources grâce à la primitive MDU-BCC (confirmation d'analyse) et passe à l'état "Bcc zéro".

Si le temporisateur Tbcc4 expire une première fois avant réception du message AUDIT COMPLETE, le commutateur local retransmet le message AUDIT, relance le temporisateur Tbcc4 et reste dans l'état "Bcc en attente d'analyse".

Si le temporisateur Tbcc4 expire une seconde fois avant réception du message AUDIT COMPLETE, le processus doit se terminer en passant à l'état "Bcc zéro". L'événement est signalé également à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication d'erreur d'analyse), afin que les opérations de maintenance appropriées soient effectuées.

17.5.7 Procédure de notification d'anomalie interne au réseau d'accès

Si l'entité de protocole BCC du réseau d'accès est dans l'état "Bcc opérationnelle" et reçoit une primitive MDU-BCC (demande d'anomalie AN), elle lance la procédure de notification d'anomalie interne au réseau d'accès en envoyant au commutateur local un message AN FAULT (anomalie de réseau d'accès) indiquant la connexion support à 64 kbit/s affectée par l'anomalie interne d'AN, spécifiant l'intervalle de temps V5, ou le cas échéant, le point d'accès utilisateur ou l'intervalle de temps de point d'accès, ou les deux.

A l'envoi du message AN FAULT, le réseau d'accès lance le temporisateur Tbcc5 et passe à l'état "rapport d'anomalie Bcc dans le réseau d'accès".

Lorsque l'entité de protocole BCC du commutateur local reçoit le message AN FAULT, elle signale l'événement à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication d'anomalie AN) et envoie au réseau d'accès le message AN FAULT ACKNOWLEDGE (accusé de réception d'anomalie AN).

A la réception d'un message AN FAULT ACKNOWLEDGE que, par analyse de l'élément d'information Numéro de référence BCC, le réseau d'accès considère comme étant la réponse à un message AN FAULT envoyé auparavant, il arrête le temporisateur Tbcc5, avertit l'entité de gestion des ressources grâce à la primitive MDU-BCC (confirmation d'anomalie AN) et passe à l'état "Bcc opérationnel".

Si le temporisateur Tbcc5 expire une première fois avant réception du message AN FAULT ACKNOWLEDGE, le réseau d'accès retransmet le message AN FAULT, relance le temporisateur Tbcc5 et reste dans l'état "rapport d'anomalie Bcc dans le réseau d'accès".

Si le temporisateur Tbcc5 expire une seconde fois avant réception du message AN FAULT ACKNOWLEDGE, le processus se termine et on passe à l'état "Bcc opérationnelle". L'événement est signalé également à l'entité de gestion des ressources grâce à une primitive MDU-BCC (indication d'erreur anomalie AN), afin que les opérations de maintenance appropriées soient effectuées.

17.5.8 Traitement des situations d'erreur

Avant de réagir à un message, l'entité de réception, c'est-à-dire l'entité de protocole BCC d'interface V5.2 du réseau d'accès ou du commutateur local exécute les procédures spécifiées dans le présent sous-paragraphe.

En règle générale, tous les messages contiennent au moins les éléments d'information suivants: Discriminateur de protocole, Numéro de référence BCC et Type de message. Ces éléments qui font office d'en-tête pour tous les messages BCC, sont spécifiés au 13.2. Lorsqu'elle reçoit un message comportant moins de 4 octets, l'entité de protocole destinataire du réseau d'accès ou du commutateur local envoi à la gestion-systèmes une primitive MDU-BCC (indication d'erreur de protocole) et ignore le message.

Si plus de 3 éléments d'information facultatifs sont détectés dans un message, alors celui-ci est considéré comme étant trop long et doit être tronqué après le troisième élément d'information facultatif. On suppose que tous les éléments d'information tronqués sont des éléments d'information facultatifs répétés. En effectuant la troncature, l'entité réagit aux éléments d'information répétés conformément au 17.5.8.4.

Chaque réception d'un message, de l'ensemble des messages du protocole BCC, active les vérifications décrites aux 17.5.8.1 à 17.5.8.10 par ordre de préséance. Aucune transition d'état n'a lieu au cours de ces vérifications.

Après vérification du message par les procédures de traitement d'erreur décrites dans la suite du paragraphe, si le message ne doit pas être ignoré, les procédures suivantes se déroulent alors:

– procédures d'affectation de canal support (voir 17.5.2 et 17.5.3);
– procédures de désaffectation de canal support (voir 17.5.4 et 17.5.5);
– procédure d'analyse (voir 17.5.6);
– procédure de notification d'anomalie interne au réseau d'accès (voir 17.5.7).

NOTE – Dans le présent paragraphe, le terme "ignorer le message" signifie ne pas en modifier le contenu.

17.5.8.1 Erreur de discriminateur de protocole

Si un message est reçu par l'entité de protocole BCC de couche 3 et que le discriminateur de protocole est codé conformément aux spécifications du 13.2.1 pour l'utilisation dans les protocoles V5:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion système, ignore le message et envoie un message PROTOCOL ERROR (erreur de protocole) indiquant la cause d'erreur de protocole "erreur de discriminateur de protocole";
– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

17.5.8.1a Erreur de codage de numéro de référence BCC

Si un message est reçu par l'entité de protocole BCC de couche 3 avec un Numéro de référence BCC codé différemment de ce qui est spécifié au paragraphe 17.4.1, alors:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion système, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "erreur de codage de numéro de référence BCC";
– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

17.5.8.2 Erreur de type de message

Chaque fois qu'un message non reconnu est reçu:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "type de message non reconnu" comprenant le diagnostic approprié spécifié par le 17.4.2.6;
– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

17.5.8.3 Elément d'information Hors séquence

Un élément d'information dont la valeur de code d'identifiant est inférieure à la valeur de code de l'élément d'information précédent est considéré comme étant hors séquence.

Chaque fois qu'un élément d'information Hors séquence est reçu:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime l'élément d'information Hors séquence et continue à traiter le message; elle envoie également un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information hors séquence" comprenant le diagnostic correspondant spécifié par le 17.4.2.6;
– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime l'élément d'information Hors séquence et continue à traiter le message.

Si l'élément d'information supprimé est obligatoire, cela se traduit par une situation d'erreur Elément d'information obligatoire manquant qui est traitée conformément au 17.5.8.5.

17.5.8.4 Eléments d'information obligatoires répétés

Chaque fois qu'un élément d'information obligatoire est répété dans un message, l'entité destinataire doit réagir de la manière suivante:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "Elément d'information obligatoire répété" comprenant le diagnostic approprié spécifié par le 17.4.2.6;

– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

NOTE – Le présent paragraphe s'applique aussi aux éléments d'information conditionnels qui doivent être traités comme des éléments d'information obligatoires (messages ALLOCATION et DE-ALLOCATION).

17.5.8.4a Eléments d'information facultatifs répétés

Chaque fois qu'un élément d'information facultatif est répété dans un message, l'entité de réception doit réagir de la manière suivante:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime l'élément d'information facultatif répété et continue à traiter le message; elle envoie également un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information facultatif répété" comprenant le diagnostic approprié spécifié par le 17.4.2.6;

– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime l'élément d'information facultatif répété et continue à traiter le message.

17.5.8.5 Elément d'information obligatoire manquant

Chaque fois qu'un élément d'information obligatoire manque dans un message, l'entité de réception doit réagir de la manière suivante:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information obligatoire manquant" comprenant le diagnostic approprié spécifié par le 17.4.2.6;

– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

Si plusieurs éléments d'information obligatoires manquent, la réaction de l'entité de réception doit se fonder sur le premier élément d'information obligatoire manquant détecté.

NOTE – Le présent paragraphe s'applique aussi aux éléments d'information conditionnels qui doivent être traités comme des éléments d'information obligatoires (messages ALLOCATION et DE-ALLOCATION).

17.5.8.6 Elément d'information non reconnu

Chaque fois qu'un message reçu contient un ou plusieurs éléments d'information non reconnus, l'entité de récepteur doit réagir de la manière suivante:

– l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime tous les éléments d'information non reconnus et poursuit le traitement du message; elle envoie également un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information non reconnu" comprenant le diagnostic correspondant spécifié par le 17.4.2.6;

– l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime tous les éléments d'information non reconnus et poursuit le traitement du message.

Dans le cas où plusieurs éléments d'information ne sont pas reconnus, la réaction de l'entité de réception doit se fonder sur le premier élément d'information non reconnu détecté.

En ce qui concerne les procédures de traitement des erreurs de protocole BCC, les éléments d'information non reconnus sont ceux qui ne sont pas définis aux 13.2 et 17.4.

17.5.8.7 Erreur de contenu d'élément d'information obligatoire

Si un message reçu contient un élément d'information obligatoire dont le contenu est erroné:

a) soit que la longueur ne soit pas conforme aux spécifications des 13.2 et 17.4;

b) soit que le contenu ne soit pas reconnu; alors:

- l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "erreur de contenu d'élément d'information obligatoire" comprenant le diagnostic approprié spécifié par le 17.4.2.6;
- l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

NOTE – Le présent paragraphe s'applique aussi aux éléments d'information conditionnels qui doivent être traités comme des éléments d'information obligatoires (messages ALLOCATION et DE-ALLOCATION).

17.5.8.8 Erreur de contenu d'élément d'information facultatif

Si un message reçu contient un élément d'information facultatif dont le contenu est erroné:

a) soit que la longueur ne soit pas conforme aux spécifications du 17.4;

b) soit que le contenu ne soit pas reconnu; alors:

- l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime l'élément d'information dont le contenu est erroné et poursuit le traitement du message; elle envoie également un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "erreur de contenu d'élément d'information facultatif" comprenant le diagnostic approprié spécifié par le 17.4.2.6;
- l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, supprime l'élément d'information dont le contenu est erroné et poursuit le traitement du message.

17.5.8.9 Message non attendu

Lorsqu'un message non attendu est reçu, il se produit une erreur de flux de message. Les tables des transitions d'état indiquent les mesures à prendre à la réception d'un événement quelconque.

Lorsqu'un message non attendu est reçu, il ne se produit pas de transition d'état, alors:

- l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "message incompatible avec l'état du protocole BCC", comprenant le diagnostic correspondant spécifié par le 17.4.2.6;
- l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

17.5.8.10 Elément d'information facultatif non autorisé

Lorsqu'un message contenant plus d'éléments d'information facultatifs que nécessaire est reçu, alors:

- l'entité de protocole BCC du réseau d'accès envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "éléments d'information trop nombreux" comprenant le diagnostic correspondant spécifié par le 17.4.2.6;
- l'entité de protocole BCC du commutateur local envoie une primitive MDU-BCC (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

17.6 Liste des paramètres système (temporisateurs)

Le Tableau 46 définit les temporisateurs utilisés par le protocole BCC. Les temporisateurs mentionnés sont entretenus par l'entité de protocole BCC du commutateur local ou du réseau d'accès. La tolérance sur les temporisations est de ±10%.

Tableau 46/G.965 – Temporisateurs de protocole BCC

Numéro du temporisateur	Durée	Etat	Cause de déclenchement	Arrêt normal	Opérations lors de la première expiration	Opérations lors de la seconde expiration	Référence
Tbcc1	0,5 à 30 s (Note)	LE Bcc0 LE Bcc1	Message ALLOCATION envoyé	Après réception d'un message ALLOCATION COMPLETE, ALLOCATION REJECT, ou d'une demande d'interruption d'affectation	Répéter le message ALLOCATION et relancer Tbcc1	Terminer le processus d'affectation et le signaler à la gestion des ressources	17.5.2
Tbcc2	2 s	LE Bcc1 LE Bcc2	Message DE-ALLOCATION envoyé	Après réception d'un message DE-ALLOCATION COMPLETE ou DE-ALLOCATION REJECT	Répéter le message DE-ALLOCATION et relancer Tbcc2	Terminer le processus de désaffectation et le signaler à la gestion des ressources	17.5.3
Tbcc3	2 s	LE Bcc0 LE Bcc3	Message DE-ALLOCATION envoyé	Après réception d'un message DE-ALLOCATION COMPLETE ou DE-ALLOCATION REJECT	Répéter le message DE-ALLOCATION et relancer Tbcc3	Terminer le processus de désaffectation et le signaler à la gestion des ressources	17.5.4
Tbcc4	500 à 1500 ms (Note)	LE Bcc0 LE Bcc4	Message AUDIT envoyé	Après réception d'un message AUDIT COMPLETE	Répéter le message AUDIT et relancer Tbcc4	Terminer le processus d'analyse et le signaler à la gestion des ressources	17.5.6
Tbcc5	500 à 1500 ms (Note)	AN Bcc0 AN Bcc1	Message AN FAULT envoyé	Après réception d'un message AN FAULT ACKNOWLEDGE	Répéter le message AN FAULT et relancer Tbcc5	Terminer le processus d'anomalie interne AN et le signaler à la gestion des ressources	17.5.7
NOTE – La somme des valeurs de Tbcc1 et du temporisateur T1 du protocole RTPC de V5.1 ne doit pas dépasser 30 s. La valeur par défaut de Tbcc1 doit être 1500 ms.							

17.7 Tables de transition d'état côté commutateur local et côté réseau d'accès

Le Tableau 47 définit la table des transitions d'état pour un processus, côté commutateur local de l'entité de protocole BCC de l'interface V5.2.

Tableau 47/G.965 – Tables de transition d'état côté commutateur local

Etat / Evénement	Bcc zéro (LEBcc0)	Bcc en attente d'affectation (LEBcc1)	Abandon d'affectation Bcc (LEBcc2)	Bcc en attente de désaffectation (LEBcc3)	Bcc en attente d'analyse (LEBcc4)
MDU-BCC (demande d'affectation)	ALLOCATION; lancer Tbcc1; LEBcc1; –	/	/	/	/
ALLOCATION COMPLETE	MDU-BCC (confirmation d'affectation); –	MDU-BCC (confirmation d'affectation); arrêter Tbcc1; LEBcc0	–	/	/
ALLOCATION REJECT	MDU-BCC (indication de rejet d'affectation); –	MDU-BCC (indication de rejet d'affectation); arrêter Tbcc1; LEBcc0	–	/	/
MDU-BCC (demande de désaffectation)	DE-ALLOCATION; lancer Tbcc3; LEBcc3	DE-ALLOCATION; arrêter Tbcc1; lancer Tbcc2; LEBcc2	/	/	/
DE-ALLOCATION COMPLETE	MDU-BCC (confirmation de désaffectation); –	/	MDU-BCC (confirmation de désaffectation); arrêter Tbcc2; LEBcc0	MDU-BCC (confirmation de désaffectation); arrêter Tbcc3; LEBcc0	/
DE-ALLOCATION REJECT	MDU-BCC (indication de rejet de désaffectation); –	/	MDU-BCC (indication de rejet de désaffectation); arrêter Tbcc2; LEBcc0	MDU-BCC (indication de rejet de désaffectation); arrêter Tbcc3; LEBcc0	/
MDU-BCC (demande d'analyse)	AUDIT; lancer Tbcc4; LEBcc4	/	/	/	/
AUDIT COMPLETE	/	/	/	/	MDU-BCC (confirmation d'analyse); arrêter Tbcc4; LEBcc0
Expiration Tbcc1 (première)	/	ALLOCATION; relancer Tbcc1; –	/	/	/
Expiration Tbcc1 (seconde)	/	MDU-BCC (indication d'erreur d'affectation); LEBcc0	/	/	/
Expiration Tbcc2 (première)	/	/	DE-ALLOCATION; relancer Tbcc2; –	/	/
Expiration Tbcc2 (seconde)	/	/	MDU-BCC (indication d'erreur de désaffectation); LEBcc0	/	/
Expiration Tbcc3 (première)	/	/	/	DE-ALLOCATION; relancer Tbcc3; –	/
Expiration Tbcc3 (seconde)	/	/	/	MDU-BCC (indication d'erreur de désaffectation); LEBcc0	/

Tableau 47/G.965 – Tables de transition d'état côté commutateur local

Etat / Evénement	Bcc zéro (LEBcc0)	Bcc en attente d'affectation (LEBcc1)	Abandon d'affectation Bcc (LEBcc2)	Bcc en attente de désaffectation (LEBcc3)	Bcc en attente d'analyse (LEBcc4)
Expiration Tbcc4 (première)	/	/	/	/	AUDIT; relancer Tbcc4; –
Expiration Tbcc4 (seconde)	/	/	/	/	MDU-BCC (indication d'erreur d'analyse); LEBcc0
AN FAULT	AN FAULT ACK; MDU-BCC (indication d'anomalie AN); –	/	/	/	/
PROTOCOL ERROR	/	MDU-BCC (indication d'erreur de protocole); arrêter Tbcc1; LEBcc0	MDU-BCC (indication d'erreur de protocole); arrêter Tbcc2; LEBcc0	MDU-BCC (indication d'erreur de protocole); arrêter Tbcc3; LEBcc0	MDU-BCC (indication d'erreur de protocole); arrêter Tbcc4; LEBcc0

– Un tiret indique l'absence de transition d'état

/ Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état

Le Tableau 48 définit la table des transitions d'état pour un processus, côté réseau d'accès de l'entité de protocole BCC de l'interface V5.2.

Tableau 48/G.965 – Tables des transitions d'état côté réseau d'accès

Etat / Evénement	Bcc opérationnel (ANBcc0)	Rapport d'anomalie BCC dans le réseau d'accès (ANBcc1)
ALLOCATION	MDU-BCC (indication d'affectation); ANBcc0	/
MDU-BCC [réponse d'affectation (achevée)]	ALLOCATION COMPLETE; ANBcc0	/
MDU-BCC [réponse d'affectation (rejet)]	ALLOCATION REJECT; ANBcc0	/
DE-ALLOCATION	MDU-BCC (indication de désaffectation); ANBcc0	/
MDU-BCC [réponse de désaffectation (achevée)]	DE-ALLOCATION COMPLETE; ANBcc0	/
MDU-BCC [réponse de désaffectation (rejet)]	DE-ALLOCATION REJECT; ANBcc0	/
AUDIT	MDU-BCC (indication d'audit); ANBcc0	/
MDU-BCC (réponse d'analyse)	AUDIT COMPLETE; ANBcc0	/
MDU-BCC (demande d'anomalie AN)	AN FAULT, lancer Tbcc5; ANBcc1	/

Tableau 48/G.965 – Tables des transitions d'état côté réseau d'accès

Etat / Evénement	Bcc opérationnel (ANBcc0)	Rapport d'anomalie BCC dans le réseau d'accès (ANBcc1)
AN FAULT ACKNOWLEDGE	/	MDU-BCC (confirmation d'anomalie AN), Arrêter Tbcc5; ANBcc0
Expiration Tbcc5 (première)	/	AN FAULT, relancer Tbcc5; ANBcc1
Expiration Tbcc5 (seconde)	/	MDU-BCC (indication d'anomalie AN); ANBcc0
– Un tiret indique l'absence de transition d'état / Une barre oblique indique un événement intempestif qui ne provoque pas de transition d'état		

18 Spécifications du protocole de protection

18.1 Généralités

18.1.1 Introduction

Une interface V5.2 simple peut comporter jusqu'à seize (16) liaisons à 2048 kbit/s. Selon l'architecture de protocole et la structure de multiplexage (voir paragraphe 8), un trajet de communication peut acheminer des informations associées à plusieurs liaisons à 2048 kbit/s (transfert d'informations non associé). Une anomalie de fonctionnement dans un trajet de communication pourrait donc altérer de façon inacceptable le service offert à de nombreux abonnés. Ceci vaut en particulier pour le protocole BCC, le protocole de commande et le protocole de commande de liaison où tous les points d'accès utilisateur sont touchés en cas d'anomalie dans le trajet de communication correspondant.

Des mécanismes de protection sont prévus pour la commutation de trajets de communication défaillants, afin d'améliorer la fiabilité de l'interface V5.2.

Les mécanismes de protection serviront à protéger toutes les voies C actives. Ils protégeront également le trajet C du protocole de protection (proprement dit) utilisé pour la commande des procédures de commutation de protection.

Le protocole de protection ne protège pas les canaux supports et ne permet pas la reconfiguration des canaux supports si la liaison à 2048 kbit/s qui leur est associée présente une anomalie de fonctionnement. En pareil cas, les liaisons d'abonné établies sur ces canaux supports présenteront elles aussi des anomalies de fonctionnement, ce qui est considéré comme acceptable car des anomalies de ce genre devraient être relativement rares. Il faut avant tout se protéger contre des anomalies de fonctionnement dans des liaisons à 2048 kbit/s. Le protocole de protection protégera aussi contre des anomalies répétées de liaisons de données V5 (c'est-à-dire une anomalie persistante sur une des liaisons de données pour le protocole de commande, le protocole de commande de liaison, le protocole BCC, le protocole RTPC ou le protocole de protection). Les drapeaux doivent par ailleurs être surveillés en permanence sur toutes les voies C physiques (voies C actives et voies C en attente) pour se protéger contre des anomalies que les mécanismes de détection de la couche 1 n'ont pas déjà repérées.

Si une anomalie est détectée sur une voie C en attente, la gestion-systèmes en est informée et ne commutera pas en conséquence une voie C logique sur cette voie C en attente non opérationnelle. Les autres anomalies d'équipement (dans d'autres couches, à l'intérieur du réseau d'accès ou du commutateur local) seront traitées une à une, selon l'implémentation particulière; elles ne relèvent pas des spécifications de l'interface V5.

Aucune protection ne sera prévue pour les voies C logiques dans le cas d'une liaison simple à 2048 kbit/s, ce qui signifie qu'il n'y aura pas de protocole de protection dans l'intervalle de temps 16 ou sur toute autre voie C physique et que la liaison de données nécessaire pour la protection ne sera pas établie pendant la phase de démarrage du système.

La mise en œuvre d'une procédure de commutation de protection peut entraîner la perte de messages de couche 2 et/ou de couche 3. Il appartient aux entités de protocole de couche 3 concernées de faire face à ces situations.

Le présent paragraphe énonce les principes et les spécifications du protocole de protection.

18.1.2 Profilage de voies C physiques et voies C logiques

Les mappages trajet C – voies C logiques sont profilés dans le commutateur local et le réseau d'accès.

Les mappages initiaux voies C logiques – voies C physiques sont profilés dans le commutateur local et le réseau d'accès.

Les deux trajets C du protocole de protection sont toujours profilés dans les intervalles de temps 16 des liaisons primaire et secondaire et ne sont pas commutés par le mécanisme de protection.

Les trajets C du protocole de commande, du protocole de commande de liaison et du protocole BCC commenceront dans l'intervalle de temps 16 de la liaison primaire. L'intervalle de temps 16 de la liaison secondaire servira à leur protection.

En mode transmission de trames, les messages du protocole de protection sont prioritaires sur d'autres messages acheminés sur la même voie C physique. La résolution des conflits se fonde sur l'adresse d'enveloppe, qui est identique pour tous les messages du protocole de protection et donne la priorité à l'adresse de fonction d'enveloppement = 8179.

Chaque interface V5.2 comprenant plusieurs liaisons à 2048 kbit/s se voit accorder un groupe de protection 1 et, si elle est profilée, un groupe de protection 2.

Le groupe de protection 1 se compose toujours de l'intervalle de temps 16 de la liaison primaire et de l'intervalle de temps 16 de la liaison secondaire. Ainsi, on utilise les valeurs fixées suivantes pour le groupe de protection 1 (se reporter aux définitions):

$N1 = 1$;

$K1 = 1$.

Si le groupe de protection 2 est profilé, N2 voies C logiques (et trajets C contenus) seront profilées et un groupe de K2 voies C en attente seront profilées avec:

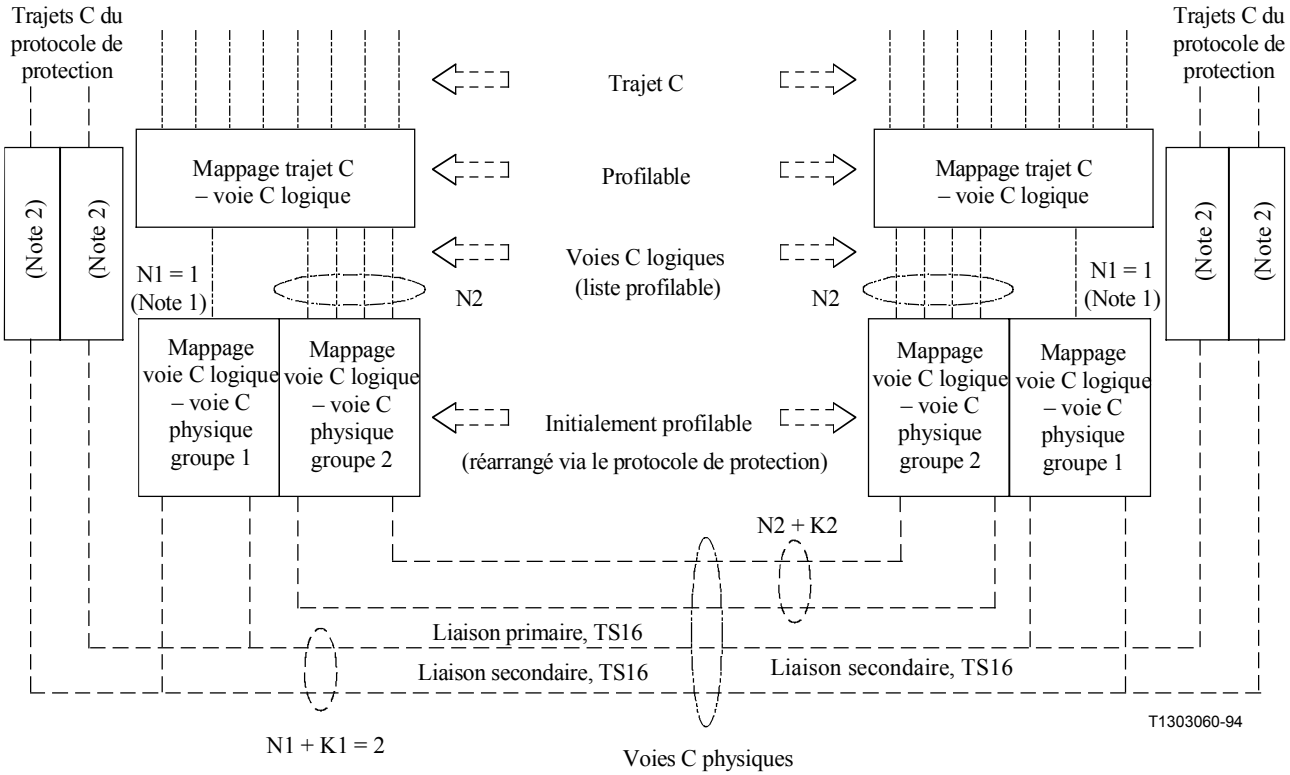
$1 \leq K2 \leq 3$;

$1 \leq N2 \leq (3 \times L - 2 - K2)$

où L est le nombre de liaisons à 2048 kbit/s sur l'interface V5.2. K2 est choisi de façon à ce qu'il soit égal ou supérieur au nombre maximal de voies C physiques sur une liaison à 2048 kbit/s simple de cette interface V5.2. Dans ce cas, les intervalles de temps 16 de la liaison primaire et de la liaison secondaire ne sont pas pris en compte. Toutes les voies C actives peuvent ainsi être protégées en cas d'anomalie sur une liaison à 2048 kbit/s simple.

NOTE – Il se peut que l'exploitant de réseau ne profile aucune voie C en attente pour le groupe de protection 2 (K2 = 0) si aucune protection n'est nécessaire pour les voies C logiques du groupe de protection 2, mais dans ce cas, certaines anomalies sur des liaisons à 2048 kbit/s simples peuvent avoir des conséquences sur les services associés aux voies C logiques défaillantes.

La Figure 25 illustre le mappage trajets C – voies C logiques et trajets C – voies C physiques.



NOTE 1 – Trajets C du protocole de commande, du protocole de commande de liaison et du protocole BCC plus éventuellement d'autrets trajets C.

NOTE 2 – Affectation d'un trajet C à une voie C physique.

Figure 25/G.965 – Mappage trajets C – Voies C logiques puis voies C physiques

18.1.3 Séparation des responsabilités

Une commutation de protection peut être déclenchée de façon autonome par la gestion-systèmes du commutateur local ou du réseau d'accès après détection d'une anomalie ou à la suite d'une procédure de blocage de liaison, soit par le ou les exploitants via les interfaces Q_{CL} et Q_{AN}. Pour le groupe de protection 1, la gestion-systèmes ne permet pas que la commutation soit lancée par le ou les exploitants via les interfaces Q_{AN} ou Q_{CL}.

Le commutateur local régit la commutation de protection, en ce sens qu'il affecte une autre voie C physique à la voie C logique considérée.

Le réseau d'accès peut demander à tout moment la commutation d'une voie C logique. Si cette commutation a été lancée par l'exploitant du réseau d'accès via l'interface Q_{AN}, l'exploitant peut demander la commutation sur une voie C physique préférée. Le commutateur local doit, si possible, satisfaire à la demande. Si le réseau d'accès n'indique aucune préférence (ce qui est toujours le cas si une anomalie est détectée dans le réseau d'accès et si une commutation autonome est lancée par la gestion-systèmes du réseau d'accès) la gestion-systèmes du commutateur local choisira une voie C en attente disponible.

Le réseau d'accès peut rejeter une commande de protection émanant du commutateur local, si pour une raison ou une autre il n'est pas en mesure d'y donner suite. S'ils ne peuvent pas donner suite à la demande, le commutateur local ou le réseau d'accès doivent en indiquer les causes via l'interface Q_{CL} et Q_{AN}.

18.1.4 Gestion des ressources de voie C après anomalie de fonctionnement

La gestion-systèmes du commutateur local décide quelle voie C physique sera utilisée pour protéger une voie C logique. Il convient de respecter les règles suivantes pour la gestion et le contrôle des ressources disponibles.

Si une commutation de protection est déclenchée de façon autonome par la gestion-systèmes du commutateur local ou du réseau d'accès après détection d'une anomalie, les voies C actives ne font pas l'objet d'une préemption pour protéger une autre voie C logique. Il en va de même pour une commutation lancée via l'interface Q_{AN}.

Seul l'exploitant du commutateur local (via l'interface Q_{CL}) peut demander l'affectation d'une voie C logique défaillante à une voie C active (voie C physique qui transporte déjà une voie C logique). Dans ce cas, une commande spécialisée est envoyée au réseau d'accès, lequel ne doit pas rejeter la commutation au motif qu'une voie C logique a déjà été affectée à cette voie C physique. Le réseau d'accès désaffecte les voies C logiques précédemment assignées et affecte les nouvelles voies C logiques qui doivent être protégées. La voie C logique désaffectée est ensuite protégée par le mécanisme de protection normal tant que des ressources sont disponibles. Ce mécanisme permet à l'exploitant du commutateur local de protéger manuellement des protocoles plus prioritaires (protocole RTPC par exemple) en cas d'anomalies de fonctionnement de liaisons à 2048 kbit/s multiples même lorsque le mécanisme de protection autonome n'a pas abouti faute de ressources (voies C en attente opérationnelles).

Lorsqu'une protection est requise, on choisit et on utilise une voie C en attente disponible du même groupe de protection. Si plusieurs voies C en attente sont disponibles, le gestionnaire de ressources procède comme suit: il utilise d'abord toutes les voies C en attente disponibles sur les intervalles de temps 16, puis les intervalles de temps 15 et enfin les intervalles de temps 31. Une fois la liaison rétablie, toutes les voies C physiques profilées sur cette liaison deviendront des voies C en attente (la commutation de protection n'est pas réversible).

De plus, le reprofilage permettrait d'imposer manuellement une priorité si une anomalie grave l'imposait (par exemple anomalie sur la liaison primaire ou la liaison secondaire). Les services pris en charge par l'interface V5 sont indisponibles pendant le reprofilage de l'interface V5 et la phase de démarrage du système. La priorité, imposée manuellement pendant le profilage initial, peut être modifiée après une commutation de protection, par exemple à la suite d'une anomalie sur une liaison à 2048 kbit/s.

En cas d'anomalie sur une liaison à 2048 kbit/s, le gestionnaire de ressources du protocole de gestion doit commuter tout d'abord la voie C logique dans le TS16, puis celle du TS15 et enfin celle du TS31, tant que des ressources restent disponibles. Si toutes les voies C logiques ne peuvent être commutées sur des voies C physiques, il faut en informer l'exploitant de réseau via l'interface Q_{CL} ou Q_{AN}.

En cas de perte de protection des trajets C des protocoles BCC, de commande et de commande de liaison, due à une anomalie sur la liaison primaire ou la liaison secondaire à 2048 kbit/s, il faut procéder à un reprofilage sur une autre liaison à 2048 kbit/s.

Les opérations de commutation doivent être séquentielles, c'est-à-dire qu'une seconde commutation n'est lancée qu'une fois la première achevée.

Un message de protocole de protection ne peut invoquer qu'une seule opération (par exemple, commutation d'une voie C logique X sur une voie C en attente Y).

Une demande de commutation émanant du réseau d'accès ou une commande de commutation émanant du commutateur local ne peuvent que faire l'objet d'un accusé de réception ou être rejetées par l'entité homologue. Le message de rejet ne doit pas contenir d'autres propositions de commutation. Une nouvelle opération de commutation peut être lancée par l'un ou l'autre côté, à la suite d'un rejet de commutation.

18.1.5 Fonctions de surveillance et détection des anomalies de fonctionnement

Il faut avant tout se protéger contre les anomalies de fonctionnement sur des liaisons à 2048 kbit/s.

Indépendamment de la surveillance de couche 1, on utilise deux autres fonctions de surveillance pour détecter des anomalies sur des voies C et déclencher une commutation de protection autonome. Ces deux fonctions sont la surveillance des drapeaux et la surveillance des liaisons de données.

18.1.5.1 Anomalie sur une liaison à 2048 kbit/s

A la réception d'une primitive MDU-DI émanant de la machine FSM de commande de liaison du réseau d'accès ou du commutateur local (voir 16.1), ou si la liaison est bloquée au réseau d'accès ou au commutateur local (voir 16.2), la gestion-systèmes du réseau d'accès ou du commutateur local déclenche une commutation autonome pour toutes les voies C actives sur cette liaison à 2048 kbit/s.

18.1.5.2 Surveillance des drapeaux

Les drapeaux sont surveillés en permanence sur les voies C actives et en attente.

Si aucun drapeau n'est reçu sur une voie C physique pendant une seconde, on considère que la voie C physique est non opérationnelle et une indication d'erreur est envoyée à la gestion-systèmes. Cette condition doit être signalée de façon continue, au débit d'une notification par seconde, à la gestion-systèmes tant que la situation perdure.

Si un drapeau au moins est reçu sur une voie C physique pendant une période d'une seconde, on considère que la voie C physique est opérationnelle.

18.1.5.3 Surveillance des liaisons de données

La surveillance de liaison de données (couche 2) sera utilisée dans le réseau d'accès et dans le commutateur local sur les voies transportant des trajets C où on trouve une liaison de données V5 complète aboutissant dans le réseau d'accès (c'est-à-dire protocoles de protection, de commande, de commande de liaison, BCC et RTPC).

Une anomalie de liaison de données (voir C.17), si elle n'est pas déjà traitée par les 18.1.5.1 et 18.1.5.2 respectivement, doit servir de déclencheur pour une commutation de protection.

Si la gestion-systèmes reçoit une autre primitive d'indication MDL-RELEASE à la suite d'une anomalie sur le trajet C qui a causé la commutation, la gestion-systèmes concernée ne lancera aucune autre commutation à moins qu'elle n'ait reçu dans l'intervalle une primitive d'indication MDL-ESTABLISH ou de confirmation MDL-ESTABLISH. Cela signifie que la machine FSM de la liaison de données du trajet C défaillant passe tout d'abord à l'état trame multiple établie (au moins une fois) avant qu'une deuxième commutation ne soit lancée, déclenchée par la réception d'une primitive d'indication MDL-RELEASE. En d'autres termes, on part du principe qu'il y a eu anomalie interne impossible à réparer avec le mécanisme de protection V5. Dans ce cas, la gestion-systèmes lance les actions qui s'imposent.

18.1.6 Modèle fonctionnel du protocole de protection

Une liaison de données indépendante sera établie en permanence sur chaque TS16 de la liaison primaire et de la liaison secondaire. Les modalités applicables à la couche liaison de données sont précisées au 10.4.

L'adresse de fonction d'enveloppement et l'adresse V5DL correspondante du protocole de protection dans le TS16 de la liaison primaire et de la liaison secondaire ont la même valeur et sont codées conformément aux dispositions des paragraphes 9.2 et 10.3.2.3.

Les deux liaisons de données servent à acheminer des informations entre les entités de protocole de protection du réseau d'accès et du commutateur local. Chaque message de couche 3 est diffusé sur les deux liaisons de données. L'entité homologue de couche 3 recevant les messages en provenance des deux liaisons de données traite le message à sa première occurrence et ignore le message identique qu'elle reçoit de l'autre liaison de données. On utilise des numéros de séquence pour distinguer un message qui a été reçu pour la première fois d'un message qui a déjà été reçu sur l'autre liaison de données.

En cas de détection d'une anomalie qui rend nécessaire une commutation de protection, la gestion-systèmes du réseau d'accès ou du commutateur local demande une commutation à l'aide d'unités de données de gestion (MDU, *management data unit*).

Les interfaces Q_{AN} et Q_{CL} seront averties en cas de commutation de protection et donneront l'état des voies C logiques ou physiques touchées.

Les systèmes d'exploitation du commutateur local et du réseau d'accès peuvent récupérer le mappage existant voies C logiques – voies C physiques sur demande via l'interface Q_{AN} ou Q_{CL}.

La Figure 26 illustre le modèle fonctionnel du protocole de protection.

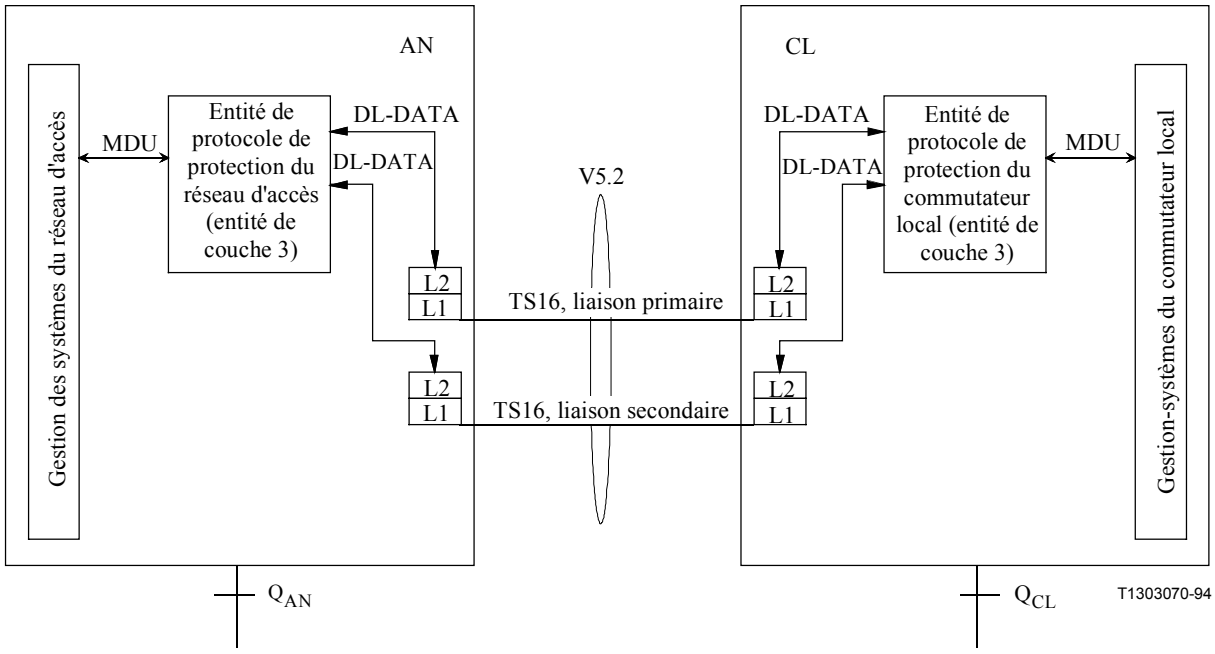


Figure 26/G.965 – Modèle fonctionnel du protocole de protection

18.2 Autres principes

La commutation de protection s'effectue en fait sur une voie C logique, c'est-à-dire que la commutation de protection ne doit pas entraîner de modification d'affectation du trajet C à la voie C logique.

Lorsqu'une voie C logique est protégée, tous les trajets C de cette voie C logique quittent la voie C active et sont commutés sur une voie C en attente.

La présente Recommandation ne précise pas si l'application commute les voies C logiques ou chaque trajet C d'une voie C logique.

Après commutation d'une voie C logique, les liaisons de données LAPV5 suivantes sont rétablies si elles sont transportées sur cette voie C logique: les liaisons du protocole BCC, du protocole de commande de liaison, du protocole de commande et du protocole RTPC. Les liaisons de données du protocole de protection ne sont pas rétablies automatiquement après la commutation. Le rétablissement d'une liaison de données du protocole de protection ne doit être tenté qu'en cas d'anomalie sur cette liaison de données.

18.3 Définition de l'entité de protocole de protection

18.3.1 Définition des états du protocole de protection

18.3.1.1 Etats dans le réseau d'accès

Etat ZÉRO (SOAN0)

La commutation n'a été lancée ni par le côté réseau d'accès ni par le côté commutateur local.

Etat SWITCH-OVER REQUESTED BY AN (commutation demandée par le réseau d'accès) (SOAN1)

La commutation a été demandée par la gestion-systèmes du réseau d'accès à l'aide d'une unité de données de gestion (MDU) spécialisée.

Etat SWITCH-OVER INITIATED BY LE (commutation lancée par le commutateur local) (SOAN2)

Un message SWITCH-OVER COM (commande de commutation) ou OS-SWITCH-OVER COM (commande de commutation par le système fonctionnel) a été reçu en provenance du côté commutateur local. La gestion-systèmes du réseau d'accès doit maintenant décider si cette commutation est possible ou non.

18.3.1.2 Etats dans le commutateur local

Etat ZÉRO (SOLE0)

La commutation n'a été lancée ni par le côté réseau d'accès ni par le côté commutateur local.

Etat SWITCH-OVER INITIATED BY LE (commutation lancée par le commutateur local) (SOLE1)

La commutation a été demandée par la gestion-systèmes du commutateur local à l'aide d'une unité MDU spécialisée.

Etat SWITCH-OVER REQUESTED BY AN (commutation demandée par le réseau d'accès) (SOLE2)

Un message SWITCH-OVER REQ (demande de commutation) a été reçu en provenance du côté réseau d'accès. La gestion-systèmes du commutateur local doit maintenant décider si cette commutation est possible ou non.

18.3.2 Définition des événements de protocole de protection

Les Tableaux 49 et 50 définissent les unités MDU, messages et temporisateurs utilisés dans la machine FSM de protection du réseau d'accès et du commutateur local.

Tableau 49/G.965 – MDU, messages et temporisateurs utilisés dans la machine FSM de protection du réseau d'accès

	Sens	Description
Protection-MDU (demande de commutation)	PROTECT_AN ← SYS	La gestion-systèmes a détecté une anomalie et demande la commutation; la commutation est lancée par l'OS du réseau d'accès via l'interface Q_{AN}.
Protection-MDU (accusé de réception de commutation)	PROTECT_AN ← SYS	La gestion-systèmes accuse réception d'une commutation dans le réseau d'accès.
Protection-MDU (rejet de commutation; cause)	PROTECT_AN ← SYS	La gestion-systèmes rejette une commutation et en indique la cause.
Protection-MDU (commande de commutation)	PROTECT_AN → SYS	L'entité de protocole de protection a reçu une commande de commutation du commutateur local.
Protection-MDU (commande de commutation-OS)	PROTECT_AN → SYS	L'entité de protocole de protection a reçu une commande de commutation de l'OS du commutateur local.
Protection-MDU (indication de rejet de commutation; cause)	PROTECT_AN → SYS	L'entité de protocole de protection indique la réception d'un message de rejet de commutation à la gestion-systèmes et en indique la cause.
Protection-MDU (indication d'erreur de commutation)	PROTECT_AN → SYS	L'entité de protocole de protection indique l'expiration du temporisateur TSO3 à la gestion-systèmes.
Protection-MDU (commande de réinitialisation du numéro de séquence)	PROTECT_AN → SYS	L'entité de protocole de protection indique à la gestion-systèmes que la réinitialisation du numéro de séquence a été lancée.
Protection-MDU (indication de réinitialisation du numéro de séquence)	PROTECT_AN → SYS	L'entité de protocole de protection indique la réception d'un message RESET SN COM par la gestion-systèmes.
Protection-MDU (accusé de réception de réinitialisation du numéro de séquence)	PROTECT_AN → SYS	L'entité de protocole de protection indique à la gestion-systèmes que l'entité homologue a accusé réception de la réinitialisation du numéro de séquence.
Protection-MDU (indication d'erreur de réinitialisation du numéro de séquence)	PROTECT_AN → SYS	L'entité de protocole de protection indique à la gestion-systèmes la présence d'une erreur dans la procédure de réinitialisation du numéro de séquence.
SWITCH-OVER COM	PROTECT_AN←PROTECT_LE	Lancement par le commutateur local de la commutation.
OS-SWITCH-OVER COM	PROTECT_AN←PROTECT_LE	Lancement par l'OS du commutateur local de la commutation.
SWITCH-OVER REQ	PROTECT_AN→PROTECT_LE	Demande par un réseau d'accès de commutation.
SWITCH-OVER ACK	PROTECT_AN→PROTECT_LE	Réponse positive à une commande de commutation.
SWITCH-OVER REJECT (cause)	PROTECT_AN↔PROTECT_LE	Rejet d'une commande de commutation et cause.
RESET SN COM	PROTECT_AN↔PROTECT_LE	Commande de réinitialisation du numéro de séquence.
RESET SN ACK	PROTECT_AN↔PROTECT_LE	Accusé de réception précisant que les variables d'état ont été réinitialisées.
PROTOCOL ERROR	PROTECT_AN→PROTECT_LE	Utilisée par le réseau d'accès pour indiquer une erreur de protocole au commutateur local.
Protection-MDU (indication d'erreur de protocole)	PROTECT_AN → SYS	Erreur de protocole détectée par le mécanisme de traitement des erreurs.
Expiration TSO3	Interne au réseau d'accès	Le temporisateur TSO3 a expiré.
Expiration TSO4	Interne au réseau d'accès	Le temporisateur TSO4 a expiré.
Expiration TSO5	Interne au réseau d'accès	Le temporisateur TSO5 a expiré.
PROTECT_AN Entité de protocole de protection du réseau d'accès PROTECT_LE Entité de protocole de protection du commutateur local SYS Gestion-systèmes		

Tableau 50/G.965 – MDU, messages et temporisateurs utilisés dans la machine FSM de protection du commutateur local

	Sens	Description
Protection-MDU (commande de commutation)	PROTECT_LE ← SYS	La gestion-systèmes a détecté une anomalie et lance une commutation ou la commutation a été lancée par l'OS du commutateur local via l'interface Q_{CL} ou par le réseau d'accès via l'interface V5.2.
Protection-MDU (commande de commutation-OS)	PROTECT_LE ← SYS	L'OS du commutateur local a lancé une commutation, cette commande peut entraîner la préemption d'une voie C physique qui transporte une voie C logique.
Protection-MDU (accusé de réception de commutation)	PROTECT_LE → SYS	L'entité de protocole de protection indique à la gestion-systèmes qu'il a reçu une réponse de commutation positive du réseau d'accès.
Protection-MDU (rejet de commutation; cause)	PROTECT_LE ← SYS	La gestion-systèmes rejette une commutation et en indique la cause.
Protection-MDU (demande de commutation)	PROTECT_LE → SYS	L'entité de protocole de protection indique à la gestion-systèmes qu'il a reçu une demande de commutation du réseau d'accès.
Protection-MDU (indication de rejet de commutation)	PROTECT_LE → SYS	L'entité de protocole de protection indique à la gestion-systèmes qu'il a reçu un message de rejet de commutation.
Protection-MDU (indication d'erreur de commutation)	PROTECT_LE → SYS	L'entité de protocole de protection indique à la gestion-systèmes l'expiration du temporisateur TSO1.
Protection-MDU (indication de réinitialisation du numéro de séquence)	PROTECT_LE → SYS	L'entité de protocole de protection indique qu'il a reçu un message RESET SN COM.
Protection-MDU (commande de réinitialisation du numéro de séquence)	PROTECT_LE → SYS	L'entité de protocole de protection indique à la gestion-systèmes que la réinitialisation du numéro de séquence a été lancée.
Protection-MDU (demande de réinitialisation du numéro de séquence)	PROTECT_LE ← SYS	La gestion-systèmes lance la réinitialisation du numéro de séquence pendant la procédure de démarrage du système.
Protection-MDU (accusé de réception de réinitialisation du numéro de séquence)	PROTECT_LE → SYS	L'entité de protocole de protection indique à la gestion-systèmes que l'entité homologue a accusé réception de la réinitialisation du numéro de séquence.
Protection-MDU (indication d'erreur de réinitialisation du numéro de séquence)	PROTECT_LE → SYS	Une erreur de procédure de réinitialisation est signalée à la gestion-systèmes.
Protection-MDU (indication d'erreur de protocole)	PROTECT_LE → SYS	Erreur de protocole détectée par le mécanisme de traitement des erreurs.
SWITCH-OVER COM	PROTECT_LE→PROTECT_AN	Lancement par le commutateur local de la commutation.
OS-SWITCH-OVER COM	PROTECT_LE→PROTECT_AN	Lancement par l'OS du commutateur local de la commutation, la préemption de la voie C active peut être nécessaire.
SWITCH-OVER REQ	PROTECT_LE←PROTECT_AN	Demande de commutation par le réseau d'accès.
SWITCH-OVER ACK	PROTECT_LE←PROTECT_AN	Réponse positive à une commande de commutation.
SWITCH-OVER REJECT (cause)	PROTECT_LE↔PROTECT_AN	Rejet d'une demande de commutation et cause.

Tableau 50/G.965 – MDU, messages et temporisateurs utilisés dans la machine FSM de protection du commutateur local

	Sens	Description
PROTOCOL ERROR	PROTECT_LE←PROTECT_AN	Erreur de protocole détectée par le mécanisme de traitement des erreurs du réseau d'accès, indication donnée au commutateur local.
RESET SN COM	PROTECT_LE↔PROTECT_AN	Commande de réinitialisation du numéro de séquence.
RESET SN ACK	PROTECT_LE↔PROTECT_AN	Accusé de réception indiquant que les variables d'état ont été réinitialisées.
Expiration TSO1	Interne au commutateur local	Le temporisateur TSO1 a expiré.
Expiration TSO2	Interne au commutateur local	Le temporisateur TSO2 a expiré.
Expiration TSO4	Interne au commutateur local	Le temporisateur TSO4 a expiré.
Expiration TSO5	Interne au commutateur local	Le temporisateur TSO5 a expiré.
PROTECT_AN Entité de protocole de protection du réseau d'accès PROTECT_LE Entité de protocole de protection du commutateur local SYS Gestion-systèmes		

18.4 Définition et contenu des messages de protocole de protection

L'ensemble complet des messages du protocole de protection est donné dans le Tableau 51. Le présent paragraphe donne la structure de message détaillée pour chacun de ces messages.

Tableau 51/G.965 – Ensemble des messages du protocole de protection

Codage à l'intérieur de l'élément d'information type de message							Messages du protocole de protection	Référence
7	6	5	4	3	2	1		
0	0	1	1	0	0	0	SWITCH-OVER REQ (demande de commutation)	18.4.1
0	0	1	1	0	0	1	SWITCH-OVER COM (commande de commutation)	18.4.2
0	0	1	1	0	1	0	OS-SWITCH-OVER COM (commande de commutation OS)	18.4.3
0	0	1	1	0	1	1	SWITCH-OVER ACK (accusé de réception de commutation)	18.4.4
0	0	1	1	1	0	0	SWITCH-OVER REJECT (rejet de commutation)	18.4.5
0	0	1	1	1	0	1	PROTOCOL ERROR (erreur de protocole)	18.4.6
0	0	1	1	1	1	0	RESET SN COM (commande de réinitialisation du numéro de séquence)	18.4.7
0	0	1	1	1	1	1	RESET SN ACK (accusé de réception de réinitialisation du numéro de séquence)	18.4.8

18.4.1 Message SWITCH-OVER REQ (demande de commutation)

Le réseau d'accès utilise ce message pour demander la commutation d'une voie C logique sur une voie C physique particulière. Ce message comporte une proposition d'affectation de la voie C logique défaillante sur une nouvelle voie C physique.

Le contenu du message SWITCH-OVER REQ est défini dans le Tableau 52.

Tableau 52/G.965 – Contenu du message SWITCH-OVER REQ

Type de message: SWITCH-OVER REQ
Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Identification de la voie C logique	18.5.1	AN vers CL	M	2
Type de message	13.2.3	AN vers CL	M	1
Numéro de séquence	18.5.2	AN vers CL	M	3
Identification de la voie C physique	18.5.3	AN vers CL	M	4

18.4.2 Message SWITCH-OVER COM (commande de commutation)

Le commutateur local utilise ce message pour lancer la commutation d'une voie C logique sur une voie C physique particulière. Ce message comporte la nouvelle affectation de la voie C logique à la voie C en attente particulière qui transportera la voie C logique une fois réalisée la commutation.

Le contenu du message SWITCH-OVER COM est défini dans le Tableau 53.

Tableau 53/G.965 – Contenu du message SWITCH-OVER COM

Type de message: SWITCH-OVER COM
Sens: CL vers AN

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	CL vers AN	M	1
Identification de la voie C logique	18.5.1	CL vers AN	M	2
Type de message	13.2.3	CL vers AN	M	1
Numéro de séquence	18.5.2	CL vers AN	M	3
Identification de la voie C physique	18.5.3	CL vers AN	M	4

18.4.3 Message OS-SWITCH-OVER COM (commande de commutation OS)

Le commutateur local utilise ce message pour lancer la commutation d'une voie C logique sur une voie C physique particulière à la demande de l'exploitant via l'interface Q_{CL}. Ce message comporte la nouvelle affectation de la voie C logique à une voie C physique particulière qui transportera la voie C logique une fois réalisée la commutation.

Le contenu du message OS-SWITCH-OVER COM est défini dans le Tableau 54.

Tableau 54/G.965 – Contenu du message OS-SWITCH-OVER COM

Type de message: OS-SWITCH-OVER COM
Sens: CL vers AN

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	CL vers AN	M	1
Identification de la voie C logique	18.5.1	CL vers AN	M	2
Type de message	13.2.3	CL vers AN	M	1
Numéro de séquence	18.5.2	CL vers AN	M	3
Identification de la voie C physique	18.5.3	CL vers AN	M	4

18.4.4 Message SWITCH-OVER ACK (accusé de réception de commutation)

Le réseau d'accès utilise ce message pour accuser réception de la commutation d'une voie C logique sur une voie C physique particulière après réception d'une commande de commutation en provenance du commutateur local.

Le contenu du message SWITCH-OVER ACK est défini dans le Tableau 55.

Tableau 55/G.965 – Contenu du message SWITCH-OVER ACK

Type de message: SWITCH-OVER ACK
Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Identification de la voie C logique	18.5.1	AN vers CL	M	2
Type de message	13.2.3	AN vers CL	M	1
Numéro de séquence	18.5.2	AN vers CL	M	3
Identification de la voie C physique	18.5.3	AN vers CL	M	4

18.4.5 Message SWITCH-OVER REJECT (rejet de commutation)

Le réseau d'accès ou le commutateur local utilisent ce message pour indiquer à l'entité homologue que la commutation ne peut pas être effectuée.

Le contenu du message SWITCH-OVER REJECT est défini dans le Tableau 56.

Tableau 56/G.965 –Contenu du message SWITCH-OVER REJECT

Type de message: SWITCH-OVER REJECT
Sens: les deux

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	Les deux	M	1
Identification de la voie C logique	18.5.1	Les deux	M	2
Type de message	13.2.3	Les deux	M	1
Numéro de séquence	18.5.2	Les deux	M	3
Identification de la voie C physique	18.5.3	Les deux	M	4
Cause du rejet	18.5.4	Les deux	M	3

18.4.6 Message PROTOCOL ERROR (erreur de protocole)

Le réseau d'accès utilise ce message pour indiquer au commutateur local qu'une erreur de protocole a été identifiée dans un message reçu. Une cause de l'erreur de protocole est donnée.

Le contenu du message PROTOCOL ERROR est défini dans le Tableau 57.

Tableau 57/G.965 – PROTOCOL ERROR

Type de message: PROTOCOL ERROR
Sens: AN vers CL

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	AN vers CL	M	1
Identification de la voie C logique	18.5.1	AN vers CL	M	2
Type de message	13.2.3	AN vers CL	M	1
Numéro de séquence	18.5.2	AN vers CL	M	3
Cause de l'erreur de protocole	17.5.5	AN vers CL	M	3 à 5

18.4.7 Message RESET SN COM (commande de réinitialisation du numéro de séquence)

Le commutateur local ou le réseau d'accès utilisent ce message pour indiquer à l'entité homologue qu'il y a eu erreur d'alignement des variables d'état d'émission et de réception côté émission et réception et que toutes les variables d'état ont été mises à zéro.

Le contenu du message RESET SN COM est défini dans le Tableau 58.

Tableau 58/G.965 – Contenu du message RESET SN COM

Type de message: RESET SN COM
Sens: les deux

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	Les deux	M	1
Identification de la voie C logique	18.5.1	Les deux	M	2
Type de message	13.2.3	Les deux	M	1

18.4.8 Message RESET SN ACK (accusé de réception de réinitialisation du numéro de séquence)

Le commutateur local ou le réseau d'accès utilisent ce message pour envoyer à l'entité homologue un message d'accusé de réception indiquant que les variables d'état d'émission et de réception ont été mises à zéro.

Le contenu du message RESET SN ACK est défini dans le Tableau 59.

Tableau 59/G.965 – Contenu du message RESET SN ACK

Type de message: RESET SN ACK
Sens: les deux

Elément d'information	Référence	Sens	Type	Longueur
Discriminateur de protocole	13.2.1	Les deux	M	1
Identification de la voie C logique	18.5.1	Les deux	M	2
Type de message	13.2.3	Les deux	M	1

18.5 Définition, structure et codage des éléments d'information du protocole de protection

Le présent paragraphe définit le codage des éléments d'information propres aux messages du protocole de protection. Le codage des différents champs est fourni pour chacun des éléments d'information.

Tous les éléments d'information propres au protocole de protection, à l'exception de l'élément d'information Identification de la voie C logique, sont énumérés dans le Tableau 60 qui donne par ailleurs le codage de l'identifiant d'élément d'information.

Tableau 60/G.965 – Eléments d'information propres au protocole de protection

Codage d'élément d'information								Messages du protocole de protection	Référence
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
0	–	–	–	–	–	–	–	Longueur variable	
0	1	0	1	0	0	0	0	Numéro de séquence	18.5.2
0	1	0	1	0	0	0	1	Identification de la voie C physique	18.5.3
0	1	0	1	0	0	1	0	Cause du rejet	18.5.4
0	1	0	1	0	0	1	1	Cause de l'erreur de protocole	18.5.5
NOTE – Toutes les autres valeurs sont réservées.									

18.5.1 Elément d'information Identification de la voie C logique

Le réseau d'accès et le commutateur local tiennent à jour une liste profilée des voies C logiques. Une voie C logique est identifiée sans ambiguïté par un numéro d'identification de voie C logique particulier.

Le numéro d'identification de voie C logique a une longueur de 16 bits et est codé en binaire. Tous les numéros de 0 à 65535 sont valables. Jusqu'à 44 numéros d'identification de voie C logique différents peuvent être profilés pour une interface V5.2 simple.

NOTE – La valeur 44 correspond au nombre maximal de voies C logiques sur une interface V5.2. Elle est égale au nombre maximal de voies C physiques (= 3 × 16 = 48) moins une voie C en attente pour le groupe de protection 1 et 3 voies C en attente pour le groupe de protection 2 (48 – 1 – 3 = 44).

La longueur de l'élément d'information Identification de voie C logique est de 2 octets.

Dans les messages RESET SN COM et RESET SN ACK la valeur de l'identification de voie C logique est 0 (c'est-à-dire que tous les bits sont mis à zéro).

Le codage de l'élément d'information Identification de voie C logique se fait conformément à la Figure 27.

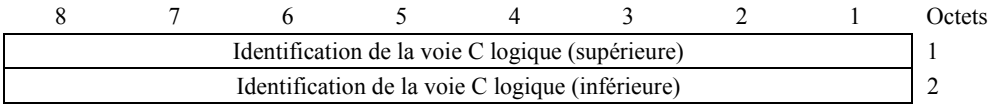


Figure 27/G.965 – Elément d'information Identification de voie C logique

18.5.2 Elément d'information Numéro de séquence

L'entité de réception utilise l'élément d'information Numéro de séquence pour faire la distinction entre le message qui est reçu pour la première fois et un message qui a déjà été reçu sur l'autre liaison de données du protocole de protection.

La longueur de cet élément d'information est de 3 octets.

L'élément d'information Numéro de séquence contient un champ numéro de séquence de 7 bits. Le numéro de séquence est codé en binaire et peut prendre des valeurs comprises entre 0 et 127.

Le codage de cet élément d'information se fait conformément à la Figure 28.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	1	0	0	0	0	1
Longueur du contenu du numéro de séquence								2
ext. 1	Numéro de séquence							3

Figure 28/G.965 – Elément d'information Numéro de séquence

18.5.3 Elément d'information Identification de voie C physique

Cet élément d'information identifie l'intervalle de temps dans une interface V5.2 qui est affecté à une voie C physique particulière. La gestion-systèmes du commutateur local fait en sorte que seuls les intervalles de temps profilés comme voies C physiques soient pris en compte dans cet élément d'information.

La longueur de l'élément d'information Identification de voie C physique est de 4 octets.

La structure de l'élément d'information Identification de voie C physique est celle indiquée à la Figure 29.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	1	0	0	0	0	1
Longueur du contenu de l'élément d'information								2
Identifiant de liaison V5 à 2048 kbit/s								3
0	0	0	Numéro d'intervalle de temps V5					4

Figure 29/G.965 – Elément d'information Identification de voie C physique

L'identifiant de liaison V5 à 2048 kbits est un champ de huit bits servant à fournir le codage binaire permettant d'identifier une liaison à 2048 kbit/s particulière parmi celles qui constituent l'interface V5.2 où est situé l'intervalle de temps V5 choisi qui sera utilisé comme voie C physique. Il est possible d'identifier expressément 256 liaisons à 2048 kbit/s au plus.

Le numéro d'intervalle de temps V5 est un champ de cinq bits servant à fournir le codage binaire qui identifie l'intervalle de temps V5 (dans la liaison à 2048 kbit/s identifiée dans l'octet précédent) qui sera utilisé comme voie C physique.

18.5.4 Elément d'information Cause du rejet

L'élément d'information Cause du rejet sert à indiquer à l'entité homologue la cause pour lequel la commutation d'une voie C logique donnée sur une autre voie C physique a été rejetée.

La longueur de l'élément d'information Cause du rejet est de trois octets.

Le codage de l'élément d'information Cause du rejet se fait conformément à la Figure 30.

8	7	6	5	4	3	2	1	Octets
	Identifiant élément d'information							
0	1	0	1	0	0	0	0	1
Longueur du contenu de l'élément d'information cause du rejet								2
ext. 1	Type de cause de rejet							3

Figure 30/G.965 – Elément d'information Cause du rejet

Le Tableau 61 donne la liste complète des types de cause du rejet et les codages correspondants. Il indique par ailleurs les sens dans lesquels le type de cause du rejet peut être utilisé.

Tableau 61/G.965 – Codage du champ type de cause du rejet

7	6	5	4	3	2	1	Signification	Sens
0	0	0	0	0	0	0	Pas de voie C en attente disponible	CL vers AN
0	0	0	0	0	0	1	Voie C physique cible non opérationnelle	Les deux
0	0	0	0	0	1	0	Voie C physique cible non profilée	Les deux
0	0	0	0	0	1	1	Commutation de protection impossible (anomalie dans le réseau d'accès/ commutateur local)	Les deux
0	0	0	0	1	0	0	Non concordance des groupes de protection	Les deux
0	0	0	0	1	0	1	L'affectation demandée existe déjà	Les deux
0	0	0	0	1	1	0	La voie C physique cible a déjà une voie C logique	Les deux
NOTE – Toutes les autres valeurs sont réservées.								

18.5.5 Elément d'information Cause d'erreur de protocole

Le réseau d'accès utilise l'élément d'information Cause d'erreur de protocole pour indiquer au commutateur local le type d'erreur de protocole détectée dans un processus donné.

L'élément d'information Cause d'erreur de protocole contient, pour certains types de causes d'erreur de protocole, un champ de diagnostic afin de fournir les informations supplémentaires relatives à ces types de causes d'erreur de protocole. Ce champ de diagnostic d'un ou deux octets, lorsqu'il est présent, est une copie de l'identifiant de type de message reçu qui a déclenché l'envoi du message contenant l'élément d'information Cause d'erreur de protocole et, lorsque cela est nécessaire, l'identifiant d'élément d'information pertinent dans ce message.

La longueur de l'élément d'information Cause d'erreur de protocole est comprise entre trois et cinq octets. Pour les types de causes d'erreur de protocole, qui ne contiennent pas une information de diagnostic, la longueur de l'élément d'information est de trois octets. Pour les autres, elle est de quatre ou cinq octets.

La structure de l'élément d'information Cause d'erreur de protocole est celle indiquée à la Figure 31.

8	7	6	5	4	3	2	1	Octets
	Identifiant d'élément d'information							
0	1	0	1	0	0	1	1	1
Longueur du contenu d'élément d'information								2
1	Type de cause d'erreur de protocole							3
0	Diagnostic (Identifiant de type de message)							4
Diagnostic (Identifiant d'élément d'information)								5

Figure 31/G.965 – Elément d'information Cause d'erreur de protocole

On utilise un champ de sept bits pour indiquer le type de cause d'erreur de protocole (Tableau 62).

Tableau 62/G.965 – Codage du type de cause d'erreur de protocole

7	6	5	4	3	2	1	Type de cause d'erreur de protocole
0	0	0	0	0	0	1	Erreur de discriminateur de protocole
0	0	0	0	1	0	0	Type de message non reconnu
0	0	0	0	1	1	1	Elément d'information obligatoire manquant
0	0	0	1	0	0	0	Elément d'information non reconnu
0	0	0	1	0	0	1	Erreur de contenu de l'élément d'information obligatoire
0	0	0	1	0	1	1	Message incompatible avec l'état du protocole de protection
0	0	0	1	1	0	0	Elément d'information obligatoire répété
0	0	0	1	1	0	1	Eléments d'information trop nombreux
0	0	0	1	1	1	1	Erreur d'identification de voie C logique
NOTE – Toutes les autres valeurs sont réservées.							

Le paragraphe 18.6.6 précise quand utiliser les valeurs associées aux différents types de cause d'erreur de protocole.

Le champ de diagnostic est un champ de plusieurs octets (le nombre d'octets dépend de la valeur de cause) fournissant le diagnostic pour chaque valeur associée à la cause d'erreur de protocole (Tableau 63).

Tableau 63/G.965 – Champ de diagnostic pour les types d'erreur de protocole

Cause	Diagnostic	Longueur
Erreur de discriminateur de protocole	Pas de diagnostic	0
Erreur d'identification de voie C logique	Pas de diagnostic	0
Type de message non reconnu	Identifiant de type de message	1
Elément d'information obligatoire manquant	Identifiant de type de message Identifiant d'élément d'information	2
Elément d'information non reconnu	Identifiant de type de message Identifiant d'élément d'information	2
Erreur de contenu d'élément d'information obligatoire	Identifiant de type de message Identifiant d'élément d'information	2
Message incompatible avec l'état du protocole de protection	Identifiant de type de message	1
Elément d'information obligatoire répété	Identifiant de type de message Identifiant d'élément d'information	2
Eléments d'information trop nombreux	Identifiant de type de message	1

18.6 Procédures associées au protocole de protection

18.6.1 Généralités

Le protocole de protection est un protocole fonctionnel. Les entités homologues accusent explicitement réception d'une demande de commutation émanant du côté réseau d'accès ou d'une commande de commutation émanant du côté commutateur local à l'aide des messages SWITCH-OVER COM ou SWITCH-OVER ACK respectivement. La réception d'un accusé de réception est supervisée par des temporisateurs. A la première expiration d'un temporisateur sans accusé de réception de l'entité homologue, le message est retransmis. A la seconde expiration, une indication d'erreur est envoyée à la gestion-systèmes et l'entité de protocole de protection passe à l'état zéro sans retransmettre de nouveau le message. La gestion-systèmes a alors la responsabilité d'effectuer les opérations de maintenance qui s'imposent.

Il appartient à la gestion-systèmes du commutateur local de contrôler à quelle voie C physique est attribuée une voie C logique à l'aide du protocole de protection. Elle obtient cette information de façon autonome depuis le gestionnaire des ressources de protection de la gestion-systèmes du commutateur local en cas d'anomalie détectée par le commutateur local; autre solution, cette information lui est fournie par l'exploitant du commutateur local via l'interface Q_{CL}.

Si la commutation est lancée par l'exploitant via l'interface Q_{CL} et si l'exploitant a décidé que la préemption d'une voie C active était nécessaire, la gestion-systèmes du commutateur local l'indique à l'entité du protocole de protection à l'aide d'une primitive spécialisée [MDU-Protection (commande de commutation de l'OS)]. La préemption n'est utilisée que pour le groupe de protection 1.

La gestion-systèmes du réseau d'accès peut lancer une commutation après avoir détecté une anomalie interne; cette commutation peut aussi être lancée par l'exploitant de l'OS via l'interface Q_{AN}. L'exploitant peut indiquer la voie C en attente qu'il préfère utiliser.

A réception d'une primitive MDU-Protection (commande de commutation) ou MDU-Protection (commande de commutation de l'OS) la gestion-systèmes du réseau d'accès vérifie uniquement si les ressources requises pour la commutation sont disponibles ou non. Le résultat de cette vérification est communiqué au commutateur local à l'aide d'un message SWITCH-OVER ACK ou SWITCH-OVER REJECT, ce qui signifie qu'il n'y aura pas d'accusé de réception pour la commutation elle-même accomplie avec succès. Si l'un ou l'autre côté s'aperçoit plus tard qu'il a eu des problèmes avec la commutation, une nouvelle commutation doit être lancée.

18.6.2 Diffusion de messages de protocole de protection sur les deux liaisons de données de la liaison primaire et de la liaison secondaire

18.6.2.1 Transmission de messages de protocole de protection

Les entités de protocole de protection du réseau d'accès et du commutateur local transmettent tous les messages de protocole de protection, via des primitives DL-DATA, aux couches Liaisons de données correspondantes dans les intervalles de temps 16 de la liaison primaire et de la liaison secondaire. Chaque entité de protocole de protection dispose d'une variable d'état émission VP(S). Après le démarrage du système, cette variable est mise à zéro. Chaque fois qu'un message de protocole de protection contenant un élément d'information Numéro de séquence est envoyé, le numéro de séquence (SN) à l'intérieur de l'élément d'information Numéro de séquence est égal à la variable d'état émission côté émission. Le message est ensuite envoyé aux deux entités de liaisons de données via des primitives DL-DATA et la variable d'état émission côté émission est incrémentée d'un modulo 128.

NOTE – Les valeurs de SN et VP(S) peuvent être comprises entre 0 et 127 et le modulo est 128.

18.6.2.2 Réception de messages de protocole de protection

Chaque entité de protocole de protection dispose d'une variable d'état réception VP(R). Elle indique le numéro de séquence du prochain message de la séquence que l'on espère recevoir. Après le démarrage du système, la variable d'état réception VP(R) est mise à zéro.

Un message reçu par une entité de protocole de protection de couche 3 est vérifié tout d'abord par le mécanisme de traitement des erreurs présentées au 18.6.6.

Si le message de protocole de protection contient un élément d'information Numéro de séquence, l'entité de protocole de protection côté réception décide compte tenu du numéro de séquence et de la variable d'état réception VP(R) si ce message a déjà été reçu sur l'autre liaison de données, s'il s'agit d'un nouveau message valable reçu pour la première fois ou s'il y a défaut d'alignement entre les variables d'état émission et réception côté émission et réception respectivement.

NOTE 1 – Les valeurs de VP(R) peuvent être comprises entre 0 et 127 et le modulo est 128.

L'entité de réception:

– ignore le message si le numéro de séquence se trouve dans la fourchette $VP(R) - 5 \leq SN \leq VP(R) - 1$, sans notification à la gestion-systèmes;

– considère le message comme un nouveau message valable, si le numéro de séquence est compris dans la fourchette $VP(R) \leq SN \leq VP(R) + 4$. Dans ce cas VP(R) est d'abord égalisé à SN puis incrémenté d'un modulo 128;

– autre cas, l'entité de réception suppose qu'il y a défaut d'alignement entre les variables d'état côté d'émission et côté réception. L'entité de protocole engage alors la procédure de réinitialisation du numéro de séquence décrite au 18.6.2.3.

NOTE 2 – Les inégalités suivantes tiennent compte du modulo 128.

18.6.2.3 Procédure de réinitialisation du numéro de séquence

18.6.2.3.1 Procédure normale

La procédure de réinitialisation du numéro de séquence est une procédure symétrique qui est lancée par l'entité détectant un défaut d'alignement des variables d'état. Elle sera aussi lancée pendant la phase de démarrage du système après l'établissement d'au moins une des deux liaisons de données de protection. Dans ce cas, la procédure est lancée par la gestion-systèmes du commutateur local qui enverra une primitive MDU-Protection (accusé de réception de la réinitialisation du numéro de séquence) à l'entité de protocole de protection du commutateur local. Cette procédure utilise les messages RESET SN COM et RESET SN ACK, qui ne contiennent pas d'élément d'information Numéro de séquence.

L'entité lançant la procédure de réinitialisation envoie un message RESET SN COM à l'entité homologue, remet à zéro la variable d'état émission VP(S) et la variable d'état réception VP(R), déclenche le temporisateur TSO4, et envoie une primitive MDU-Protection (commande de réinitialisation du numéro de séquence) à la gestion-systèmes. Si le commutateur local a déclenché la réinitialisation du numéro de séquence et si l'entité de protocole de protection du commutateur local ne se trouve pas dans l'état zéro (SOLE0), les temporisateurs TSO1 et TSO2, s'ils fonctionnent, sont arrêtés et l'entité de protocole de protection du commutateur local revient à l'état zéro. Si le réseau d'accès a déclenché la réinitialisation du numéro de séquence et si l'entité de protocole de protection du réseau d'accès n'est pas dans l'état zéro (SOAN0) le temporisateur TSO3, s'il fonctionne, est arrêté et l'entité de protocole de protection du réseau d'accès revient à l'état zéro.

Le côté recevant le message RESET SN COM répond, si le temporisateur TSO5 ne fonctionne pas, avec un message RESET SN ACK, remet à zéro la variable d'état émission VP(S) et la variable d'état réception VP(R), déclenche le temporisateur TSO5 et envoie une primitive MDU-Protection (indication de réinitialisation du numéro de séquence) à la gestion-systèmes. Si le commutateur local a reçu le message RESET SN COM et si l'entité de protocole de protection du commutateur local ne se trouve pas dans l'état zéro (SOLE0) les temporisateurs TSO1 et TSO2, s'ils fonctionnent, sont arrêtés et l'entité de protocole de protection du commutateur local revient à l'état zéro. Si le réseau d'accès a reçu le message RESET SN COM et si l'entité de protocole de protection du réseau d'accès ne se trouve pas dans l'état zéro (SOAN0) le temporisateur TSO3, s'il fonctionne, est arrêté et l'entité de protocole de protection du réseau d'accès revient à l'état zéro.

Si un message RESET SN COM est reçu pendant que le temporisateur TSO5 fonctionne, il n'y a pas d'action et pas de transition d'état.

A réception d'un message RESET SN ACK, le temporisateur TSO4, s'il fonctionne, est arrêté et une primitive MDU-Protection (accusé de réception de réinitialisation du numéro de séquence) est envoyée à la gestion-systèmes. A la réception d'un message RESET SN ACK, si le temporisateur TSO4 ne fonctionne pas, il n'y a pas d'action et pas de transition d'état.

Tant que le temporisateur TSO4 fonctionne, tous les messages reçus qui contiennent un élément d'information Numéro de séquence sont rejetés sans notification à la gestion-systèmes. Dans ce cas, les procédures de vérification du numéro de séquence décrites au 18.6.2.2 ne sont pas traitées. Il n'y a pas de transition d'état.

Tant que le temporisateur TSO4 du réseau d'accès fonctionne, à réception d'une primitive MDU-Protection (demande de commutation) dans le réseau d'accès, une primitive MDU-Protection (indication d'erreur de réinitialisation du numéro de séquence) est envoyée à la gestion-systèmes. Il n'y a pas de transition d'état.

Tant que le temporisateur TSO4 du commutateur local fonctionne, à réception d'une primitive MDU-Protection (commande de commutation) ou d'une primitive MDU-Protection (commande de commutation OS) dans le commutateur local, une primitive MDU-Protection (indication d'erreur de réinitialisation du numéro de séquence) est envoyée à la gestion-systèmes. Il n'y a pas de transition d'état.

A l'expiration du temporisateur TSO5, il n'y a pas d'action et pas de transition d'état.

18.6.2.3.2 Procédures exceptionnelles

A la première expiration du temporisateur TSO4, un message RESET SN COM est envoyé à l'entité homologue, la variable d'état émission VP(S) et la variable d'état réception VP(R) sont remises à zéro, une primitive MDU-Protection (commande de réinitialisation du numéro de séquence) est envoyée à la gestion-systèmes et le temporisateur TSO4 est redémarré.

A la seconde expiration du temporisateur TSO4, une primitive MDU-Protection (indication d'erreur de réinitialisation du numéro de séquence) est envoyée à la gestion-systèmes. Il appartient alors à la gestion-systèmes d'effectuer les opérations qui s'imposent.

En cas d'expiration intempestive du temporisateur TSO4 (c'est-à-dire lorsqu'il n'est pas dans l'état zéro) il n'y a pas d'action et pas de transition d'état.

18.6.3 Procédure standard de commutation de protection lancée par le commutateur local

18.6.3.1 Procédure normale

Cette procédure est utilisée si le côté commutateur local détecte une anomalie ou si une commutation est lancée via l'interface Q_{CL}. Elle fait appel à la commande SWITCH-OVER, ce qui n'autorise pas la préemption de voies C affectées.

Lorsque le protocole de protection du commutateur local se trouve dans l'état zéro (SOLE0) ou l'état commutation demandée par le réseau d'accès (SOLE2) et reçoit une primitive MDU-Protection (commande de commutation), il doit envoyer un message SWITCH-OVER COM, déclencher le temporisateur TSO1 et passer à l'état commande lancée par le commutateur local (SOLE1). Le message SWITCH-OVER COM indique la voie C logique à commuter et la voie C en attente cible.

A réception du message SWITCH-OVER COM par l'entité de protocole de protection du réseau d'accès, le réseau d'accès se trouvant dans l'état zéro (SOAN0) passe à l'état commutation lancée par le commutateur local (SOAN2) et envoie une primitive MDU-Protection (commande de commutation) à la gestion-systèmes du réseau d'accès.

La gestion-systèmes du réseau d'accès, si elle est en mesure de donner suite à la commande de commutation, lance l'opération de commutation dans le réseau d'accès et envoie une primitive MDU-Protection (accusé de réception de commutation) à l'entité de protocole de protection du réseau d'accès qui ensuite envoie un message SWITCH-OVER ACK au commutateur local et passe à l'état zéro (SOAN0).

A réception du message SWITCH-OVER ACK émanant du réseau d'accès, l'entité de protection de protocole du commutateur local envoie une primitive MDU-Protection (accusé de réception de commutation) à la gestion-systèmes du commutateur local, arrête le temporisateur TSO1 et passe à l'état zéro (SOLE0).

A réception du message SWITCH-OVER REQ émanant du réseau d'accès, et étant dans l'état commutation lancée par le commutateur local (SOLE1), il n'y a pas d'action et pas de transition d'état.

Le commutateur local doit poursuivre la commutation engagée.

18.6.3.2 Procédures exceptionnelles

La gestion-systèmes du réseau d'accès, si elle n'est pas en mesure de donner suite à la commande de commutation, envoie une primitive MDU-Protection (rejet de commutation) à l'entité de protocole de protection du réseau d'accès qui ensuite envoie un message SWITCH-OVER REJECT au commutateur local et passe à l'état zéro (SOAN0). Ce message indique au commutateur local la raison pour laquelle la commutation n'était pas possible.

A réception du message SWITCH-OVER REJECT émanant du réseau d'accès, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication de rejet de commutation) à la gestion-systèmes du commutateur local, arrête le temporisateur TSO1 et passe à l'état zéro (SOLE0).

Si l'entité de protocole de protection du réseau d'accès ou du commutateur local reçoit une primitive MDU-Protection intempestive, il n'y a pas d'action et pas de transition d'état.

18.6.3.3 Procédure lors de l'expiration du temporisateur TSO1

Si le temporisateur TSO1 expire pour la première fois alors que l'entité de protocole de protection du commutateur local se trouve dans l'état commutation lancée par le commutateur local (SOLE1), l'entité de protocole de protection du commutateur local envoie un message SWITCH-OVER COM au réseau d'accès et redémarre le temporisateur TSO1.

Dès réception d'un message SWITCH-OVER ACK émanant du réseau d'accès se trouvant dans l'état SOLE0, une primitive MDU-Protection (accusé de réception de commutation) est envoyée à la gestion-systèmes. Il appartient à cette dernière d'effectuer l'opération qui s'impose en fonction de la séquence des messages reçus précédemment (la gestion-systèmes peut déclencher la commutation dans le commutateur local ou peut engager un nouveau processus de commutation).

Dès réception d'un message SWITCH-OVER REJECT émanant du réseau d'accès qui se trouve dans l'état SOLE0, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication de rejet de commutation) à la gestion-systèmes. Il appartient à cette dernière d'effectuer l'opération qui s'impose en fonction de la séquence des messages reçus précédemment et du contenu de l'élément d'information Cause du rejet (la gestion-systèmes peut engager un nouveau processus de commutation).

Si le temporisateur TSO1 expire pour la seconde fois, alors que l'entité de protocole de protection du commutateur local se trouve dans l'état commutation lancée par le commutateur local (SOLE1) l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de commutation) à la gestion-systèmes et passe à l'état zéro (SOLE0).

En cas d'expiration intempestive du temporisateur TSO1 (expiration lorsqu'il ne se trouve pas dans l'état commutation lancée par le commutateur local) il n'y a pas d'action et pas de transition d'état.

18.6.4 Procédure de commutation de protection spécialisée lancée par l'OS du commutateur local

18.6.4.1 Procédure normale

Cette procédure n'est utilisée que si la commutation est lancée par l'exploitant du commutateur local via l'interface Q_{CL}. Si la voie C physique cible est une voie C active, la voie C physique fait l'objet d'une préemption. Cette procédure sert essentiellement à réaménager l'affectation des voies C logiques en cas d'anomalies sur plusieurs des liaisons à 2048 kbit/s. Elle n'est utilisée que pour le groupe de protection 2.

Si le protocole de protection du commutateur local, qui se trouve dans l'état zéro (SOLE0) ou l'état commutation demandée par le réseau d'accès (SOLE2) et reçoit une primitive MDU-Protection (commande de commutation OS), il envoie un message OS-SWITCH-OVER COM, démarre le temporisateur TSO2 et passe à l'état commutation lancée par le commutateur local (SOLE1). Le message OS-SWITCH-OVER COM indique la voie C logique à commuter et la voie C physique cible.

A réception du message OS-SWITCH-OVER COM par l'entité de protocole de protection du réseau d'accès qui se trouve dans l'état zéro (SOAN0), le réseau d'accès passe à l'état commutation lancée par le commutateur local (SOAN2) et envoie une primitive MDU-Protection (commande de commutation OS) à la gestion-systèmes du réseau d'accès.

La gestion-systèmes du réseau d'accès, si elle est en mesure d'exécuter la commande de commutation, lance une opération de commutation dans le réseau d'accès et envoie une primitive MDU-Protection (accusé de réception de commutation) à l'entité de protocole de protection du réseau d'accès qui envoie alors un message SWITCH-OVER ACK au commutateur local et passe à l'état zéro (SOAN0).

A réception du message SWITCH-OVER ACK émanant du réseau d'accès, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (accusé de réception de commutation) à la gestion-systèmes du commutateur local, arrête le temporisateur TSO2 et passe à l'état zéro (SOLE0).

Si le réseau d'accès reçoit un message SWITCH-OVER REQ lorsqu'il se trouve dans l'état commutation lancée par le commutateur local (SOLE1), il n'y a pas d'action et pas de transition d'état.

Le commutateur local doit poursuivre la commutation engagée.

18.6.4.2 Procédures exceptionnelles

La gestion-systèmes du réseau d'accès, si elle n'est pas en mesure d'exécuter la commande de commutation, envoie une primitive MDU-Protection (rejet de commutation) à l'entité de protocole de protection du réseau d'accès qui envoie alors un message SWITCH-OVER REJECT du commutateur local et passe à l'état zéro (SOAN0). Le message indique au commutateur local la raison pour laquelle la commutation n'était pas possible. La commande de commutation ne doit pas être rejetée parce que la voie C physique cible transportait déjà une voie C logique. La cause du rejet "la voie C physique cible a déjà une voie C logique" ne peut donc pas être une réponse à un message OS-SWITCH-OVER COM.

Dès réception du message SWITCH-OVER REJECT émanant du réseau d'accès, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication de rejet de commutation) à la gestion-systèmes du commutateur local, arrête le temporisateur TSO2 et passe à l'état zéro (SOLE0).

Si l'entité de protocole de protection du réseau d'accès ou du commutateur local reçoit une primitive MDU-Protection intempestive, il n'y a pas d'action et de transition d'état.

18.6.4.3 Procédure en cas d'expiration du temporisateur TSO2

Si le temporisateur TSO2 expire pour la première fois alors que l'entité de protocole de protection du commutateur local se trouve dans l'état commutation lancée par le commutateur local (SOLE1), l'entité de protocole de protection du commutateur local envoie un message OS-SWITCH-OVER COM au réseau d'accès et redémarre le temporisateur TSO2.

Si le temporisateur TSO2 expire pour la seconde fois, alors que l'entité de protocole de protection du commutateur local se trouve dans l'état commutation lancée par le commutateur local (SOLE1), l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de commutation) à la gestion-systèmes et passe à l'état zéro (SOLE0).

A réception d'un message SWITCH-OVER ACK émanant du réseau d'accès qui se trouve dans l'état SOLE0, une primitive MDU-Protection (accusé de réception de commutation) est envoyée à la gestion-systèmes. Il appartient à cette dernière d'effectuer l'opération qui s'impose selon la séquence des messages précédemment reçus (la gestion-systèmes peut lancer la commutation dans le commutateur local ou peut lancer un nouveau processus de commutation).

A réception d'un message SWITCH-OVER REJECT émanant du réseau d'accès qui se trouve dans l'état SOLE0, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication de rejet et de commutation) à la gestion-systèmes. Il appartient à cette dernière d'effectuer l'opération qui s'impose selon la séquence des messages précédemment reçus et le contenu de l'élément d'information Cause du rejet (la gestion-systèmes peut lancer un nouveau processus de commutation).

En cas d'expiration intempestive du temporisateur TSO2 (expiration alors qu'il ne se trouve pas dans l'état commutation lancée par le commutateur local) il n'y a pas d'action et pas de transition d'état.

18.6.5 Procédure de commutation de protection demandée par le réseau d'accès

18.6.5.1 Procédure normale

Cette procédure est utilisée si une anomalie est détectée par le côté réseau d'accès ou si une commutation est lancée via l'interface Q_{AN}. Le commutateur local ne peut répondre qu'à l'aide d'un message SWITCH-OVER COM (aucune préemption autorisée) ou d'un message SWITCH-OVER REJECT.

Si le protocole de protection du réseau d'accès se trouve dans l'état zéro (SOAN0) et reçoit une primitive MDU-Protection (demande de commutation), il envoie un message SWITCH-OVER REQ, démarre le temporisateur TSO3 et passe à l'état commutation demandée par le réseau d'accès (SOAN1). Si la commutation a été lancée par l'exploitant de l'OS via l'interface Q_{AN}, le message SWITCH-OVER REQ indique la voie C logique à commuter et éventuellement la voie C physique cible préférée (voie C en attente). Si la commutation a été déclenchée de façon autonome par la gestion-systèmes du réseau d'accès à la suite de la détection d'une anomalie, le message SWITCH-OVER REQ indique uniquement la voie C logique à commuter et aucune préférence n'est donnée pour une voie C en attente particulière.

Lorsque aucune préférence n'est indiquée, on code à zéro tous les bits de l'identifiant de liaison à 2048 kbit/s et du numéro d'intervalle de temps dans l'élément d'information Voie C physique.

A réception du message SWITCH-OVER REQ par l'entité de protocole de protection du commutateur local, le commutateur local qui se trouve dans l'état zéro (SOLE0) passe à l'état commutation demandée par le réseau d'accès (SOLE2) et envoie une primitive MDU-Protection (demande de commutation) à la gestion-systèmes du commutateur local.

A réception du message SWITCH-OVER REQ par l'entité de protocole de protection du commutateur local, le commutateur local qui se trouve dans l'état commutation lancée par le commutateur local (SOLE1) ignore le message et ne change pas d'état.

La gestion-systèmes du commutateur local, si elle est en mesure d'exécuter la demande de commutation, lance la procédure de commutation en envoyant une primitive MDU-Protection (commande de commutation) à l'entité de protocole de protection du commutateur local, qui envoie alors un message SWITCH-OVER COM au réseau d'accès, passe à l'état commutation lancée par le commutateur local (SOLE1) et démarre le temporisateur TSO1.

A réception du message SWITCH-OVER COM par l'entité de protocole de protection du réseau d'accès, le réseau d'accès qui se trouve à l'état commutation lancée par le réseau d'accès (SOAN1) passe à l'état commutation lancée par le commutateur local (SOAN2) envoie une primitive MDU-Protection (commande de commutation) à la gestion-systèmes du réseau d'accès et arrête le temporisateur TSO3.

A réception du message OS-SWITCH-OVER COM par l'entité de protocole de protection du réseau d'accès, le réseau d'accès qui se trouve dans l'état commutation demandée par le réseau d'accès (SOAN1) passe à l'état commutation lancée par le commutateur local (SOAN2) envoie une primitive MDU-Protection (commande de commutation OS) à la gestion-systèmes du réseau d'accès et arrête le temporisateur TSO3.

La gestion-systèmes du réseau d'accès, si elle est en mesure d'exécuter la commande de commutation, lance l'opération de commutation dans le réseau d'accès et envoie une primitive MDU-Protection (accusé de réception de commutation) à l'entité de protocole de protection du réseau d'accès qui envoie alors un message SWITCH-OVER ACK au commutateur local et passe à l'état zéro (SOAN0).

A réception du message SWICH-OVER ACK émanant du réseau d'accès, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (accusé de réception de commutation) à la gestion-systèmes du commutateur local, arrête le temporisateur TSO1 et passe à l'état zéro (SOLE0).

Le commutateur local exécute alors la commutation. Si pour une raison ou une autre, il ne peut exécuter la commutation, il appartient à la gestion-systèmes du commutateur local de lancer une nouvelle opération de commutation.

18.6.5.2 Procédure exceptionnelle – Le réseau d'accès ne peut pas exécuter la commande de commutation émanant du commutateur local

La gestion-systèmes du réseau d'accès, si elle n'est pas en mesure d'exécuter la commande de commutation, envoie une primitive MDU-Protection (rejet de commutation) à l'entité de protocole de protection du réseau d'accès qui envoie alors un message SWITCH-OVER REJECT au commutateur local et passe à l'état zéro (SOAN0). Le message indique au commutateur local la raison pour laquelle la commutation n'est pas possible.

A réception du message SWITCH-OVER REJECT émanant du réseau d'accès, l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication de rejet de commutation) à la gestion-systèmes du commutateur local, arrête le temporisateur TSO1 et passe à l'état zéro (SOLE0).

Si une primitive MDU-Protection intempestive est reçue par l'entité de protocole de protection du réseau d'accès ou du commutateur local, il n'y a pas d'action et pas de transition d'état.

18.6.5.3 Procédure exceptionnelle – Le commutateur local ne peut pas exécuter la demande de commutation émanant du réseau d'accès

La gestion-systèmes du commutateur local, qui se trouve dans l'état commutation demandée par le réseau d'accès (SOLE2), si elle n'est pas en mesure d'exécuter la commande de commutation, envoie une primitive MDU-Protection (rejet de commutation) à l'entité de protocole de protection du commutateur local qui envoie alors un message SWITCH-OVER REJECT au réseau d'accès et passe à l'état zéro (SOLE0). Ce message indique au réseau d'accès la raison pour laquelle la commutation n'est pas possible.

A réception du message SWITCH-OVER REJECT émanant du commutateur local, qui se trouve dans l'état commutation demandée par le réseau d'accès, l'entité de protocole de gestion du réseau d'accès envoie une primitive MDU-Protection (indication de rejet de commutation) à la gestion-systèmes du réseau d'accès, arrête le temporisateur TSO3 et passe à l'état zéro (SOAN0).

Si une primitive MDU-Protection intempestive est reçue par l'entité de protocole protection du réseau d'accès ou du commutateur local, il n'y a pas d'opération et de transition d'état.

18.6.5.4 Procédure en cas d'expiration du temporisateur TSO3

Si le temporisateur TSO3 expire pour la première fois alors que l'entité de protocole de protection du réseau d'accès se trouve dans l'état commutation demandée par le réseau d'accès (SOAN1), l'entité de protocole de protection du réseau d'accès envoie un message SWITCH-OVER REQ au commutateur local et redémarre le temporisateur TSO3.

Si le temporisateur TSO3 expire pour la seconde fois, alors que l'entité de protocole de protection du réseau d'accès se trouve dans l'état commutation demandée par le réseau d'accès (SOAN1), l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de commutation) à la gestion-systèmes et passe à l'état zéro (SOAN0).

En cas d'expiration intempestive du temporisateur TSO3 (expiration alors qu'il ne se trouve pas dans l'état commutation demandée par le réseau d'accès) il n'y a pas d'action et pas de transition d'état.

18.6.6 Traitement des conditions d'erreur

Avant d'agir sur un message, l'entité de réception, qu'il s'agisse de l'entité de protocole de protection V5.2 du réseau d'accès ou de l'entité de protocole de protection V5.2 du commutateur local, exécute les procédures énumérées dans le présent paragraphe.

En règle générale, tous les messages à l'exception des messages RESET SN COM et RESET SN ACK contiennent au moins les éléments d'information Discriminateurs de protocole, Identification de la voie C logique et Type de message. Lorsqu'elle reçoit un message ayant moins de 4 octets, l'entité de protocole de protection de réception du réseau d'accès ou du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

Un message reçu est vérifié selon les modalités décrites dans 18.6.6.1 à 18.6.6.7 par ordre de préséance. Il n'y a pas de transition d'état pendant ces vérifications.

Si plus de deux éléments d'information facultatifs sont détectés dans un message, ce message est alors considéré comme trop long et doit être tronqué après le deuxième élément d'information facultatif. On considère que toute l'information tronquée constitue des éléments d'information facultatifs répétés. Lorsqu'elle effectue la troncature, l'entité réagit conformément aux modalités du 18.6.6.3 pour les éléments d'information facultatifs répétés.

Si une erreur de protocole est détectée dans le réseau d'accès alors que le temporisateur TSO4 fonctionne, aucun message PROTOCOL ERROR n'est envoyé au côté du commutateur local.

Une fois le message vérifié à l'aide des procédures de traitement d'erreur décrites ci-après, si ce message n'est pas ignoré, on applique les procédures de protocole de protection définies dans 18.6.2 à 18.6.5.

NOTE – Dans le présent sous-paragraphe, l'expression "ignorer le message" signifie ne pas changer le contenu du message.

18.6.6.1 Erreur de discriminateur de protocole

Lorsqu'une entité de protocole de protection de couche 3 reçoit un message avec un discriminateur de protocole codé autre que celui spécifié au 13.2.1 pour être utilisé dans les protocoles V5:

– l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "erreur de discriminateur de protocole";

– l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

18.6.6.1a Erreur d'identification de voie C logique

Lorsqu'une entité de protocole de protection de couche 3 reçoit un message avec une identification de voie C logique qui:

– n'est pas codée comme spécifié au paragraphe 18.5.1;

– ne correspond pas à une voie C logique existante, alors:

  • l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "erreur d'identification de voie C logique";

  • l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

18.6.6.2 Erreur de type de message

A la réception d'un type de message non reconnu:

– l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie le message PROTOCOL ERROR indiquant la cause d'erreur de protocole "type de message non reconnu" comprenant le diagnostic correspondant, comme indiqué au 18.5.5;

– l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

18.6.6.3 Eléments d'information obligatoires répétés

Chaque fois qu'un élément d'information obligatoire est répété dans un message, l'entité de réception doit réagir comme suit:

– l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information obligatoire répété" comprenant le diagnostic correspondant comme indiqué au 18.5.5;

– l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

18.6.6.4 Elément d'information obligatoire manquant

Chaque fois qu'un message est reçu avec un élément d'information obligatoire manquant, l'entité de réception doit réagir comme suit:

– l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information obligatoire manquant" comportant le diagnostic correspondant, comme indiqué au 18.5.5;

– l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

Lorsqu'il manque plusieurs éléments d'information obligatoires, l'entité de réception réagit comme elle l'a fait pour le premier élément d'information obligatoire identifié comme manquant.

18.6.6.5 Elément d'information non reconnu

Chaque fois qu'un message est reçu avec un ou plusieurs éléments d'information non reconnus, l'entité de réception doit réagir comme suit:

– l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, supprime tous les éléments d'information non reconnus et poursuit le traitement du message; elle envoie également un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "élément d'information non reconnu" comportant le diagnostic correspondant, comme indiqué au 18.5.5;

– l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, supprime tous les éléments d'information non reconnus et poursuit le traitement du message.

En présence de plusieurs éléments d'information non reconnus, l'entité de réception réagit comme elle l'a fait lorsqu'elle a identifié le premier élément d'information non reconnu.

En matière de procédures de traitement d'erreur de protocole de protection, on entend par éléments d'information non reconnus ceux qui ne sont pas définis aux 13.2 et 18.5.

18.6.6.6 Erreur de contenu d'un élément d'information obligatoire

Lorsqu'un message reçu contient un élément d'information obligatoire comportant une erreur de contenu soit:

a) la longueur n'est pas conforme à celle indiquée aux 13.2 et 18.5;

b) le contenu n'est pas connu, alors:

- l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "erreur de contenu de l'élément d'information obligatoire" contenant le diagnostic correspondant, comme indiqué au 18.5.5;
- l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

En matière de procédures de traitement d'erreur, on entend par erreur de contenu d'élément d'information des points de code figurant dans un élément d'information particulier qui ne sont pas définis aux 13.2 et 18.5.

18.6.6.7 Message intempestif

Il y a erreur de flux de message lorsqu'on reçoit un message intempestif. Les messages intempestifs sont ceux expressément qualifiés d'intempestif dans les tableaux de transition d'état des entités de protocole de protection V5.2 du commutateur local et du réseau d'accès (voir Tableaux 65 et 66). Les tableaux de transition d'état indiquent les opérations à effectuer en pareille situation.

Lorsqu'un message intempestif est reçu, il n'y a pas de transition d'état. De plus:

- l'entité de protocole de protection du réseau d'accès envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes, ignore le message et envoie un message PROTOCOL ERROR indiquant la cause d'erreur de protocole "message incompatible avec l'état du protocole de protection" comportant le diagnostic correspondant, comme indiqué au 18.5.5;
- l'entité de protocole de protection du commutateur local envoie une primitive MDU-Protection (indication d'erreur de protocole) à la gestion-systèmes et ignore le message.

18.7 Liste de paramètres système

Les temporisateurs utilisés dans le protocole de protection sont définis dans le Tableau 64. Les temporisateurs mentionnés sont situés dans les entités de protocole de protection du commutateur local ou du réseau d'accès. Les tolérances de ces temporisateurs sont ±10%.

Tableau 64/G.965 – Temporisateurs du protocole de protection

Nom du temporisateur	Valeur de temporisation	Cause du démarrage	Arrêt normal	A la première expiration	A la seconde expiration	Référence
TSO1	1500 ms	SWITCH-OVER COM envoyé, passage à l'état SOLE1	Réception de SWITCH-OVER ACK	Retransmission de SWITCH-OVER COM	Indication d'erreur à la gestion-systèmes	18.6
TSO2	1500 ms	OS-SWITCH-OVER COM envoyé, passage à l'état SOLE1	Réception de SWITCH-OVER ACK	Retransmission de OS-SWITCH-OVER COM	Indication d'erreur à la gestion-systèmes	18.6
TSO3	1500 ms	SWITCH-OVER REQ envoyé, passage à l'état SOAN1	Réception de SWITCH-OVER COM	Retransmission de SWITCH-OVER REQ	Indication d'erreur à la gestion-systèmes	18.6
TSO4	20 s	RESET SN COM envoyé, passage à l'état ZÉRO	Réception de RESET SN ACK	Retransmission de RESET SN COM	Indication d'erreur à la gestion-systèmes	18.6
TSO5	10 s	Réception de RESET SN COM, passage à l'état ZÉRO	Le temporisateur TSO5 expirera toujours	Pas d'opération, pas de transition d'état	Sans objet	18.6

18.8 Tableaux d'état côté réseau d'accès et côté commutateur local

18.8.1 Machine FSM du protocole de protection du réseau d'accès

Le tableau de transition d'états propre à la machine FSM du protocole de protection du réseau d'accès fait l'objet du Tableau 65.

Tableau 65/G.965 – Machine FSM du protocole de protection du réseau d'accès

Etat	SOAN0	SOAN1	SOAN2
Nom de l'état / Evénement	ZÉRO	COMMUTATION DEMANDÉE PAR LE RÉSEAU D'ACCÈS	COMMUTATION DEMANDÉE PAR LE COMMUTATEUR LOCAL
MDU-Prot. (accusé de réception de commutation)	/	/	SWITCH-OVER ACK; SOAN0
MDU-Prot. (demande de commutation) (Note 1)	SWITCH-OVER REQ; démarrer TSO3; SOAN1	/	/
	MDU-Prot. (indication d'erreur de réinitialisation du numéro de séquence); –		
MDU-Prot. (rejet de commutation)	/	/	SWITCH-OVER REJECT; SOAN0
SWITCH-OVER COM (Note 1)	MDU-Prot. (commande de commutation); SOAN2	MDU-Prot. (commande de commutation); arrêter TSO3; SOAN2	/
	–		
OS-SWITCH-OVER COM (Note 1)	MDU-Prot. (commande de commutation OS); SOAN2	MDU-Prot. (commande de commutation OS); arrêter TSO3; SOAN2	/
	–		

Tableau 65/G.965 – Machine FSM du protocole de protection du réseau d'accès

Etat	SOAN0	SOAN1	SOAN2
Nom de l'état / Evénement	ZÉRO	COMMUTATION DEMANDÉE PAR LE RÉSEAU D'ACCÈS	COMMUTATION DEMANDÉE PAR LE COMMUTATEUR LOCAL
SWITCH-OVER REJECT (Note 1)	/	MDU-Prot. (indication de rejet de commutation); arrêter TSO3; SOAN0	/
	–		
Expiration du temporisateur TSO3 (première)	/	SWITCH-OVER REQUEST; démarrer TSO3; –	/
Expiration du temporisateur TSO3 (seconde)	/	MDU-Prot. (indication d'erreur de commutation); SOAN0	/
VP(S), VP(R) défaut d'alignement détecté	RESET SN COM; démarrer TSO4; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; –	RESET SN COM; démarrer TSO4; arrêter TSO3; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; SOAN0	RESET SN COM; démarrer TSO4; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; SOAN0
RESET SN COM (Note 2)	RESET SN ACK; positionner VP(S) = VP(R) = 0; démarrer TSO5; MDU-Prot. (indication de réinitialisation de numéro de séquence); –	RESET SN ACK; positionner VP(S) = VP(R) = 0; démarrer TSO5; arrêter TSO3; MDU-Prot. (indication de réinitialisation de numéro de séquence); SOAN0	RESET SN ACK; positionner VP(S) = VP(R) = 0; démarrer TSO5; MDU-Prot. (indication de réinitialisation de numéro de séquence); SOAN0
	–	–	–
RESET SN ACK (Note 1)	–	–	–
	Arrêter TSO4; MDU-Prot. (accusé de réception de réinitialisation de numéro de séquence); –		
Expiration du temporisateur TSO4 (première)	RESET SN COM; démarrer TSO4; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; –	/	/
Expiration du temporisateur TSO4 (seconde)	MDU-Prot. (indication d'erreur de réinitialisation de numéro de séquence); –	/	/
Expiration du temporisateur TSO5	–	–	–
Détection d'erreur de protocole (Note 1)	MDU-Prot. (indication d'erreur de protocole); PROTOCOL ERROR; –	MDU-Prot. (indication d'erreur de protocole); PROTOCOL ERROR; –	MDU-Prot. (indication d'erreur de protocole); PROTOCOL ERROR; –
	MDU-Prot. (indication d'erreur de protocole); –		

– Pas de transition d'état, pas d'action.

/ Evénement intempestif, pas de transition d'état, pas d'action.

NOTE 1 – L'option inférieure est choisie si le temporisateur TSO4 fonctionne.

NOTE 2 – L'option inférieure est choisie si le temporisateur TSO5 fonctionne.

18.8.2 Machine FSM du protocole de protection du commutateur local

Le tableau de transition d'états propre à la machine FSM du protocole de protection du commutateur local fait l'objet du Tableau 66.

Tableau 66/G.965 – Machine FSM du protocole de protection du commutateur local

Etat	SOLE0	SOLE1	SOLE2
Nom de l'état / Evénement	ZÉRO	COMMUTATION LANCÉE PAR LE COMMUTATEUR LOCAL	COMMUTATION DEMANDÉE PAR LE RÉSEAU D'ACCÈS
MDU-Prot. (demande de commutation) (Note 1)	SWITCH-OVER COM; démarrer TSO1; SOLE1	/	SWITCH-OVER COM; démarrer TSO1; SOLE1
	MDU-Prot. (indication d'erreur de réinitialisation du numéro de séquence); –		
MDU-Prot. (commande de commutation OS) (Note 1)	OS SWITCH-OVER COM; démarrer TSO2; SOLE1	/	OS SWITCH-OVER REQ; démarrer TSO2; SOLE1
	MDU-Prot. (indication d'erreur de réinitialisation du numéro de séquence); –		
MDU-Prot. (rejet de commutation)	/	/	SWITCH-OVER REJECT; SOLE0
SWITCH-OVER ACK (Note 1)	MDU-Prot. (accusé de réception de commutation); –	MDU-Prot. (accusé de réception de commutation); arrêter TSO1; arrêter TSO2; SOLE0	/
	–		
SWITCH-OVER REQ (Note 1)	MDU-Prot. (demande de commutation); SOLE2	–	/
	–		
SWITCH-OVER REJECT (Note 1)	MDU-Prot. (indication de rejet de commutation); –	MDU-Prot. (indication de rejet de commutation); arrêter TSO1; arrêter TSO2; SOLE0	/
	–		
Expiration du temporisateur TSO1 (première)	/	SWITCH-OVER COM; démarrer TSO1; –	/
Expiration du temporisateur TSO1 (seconde)	/	MDU-Prot. (indication d'erreur de commutation); SOLE0	/
Expiration du temporisateur TSO2 (première)	/	OS SWITCH-OVER COM; démarrer TSO2; –	/
Expiration du temporisateur TSO2 (seconde)	/	MDU-Prot. (indication d'erreur de commutation); SOLE0	/
VP(S), VP(R) défaut d'alignement détecté ou MDU-Prot.(demande de réinitialisation de numéro de séquence)	RESET SN COM; démarrer TSO4; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; –	RESET SN COM; démarrer TSO4; arrêter TSO1; arrêter TSO2; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; SOLE0	RESET SN COM; démarrer TSO4; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; SOLE0
RESET SN COM (Note 2)	RESET SN ACK; positionner VP(S) = VP(R) = 0; démarrer TSO5; MDU-Prot. (indication de réinitialisation de numéro de séquence); –	RESET SN ACK; positionner VP(S) = VP(R) = 0; démarrer TSO5; arrêter TSO1; arrêter TSO2; MDU-Prot. (indication de réinitialisation de numéro de séquence.); SOLE0	RESET SN ACK; positionner VP(S) = VP(R) = 0; démarrer TSO5; MDU-Prot. (indication de réinitialisation de numéro de séquence); SOLE0
	–	–	–
RESET SN ACK (Note 1)	–	–	–
	Arrêter TSO4; MDU-Prot. (accusé de réception de réinitialisation de numéro de séquence); –		

Tableau 66/G.965 – Machine FSM du protocole de protection du commutateur local

Etat	SOLE0	SOLE1	SOLE2
Nom de l'état / Evénement	ZÉRO	COMMUTATION LANCÉE PAR LE COMMUTATEUR LOCAL	COMMUTATION DEMANDÉE PAR LE RÉSEAU D'ACCÈS
Expiration du temporisateur TSO4 (première)	RESET SN COM; démarrer TSO4; MDU-Prot. (commande de réinitialisation de numéro de séquence); positionner VP(S) = VP(R) = 0; –	/	/
Expiration du temporisateur TSO4 (seconde)	MDU-Prot. (indication d'erreur de réinitialisation du numéro de séquence); –	/	/
Expiration du temporisateur TSO5	–	–	–
PROTOCOL ERROR (Cause) (Note 1)	MDU-Prot. (indication d'erreur de protocole); –	MDU-Prot. (indication d'erreur de protocole); –	MDU-Prot. (indication d'erreur de protocole); –
	–		

– Pas de transition d'état, pas d'action.

/ Evénement intempestif, pas de transition d'état, pas d'action.

NOTE 1 – L'option inférieure est choisie si le temporisateur TSO4 fonctionne.

NOTE 2 – L'option inférieure est choisie si le temporisateur TSO5 fonctionne.

ANNEXE A

Scénarios de service, architecture et définition fonctionnelle des configurations d'accès avec un réseau d'accès au commutateur local

A.1 Conclusions relatives aux applications d'interface V5 multiples

Le présent paragraphe est identique à celui du A.1/G.964 [8].

A.2 Conclusions relatives aux aspects architecturaux

Une interface V5.2 peut avoir au moins une et jusqu'à seize voies physiques à 2048 kbit/s.

Le nombre et la combinaison des interfaces V5.1 et V5.2 entre un réseau d'accès et un commutateur local particuliers sont illimités.

Les fonctions de couche 1 du terminal propres au service d'accès de base RNIS, définies dans l'UIT-T G.960 [4], sont réparties entre le réseau d'accès et le commutateur local (voir Figure 3).

Les fonctions de couche 1 du terminal propres au service d'accès au débit primaire RNIS, définies dans l'UIT-T G.962 [10], sont supervisées par le réseau d'accès.

La commutation de voies additionnelles entre le réseau d'accès et le commutateur local, par exemple, par une interconnexion indépendante, est autorisée à condition de ne pas avoir d'incidence sur les fonctions de l'interface V5.2 définies dans la présente Recommandation. Le raccordement en cascade de réseaux d'accès (par exemple, en les connectant à l'aide d'une interface de type V5) n'a pas d'incidence sur les fonctions de l'interface V5.2.

L'utilisation de l'interface V5 ne se limite pas uniquement à des réseaux d'accès et devrait être indépendante de leur architecture. La ou les interconnexions entre le réseau d'accès et le commutateur local sont considérées du point de vue de l'interface V5 comme faisant partie intégrante du réseau d'accès.

Il est possible de faire coexister à la fois des interfaces V5.1, V5.2 et V3.

A.3 Implémentation de l'interface Q_{AN}

Le contenu du présent paragraphe est identique à celui du A.3/G.964 [8].

A.4 Conditions d'implémentation de la fonction de ligne permanente via un accès de base RNIS

Le contenu du présent paragraphe est identique à celui du A.4/G.964 [8].

A.5 Conditions d'implémentation de la fonction de ligne permanente via un accès au débit primaire au RNIS

Les lignes permanentes contournent le commutateur local et ne relèvent pas des spécifications de l'interface V5.2. Etant donné que le point d'accès au débit primaire RNIS n'est pas actif en permanence, la présence d'une machine FSM dans le commutateur local n'est pas nécessaire pour assurer cette fonction.

Pour que le protocole BCC fonctionne correctement, il doit être administré par deux gestionnaires de ressources, l'un situé dans le commutateur local et l'autre dans le réseau d'accès. Dans la présente Recommandation on suppose que ces gestionnaires de ressources existent; leurs fonctions ne sont pas limitées.

Pour que les gestionnaires de ressources fonctionnent correctement, celui situé dans le commutateur local doit être informé des demandes formulées dans les intervalles de temps du point d'accès utilisateur qu'il commande. Ces informations doivent être transmises au système via l'interface Q_{CL}.

A.6 Hypothèses et conditions de prise en charge de lignes louées semi-permanentes

A.6.1 Généralités

Les lignes louées semi-permanentes passent par l'interface V5.2.

Pour l'interface V5.2 dans laquelle le protocole BCC établit la connexion pour tous les canaux supports entre le point d'accès utilisateur du réseau d'accès et le commutateur local, aucune procédure supplémentaire entre le commutateur local et le réseau d'accès n'est nécessaire pour la prise en charge de lignes louées semi-permanentes. Leur mise en œuvre est assurée via l'interface Q_{CL}.

Il appartient au réseau d'accès de profiler le point d'accès utilisateur conformément aux exigences de l'utilisateur; ce point ne relève donc pas des spécifications de l'interface V5.2.

A.6.2 Signalisation associée aux lignes louées semi-permanentes

Le contenu du présent paragraphe est identique à celui du A.5.2/G.964 [8].

A.6.3 Points d'accès utilisateur

Le contenu du présent paragraphe est identique à celui du A.5.3/G.964 [8].

A.6.4 Spécifications des points d'accès utilisateur non RNIS pour des lignes louées semi-permanentes

Le contenu du présent paragraphe est identique à celui du A.5.4/G.964 [8].

A.7 Exemple de configuration de réseau d'accès et de commutateur local

La Figure A.1 montre le cas de deux commutateurs locaux et de deux réseaux d'accès connectés entre eux via cinq interfaces V5 avec les valeurs d'identificateur d'interface V5 v5InterfaceID suivantes données: 1, 2, 3, 4, jusqu'à $2^{24} - 1$, (16777215). LE_1 est connecté à AN_1 et à AN_2 à l'aide d'interfaces V5 aussi bien de type V5.1 que V5.2 pour le même réseau d'accès. Aussi bien LE_1 que LE_2 sont connectés à AN_2 à l'aide d'interfaces V5 séparées de différents types.

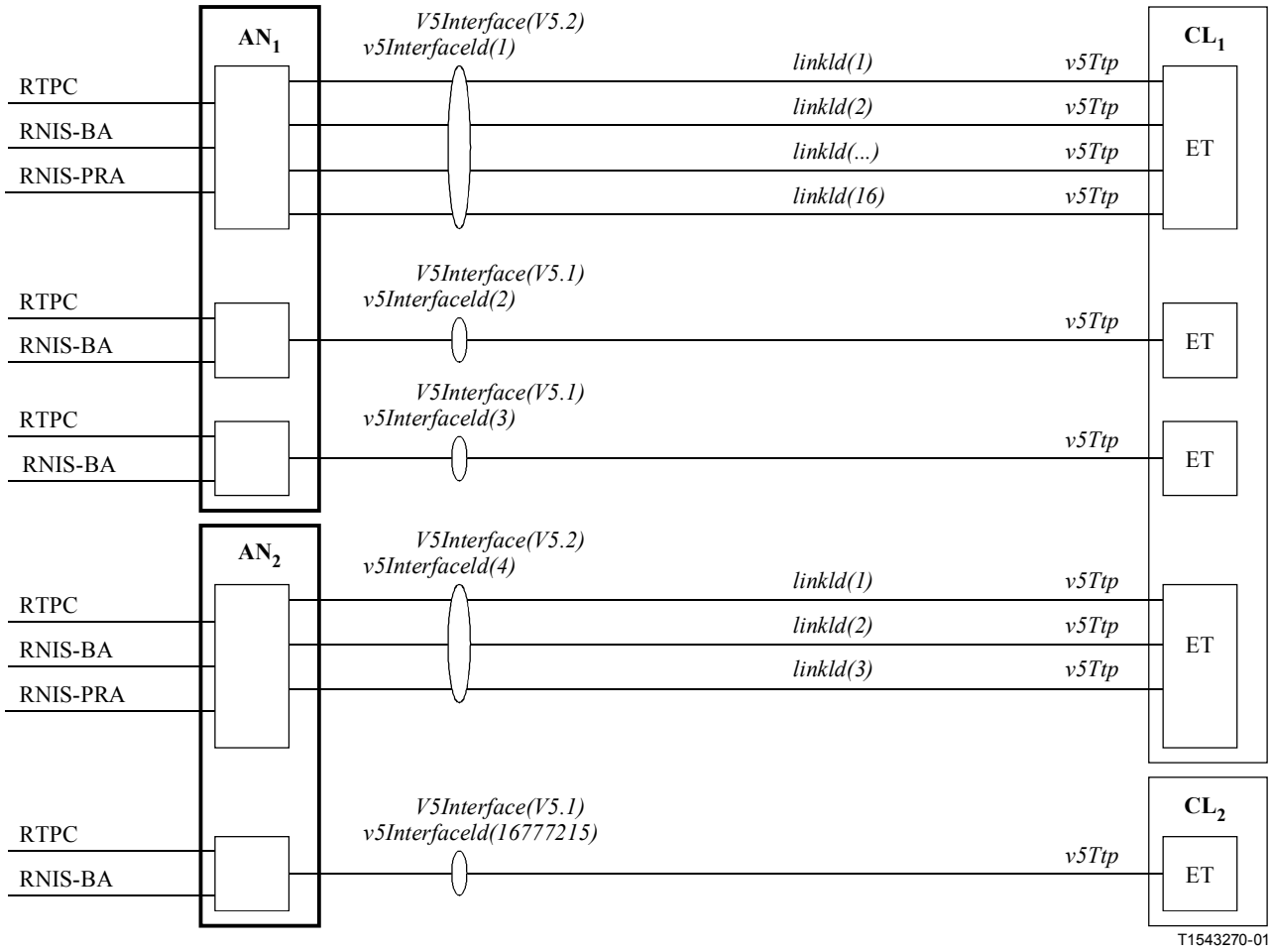


Figure A.1/G.965 – Configuration AN/CL possible, utilisant la norme V5

Pour V5.1, l'identificateur d'interface est unique pour tout ce qui se rapporte à cette interface particulière. Il en est de même pour V5.2 avec la différence que l'identificateur de voie linkID diffère pour chaque liaison à 2048 kbit/s.

La valeur de l'identificateur V5InterfaceId est définie dans la norme de gestion de configuration du commutateur local UIT-T Q.824.5 [12] à laquelle se réfère la norme de gestion de configuration du réseau d'accès. Cette valeur est établie par le nom distinctif relatif (RDN, *relative distinguished name*) de l'interface. L'identificateur v5InterfaceId doit être identique des deux côtés de l'interface V5 pour mener à bien les procédures de démarrage du système définies à l'Annexe C/G.964 [8].

Si le réseau comporte plus de deux opérateurs, il est nécessaire alors d'avoir une coordination de l'identificateur d'interface à l'intérieur du réseau avant que ne puissent débuter les activités de configuration. L'identificateur d'interface devrait être unique quelque part (qui n'est pas défini) dans le réseau. Il n'est pas suffisant qu'il soit unique dans l'élément managedElement.

ANNEXE B

Utilisation des éléments d'information de protocole pour les protocoles RTPC nationaux

Le contenu de la présente annexe est identique à celui de l'Annexe B/G.964 [8].

ANNEXE C

Prescriptions de base des fonctions de gestion-systèmes dans le réseau d'accès et dans le commutateur local

C.1 Procédure pour l'essai de continuité de l'accès RNIS au débit de base

Le contenu du présent paragraphe est identique au paragraphe C.1/G.964 [8].

C.2 Blocage de point d'accès

Le contenu du présent paragraphe est identique au paragraphe C.2/G.964 [8].

C.3 Collisions entre primitives

Le contenu du présent paragraphe est identique au paragraphe C.3/G.964 [8].

C.4 Détection par le réseau d'accès d'une anomalie physique et de performances inacceptables

Le contenu du présent paragraphe est identique au paragraphe C.4/G.964 [8].

C.5 Déblocage d'un point d'accès

Le contenu du présent paragraphe est identique au paragraphe C.5/G.964 [8].

C.6 Commande et profilage

Le contenu du présent paragraphe est identique au paragraphe C.6/G.964 [8].

C.7 Vérification de l'état du point d'accès

Pour le mécanisme de vérification du réseau d'accès on se réfèrera au paragraphe 15.3.3.4 et à l'UIT-T G.964 [8] (sous-paragraphes 14.1.3.4 et 14.2.3.4) et pour le mécanisme de vérification du commutateur local utilisant la primitive MPH-UBR, on se réfèrera au paragraphe 15.3.3.5 et à l'UIT-T G.964 [8] (sous-paragraphes 14.1.3.5 et 14.2.3.5).

C.8 Activation permanente de lignes RNIS

Se référer au paragraphe 15.3.3.3.6 et à la Note 1 du Tableau 36/G.964 [8] en ce qui concerne l'activation permanente de l'accès RNIS.

C.9 Coordination des machines FSM

Le contenu du présent paragraphe est identique au paragraphe C.9/G.964 [8].

C.10 Niveau d'erreurs sur la section numérique

Le contenu du présent paragraphe est identique au paragraphe C.10/G.964 [8].

C.11 Vérification du profilage

La procédure de vérification du profilage fait appel aux messages définis au 14.5/G.964 [8]; les éléments de protocole, le codage et les procédures sont définis aux 14.3/G.964 [8] et 14.4/G.964 [8].

Avant le reprofilage, il est conseillé de contrôler, au moyen du mécanisme de vérification, si la nouvelle variante de profilage est disponible à la fois dans le réseau d'accès et le commutateur local. A cet effet, la partie souhaitant le reprofilage émet la valeur "VERIFY RE-PROVISIONING" (vérifier le reprofilage) et reçoit:

– soit la valeur READY FOR RE-PROVISIONING (prêt pour reprofilage);
– soit la valeur NOT READY FOR RE-PROVISIONING (pas prêt pour reprofilage).

Dans ce dernier cas, c'est à la gestion-systèmes qu'appartiendra la responsabilité de la suite à donner.

C.12 Synchronisation du reprofilage

La procédure de synchronisation du reprofilage ne sera appliquée qu'au moment convenu pour le reprofilage. Cette procédure utilise les messages définis aux 14.3/G.964 [8] et 14.5/G.964 [8].

Reprofilage déclenché par la gestion du commutateur local

La procédure est représentée à la Figure C.1.

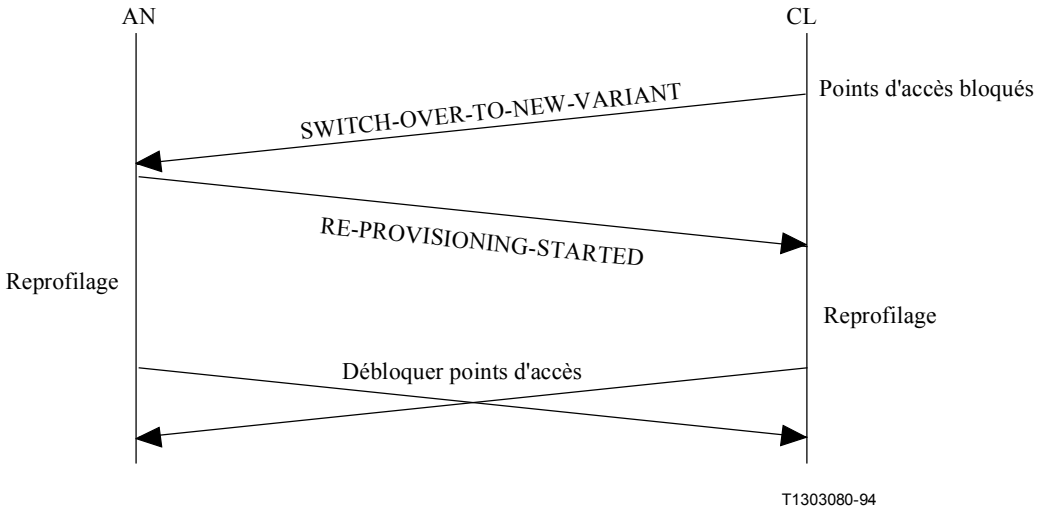


Figure C.1/G.965 – Procédure pour le reprofilage à l'initiative du commutateur local

Le commutateur local bloque tous les point d'accès concernés; il émet la valeur "SWITCH-OVER-TO-NEW-VARIANT" (passage à la nouvelle variante) et reçoit:

– soit la valeur "RE-PROVISIONING-STARTED" (reprofilage commencé);
– soit la valeur "CANNOT RE-PROVISION" (reprofilage impossible) avec la valeur correspondante de cause.

Dans le premier cas, le réseau d'accès commence le reprofilage après l'envoi de la valeur "RE-PROVISIONING-STARTED" et le commutateur local commence le reprofilage après la réception de la valeur "RE-PROVISIONING-STARTED"; quand le reprofilage est terminé, les deux extrémités commencent à débloquer les points d'accès au moyen du mécanisme de déblocage défini. Dans le second cas, le commutateur local se limite à informer sa gestion et peut débloquer des points d'accès.

Le réseau d'accès et le commutateur local peuvent retarder le reprofilage pour s'assurer de la remise, au réseau d'accès, de la valeur "RE-PROVISIONING-STARTED ACK".

Dans le second cas, c'est la gestion qui prendra les mesures qui s'imposent.

Reprofilage déclenché par la gestion du commutateur local

La procédure est représentée à la Figure C.2.

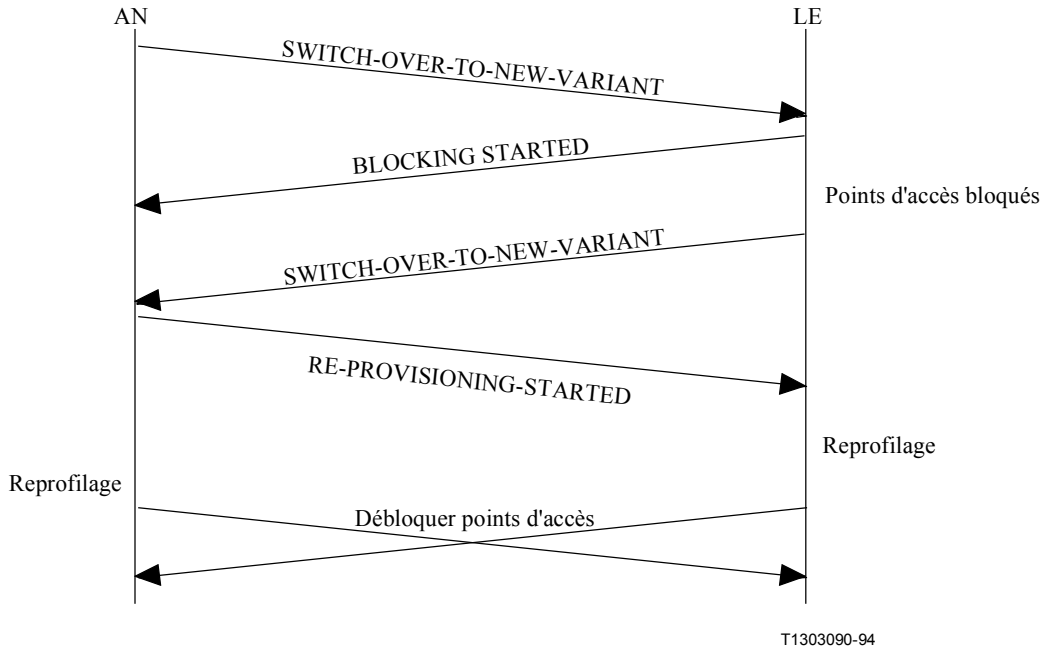


Figure C.2/G.965 – Procédure de reprofilage déclenchée par le réseau d'accès

Le réseau d'accès envoie la valeur "SWITCH-OVER-TO-NEW-VARIANT" (passage à la nouvelle variante). Si le commutateur local peut assumer le reprofilage, il commence à bloquer les points d'accès concernés et répond par la valeur "BLOCKING STARTED" (blocage commencé). La suite de la procédure est la même que dans le cas du reprofilage déclenché par le commutateur local. S'il n'y a pas de points d'accès à bloquer ou s'ils sont déjà bloqués, le commutateur local peut poursuivre immédiatement avec la valeur "SWITCH-OVER-TO-NEW-VARIANT".

Si le commutateur local ne peut pas faire le reprofilage, il répond à la valeur "SWITCH-OVER-TO-NEW-VARIANT" par la valeur "CANNOT RE-PROVISION" (reprofilage impossible). Dans ce cas, aucune autre disposition n'est prise au niveau du commutateur local.

Vérification du reprofilage

Il faut éventuellement demander l'identificateur de variante et d'interface avant de commencer à débloquer les points d'accès. Cette procédure évite une situation dans laquelle les points d'accès fonctionnent alors qu'il y a discordance d'identificateurs de variantes ou d'interfaces après le reprofilage.

Procédure de repli

On peut éventuellement "annuler" le reprofilage au moyen du mécanisme de synchronisation de reprofilage si la liaison du protocole de commande est encore active. Dans ce cas, la variante utilisée enverra un ensemble de données correspondant à l'ancien ensemble.

Application des procédures de reprofilage

Il y a des cas où les procédures de reprofilage V5 peuvent s'appliquer (affectant les deux côtés de V5: AN et CL):

a) reconfiguration du canal C;

b) mise à jour de V5.1 en V5.2.

Il y a des cas où ces procédures ne sont pas nécessaires (parce qu'elles n'affectent pas le service sur les autres points d'accès):

a) ajout, modification et suppression de points d'accès d'utilisateurs;

b) ajout et suppression de liaisons V5.2, uniquement utilisées pour des canaux supports.

C.13 Démarrage du système

Le profil par défaut contient les données de fourniture initiale pour le mappage entre les voies C logiques et physiques dans le réseau d'accès et dans le commutateur local. Le profil par défaut sera utilisé aussi bien dans le réseau d'accès que dans le commutateur local pour le démarrage du système. Aucune modification du profil par défaut n'est autorisée pendant le démarrage et dans l'état normal.

Par rapport au reste du présent paragraphe, les actions demandées pour tout élément non profilé doivent être ignorées.

Conditions préalables

Ce qui suit s'applique pour toute l'interface V5.2:

a) le profil par défaut pour la correspondance des voies C logiques et physiques;

b) BCC: tous les intervalles de temps sont désaffectés;

c) pour la liaison primaire, au moins la couche 1 et la surveillance du drapeau pour le temporisateur TS16 doivent être actifs. Autrement, la procédure exceptionnelle doit s'appliquer;

d) les états des machines FSM de commande de liaison doivent être initialisés de la façon suivante s'ils ne sont pas bloqués par la gestion-systèmes:

   A Les liaisons dans l'état anomalie de liaison (0.1 AN/CL) doivent rester dans cet état;

   B Les liaisons dans l'état anomalie de liaison et bloquées (0.2 AN/CL) doivent passer à l'état anomalie de liaison (0.1 AN/CL);

   C Les liaisons dans d'autres états doivent passer à l'état liaison opérationnelle (2.0 AN/CL).

e) les états initiaux des différentes machines FSM impliquées dans le démarrage d'une interface V5.2 sont les suivants:

   – machine FSM de protocole de commande commune – Hors service (AN0/CL0)

   – machine FSM de protocole de commande de liaison – Hors service (AN0/CL0)

   – machine FSM de protocole de commande d'accès – Hors service (AN0/CL0)

   – machines FSM d'état de point d'accès RTPC – Bloqué (AN1.0/CL1.0)

   – machines FSM d'état de point d'accès RNIS-BA – Bloqué (AN1.0/CL1.0)

– machines FSM d'état de point d'accès RNIS-PRA – Bloqué (AN1.0/CL1.0)
– machines FSM de signalisation RTPC – Accès bloqué (AN6/CL6)
– machine FSM de protocole BCC – Zéro (ANBcc0/CLBcc0)
– machine FSM de protocole de protection – Zéro (SOAN0/SOLE0)
– gestion-systèmes – Zéro (ANSYS0/LESYS0)

Procédure normale

a) activation de l'entité LAPV5_DL: la primitive de demande MDL-Establish doit être envoyée à toutes les entités LAPV5_DL. La primitive de demande MDL-Establish doit être envoyée aux deux liaisons de données de protection. L'activation des entités LAPV5_DL peut s'effectuer en suivant ou en parallèle. Si l'ordre séquentiel est choisi, il doit être le suivant: PROTECTION_DL, CONTROL_DL, LINK_CONTROL_DL, BCC_DL, et RTPC_DL.

NOTE 1 – La primitive de demande MDL-Establish n'est envoyée que si la liaison de données n'est pas déjà établie;

b) la procédure de rétablissement de numéro de séquence, telle qu'elle est décrite au paragraphe 18.6.2.3.1, s'applique lorsque l'établissement des liaisons de données a été effectué avec succès;

c) lorsqu'une primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH est reçue de la première de toutes les liaisons de données LAPV5, le temporisateur TC10 doit être lancé. Le temporisateur TC10 commande l'activation du mécanisme de commutation de protection pour la protection du démarrage du groupe 1. Des détails sur le traitement du temporisateur TC10 figurent au C.32;

d) lorsqu'une primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH est reçue de la liaison CONTROL_DL, la gestion-systèmes doit envoyer un message start-traffic à la machine FSM de protocole de commande commune;

e) lorsqu'une primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH est reçue de la liaison CONTROL_DL, LINK_CONTROL_DL et BCC_DL, le message start-traffic doit être envoyé aux machines FSM de protocole de commande d'accès et de protocole de commande de liaison. Il doit ensuite être vérifié que l'identificateur de variante et d'interface est bien identique à l'identificateur de variante et d'interface propre;

f) la gestion-systèmes:

– s'applique à la procédure de blocage de liaison. Ceci signifie que, pour les liaisons qui sont bloquées par la gestion-systèmes, la primitive MDU_LBI doit être envoyée aux machines FSM de commande de liaison concernées;

– peut appliquer la procédure d'identification de liaison. Si elle s'applique, la procédure d'identification de liaison doit être activée pour la liaison primaire et secondaire.

Ces deux procédures peuvent courir en séquence ou en parallèle;

g) passer à l'état normal;

h) après traitement;

NOTE 2 – A partir de ce moment, les procédures suivantes peuvent courir en parallèle.

A Si la procédure d'identification de liaison s'applique, elle peut débuter sur les liaisons restantes.

B Tous les points d'accès d'utilisateur pertinents doivent passer par la procédure de déblocage coordonnée. Les points d'accès utilisateur RTPC ne doivent être débloqués que si la sous-couche RTPC_DL est établie.

C Les actions de commutation de protection en cours pour le groupe 2 de protection doivent être effectuées et les procédures normales de protection s'appliquent alors.

Procédures exceptionnelles en cas d'anomalie dans le démarrage du système avant d'entrer dans l'état normal

Définitions

Démarrage de système réinitialisé: quand, pour une raison quelconque, le démarrage du système ne peut se poursuivre, il doit être réinitialisé par un processus de restauration d'intégrité du système du réseau d'accès ou du commutateur local. Ceci garantit que la gestion-systèmes est mise de façon répétée dans l'état SYSTEM STARTUP (démarrage du système). Les temporisations appropriées doivent être respectées avant la réinitialisation du démarrage du système, selon les conditions d'anomalie qui sont survenues (voir les détails au paragraphe C.29).

a) Commutation de protection dans le démarrage du système:

pendant le démarrage du système, la commutation de protection ne doit être utilisée que pour la voie C logique du groupe 1 de protection. La commutation de protection d'une voie C logique du groupe de protection 2 ne doit être autorisée que dans l'état normal.

b) Dans le cas d'anomalie de commande de liaison, de commande, de RTPC ou de BCC-DL du groupe de protection 1 dans des configurations multiliaisons et si la liaison secondaire est en fonctionnement, la procédure de commutation de protection peut être invoquée. La commutation de protection peut également s'appliquer dans le cas d'anomalie de surveillance de drapeau ou d'anomalie de liaison à 2048 kbit/s de la liaison active du groupe 1 de protection.

c) Anomalie de liaison de donnée pour les sous-couches de liaison de données de protection uniquement: si la primitive d'indication MDL-Release (indication de libération MDL) n'est reçue que pour une seule liaison de données de protection ou pour les deux liaisons de données de protection, la gestion-systèmes doit envoyer une primitive de demande MDL-Establish (demande d'établissement de MDL) à la ou aux liaisons de données de protection ayant une anomalie. Le démarrage du système ne doit pas être influencé par l'anomalie de la ou des liaisons de données de protection tant qu'aucune commutation de protection n'est nécessaire. Si les deux liaisons de données de protection sont indisponibles et qu'il devient nécessaire d'effectuer une commutation, le démarrage doit alors être réinitialisé.

d) Anomalie avec vérification d'identification de variante et d'interface: une vérification infructueuse de l'identificateur de variante et d'interface doit être notifiée à l'entité de gestion et le démarrage doit être réinitialisé. Dans le cas de l'expiration du temporisateur TV1, les actions décrites au paragraphe C.30 doivent être entreprises.

e) Anomalie de la sous-couche RTPC DL: si la sous-couche RTPC DL ne peut pas être établie, les points d'accès RTPC restent à l'état bloqué.

f) Anomalie de vérification de l'identificateur de liaison: si la vérification de l'identificateur de liaison a été effectuée pendant le démarrage du système et que la primitive FE-IDRej a été reçue pour une liaison, l'état de cette liaison ne doit pas changer. La vérification d'identificateur de liaison doit être répétée ultérieurement. Si le défaut de correspondance de l'identificateur de liaison est indiqué par la primitive MDU-EIg, la liaison doit être bloquée et la gestion-systèmes peut déclencher une procédure de commutation de protection autonome pour la voie C active du groupe 1 de protection sur cette liaison à 2048 kbit/s. Le démarrage du système peut se poursuivre après une commutation réussie ou la réception d'une primitive FE-IDRej.

g) Correction d'erreur pendant le démarrage: si pour une raison quelconque le démarrage du système ne peut se poursuivre et que la correction de l'erreur est encore possible (par exemple, correction d'anomalie de couche 1 de la liaison, commutation de protection réussie, etc), la réalisation du démarrage du système doit être suspendue. Après correction de la situation d'erreur, le démarrage doit reprendre à la dernière étape non achevée.

Pendant la correction d'erreur et si elle échoue, le démarrage du système doit être réinitialisé (se référer ci-dessus à la définition de la réinitialisation du démarrage du système).

NOTE 3 – Si la correction d'erreur échoue, le déclenchement du démarrage de la réinitialisation du système est garanti par l'expiration des temporisateurs pertinents de liaison de données (par exemple, TC2).

C.14 Procédure de redémarrage RTPC

La procédure de redémarrage RTPC sera invoquée par la gestion-systèmes dans le réseau d'accès ou dans le commutateur local après une anomalie d'exécution de la procédure RTPC_DL, décrite au paragraphe C.17.

Aucune procédure de redémarrage spécifique n'a été définie pour le protocole de commande. Au lieu de cela, la gestion-systèmes utilisera en cas de besoin la procédure de blocage et de déblocage individuel des points d'accès.

Une procédure de redémarrage RTPC doit être initialisée:

a) après une anomalie de sous-couche RTPC comme décrit au paragraphe C.17;

b) en cas de réception d'une primitive MDU-CTRL (demande de redémarrage) de l'entité de protocole de commande commune.

Dans le cas a), une primitive MDU-CTRL (demande de redémarrage) est envoyée à l'entité de protocole de commande commune et à toutes les machines FSM de point d'accès de protocole RTPC. Les temporisateurs TR1 et TR2 sont lancés.

Dans le cas b), une primitive MDU-CTRL (demande de redémarrage) est envoyée à toutes les machines FSM de point d'accès de protocole RTPC et les temporisateurs TR1 et TR2 sont lancés.

A réception de l'information de l'achèvement du redémarrage RTPC par l'entité homologue via la primitive MDU-CTRL (redémarrage effectué) en provenance de l'entité de protocole de commande commune, le temporisateur TR2 étant en cours, les actions suivantes doivent être accomplies:

– arrêter le temporisateur TR2;

– si le redémarrage de toutes les machines FSM de l'entité de protocole RTPC locale est achevé, ou si le temporisateur TR1 est arrivé à expiration, la primitive MDU-CTRL (redémarrage effectué) est envoyée aux machines FSM de protocole RTPC et la procédure se termine.

Si le temporisateur TR2 n'est pas en cours, la primitive MDU-CTRL (redémarrage effectué) doit être ignorée.

A réception de l'information de l'achèvement du redémarrage RTPC par toutes machines FSM de l'entité de protocole RTPC locale via des primitives MDU-CTRL (accusé de réception de redémarrage) en provenance de machines FSM de protocole RTPC, le temporisateur TR1 étant en cours, les actions suivantes doivent être accomplies:

– arrêter le temporisateur TR1;

– envoyer la primitive MDU-CTRL (redémarrage effectué) à l'entité de protocole de commande commune;

– si le redémarrage de l'entité homologue est achevé, la primitive MDU-CTRL (redémarrage effectué) est envoyée à toutes les machines FSM de protocole RTPC et la procédure se termine.

Si le temporisateur TR1 n'est pas en cours, la primitive MDU-CTRL (redémarrage effectué) doit être ignorée.

A expiration du temporisateur TR1, les actions suivantes doivent être accomplies:

– envoyer une indication d'erreur à l'entité de maintenance;

– envoyer la primitive MDU-CTRL (redémarrage effectué) à l'entité de protocole de commande commune;

– si le redémarrage de l'entité homologue est achevé, la primitive MDU-CTRL (redémarrage effectué) est envoyée à toutes les machines FSM de protocole RTPC et la procédure se termine.

A l'expiration du temporisateur TR2, les actions suivantes doivent être accomplies:

– envoyer une indication d'erreur à l'entité de maintenance;

– envoyer la primitive MDU-CTRL (redémarrage effectué) à toutes les machines FSM de protocole RTPC;

– terminer la procédure.

A réception de l'indication de redémarrage RTPC initialisée par la gestion-systèmes homologue via une primitive MDU-CTRL (demande de redémarrage) provenant de l'entité de protocole de commande commune alors que les temporisateurs TR1 ou TR2 sont en cours, l'entité de maintenance doit ignorer la primitive.

C.15 Procédure d'activation de la liaison de données

La procédure d'activation de données est décrite au C.13.

C.16 Réinitialisation de la liaison de données

La réception d'une primitive d'indication MDL-Establish émanant d'une liaison de données, que la gestion-systèmes considère comme étant déjà établie, doit être ignorée.

C.17 Anomalie sur une liaison de données

Les anomalies de liaisons de données doivent être détectées pour toute liaison de données lorsque survient un des événements suivants:

a) pour une liaison de données qui n'a pas encore été établie depuis l'initialisation du démarrage réel:

   expiration ou arrêt du temporisateur TC10 (voir au C.32).

b) pour une liaison de données établie:

   réception de la primitive d'indication MDL-Release.

Une anomalie de la liaison à 2048 kbit/s portant la voie C qui transporte la liaison de données (voir 18.1.5.1).

Une anomalie de surveillance du drapeau de la voie C qui transporte la liaison de données (voir 18.1.5.2).

Dans le cas d'une anomalie de la liaison de données pour Commande_DL, Commande de liaison_DL, BCC_DL et RTPC_DL, le temporisateur pertinent, respectivement TC1, TC3, TC4 et TC6, doit être lancé.

La gestion-systèmes doit continuellement essayer d'établir toutes les liaisons de données anormales même si une primitive d'indication MDL-RELEASE est émise de la liaison de données vers la gestion-systèmes avec les exceptions suivantes:

– anomalie de la liaison à 2048 kbit/s portant la voie C qui transporte la liaison de données (voir au paragraphe 18.1.5.1);

– une anomalie de surveillance du drapeau de la voie C qui transporte la liaison de données (voir le paragraphe 18.1.5.2).

Si l'anomalie de la liaison de données a été causée par l'un de ces deux événements, les liaisons de données affectées doivent être arrêtées immédiatement par l'envoi d'une primitive d'indication MDL-LAYER_1_FAILURE.

Les tentatives d'établissement doivent être recommencées lorsque la dernière des conditions d'anomalie a disparu.

NOTE – Ceci peut arriver comme conséquence d'une commutation de protection.

Si une primitive d'indication MDL-ESTABLISH ou de confirmation MDL-ESTABLISH est reçue après une primitive d'indication MDL-RELEASE, le temporisateur pertinent doit être arrêté. Si l'événement provient de la sous-couche CONTROL_DL ou LINK_CONTROL_DL et que le ou les protocoles ont été arrêtés, le ou les événements MDU-Start-traffic doivent être envoyés aux protocoles pertinents.

Si aucune primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH n'est reçue en provenance de la sous-couche RTPC_DL dans un intervalle de 15 secondes (temporisateur TC3), on doit demander le blocage de tous les accès RTPC comme décrit au paragraphe C.31. La procédure de redémarrage RTPC (voir le paragraphe C.14) doit être invoqué après le rétablissement de la sous-couche RTPC_DL. A l'achèvement du redémarrage RTPC, les points d'accès RTPC doivent être débloqués conformément au paragraphe C.31.

Si aucune primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH n'est reçue en provenance de la sous-couche CONTROL_DL dans un intervalle de 15 secondes (temporisateur TC1), une primitive MDU_stop_traffic doit être envoyée à toutes les entités du protocole de commande; le blocage des points d'accès RNIS doit être demandé par la gestion-systèmes concernée et le temporisateur TC2 (une minute) doit être démarré. A l'expiration du temporisateur TC2, le temporisateur TC8 doit être lancé. A l'expiration du temporisateur TC8, le démarrage du système doit être initialisé.

Si aucune primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH n'est reçue en provenance de la sous-couche LINK_CONTROL_DL dans un intervalle de 15 secondes (temporisateur TC4), une primitive MDU_stop_traffic doit être envoyée aux entités de commande de liaison (mais il n'y a pas blocage des liaisons) et le temporisateur TC5 (une minute) doit être démarré. A l'expiration du temporisateur TC5, le temporisateur TC8 doit être lancé. A l'expiration du temporisateur TC8, le démarrage du système doit être initialisé.

Si aucune primitive de confirmation MDL-ESTABLISH ou d'indication MDL-ESTABLISH n'est reçue en provenance de la sous-couche BCC_DL dans un intervalle de 15 secondes (temporisateur TC6), le temporisateur TC7 (une minute) doit être démarré. A l'expiration du temporisateur TC7, le temporisateur TC8 doit être lancé. A l'expiration du temporisateur TC8, le démarrage du système doit être initialisé.

C.18 Erreur du mécanisme de protection de couche 3 du protocole de commande

Le contenu du présent paragraphe est identique au C.18/G.964 [8].

C.19 Temporisateurs de l'entité de gestion-systèmes

Les temporisateurs de la gestion-systèmes du réseau d'accès et du commutateur local sont décrits dans le Tableau C.1. Tous les temporisateurs définis dans ce tableau ont une tolérance supérieure à ± 5%.

C.20 Application d'une procédure d'identification de liaison

Une identification de liaison peut être nécessaire une fois réparée l'anomalie sur une liaison de couche 1; le rétablissement de la liaison est indiqué par une primitive MPH-AI émanant de la machine FSM de couche 1 et signalé à la gestion-systèmes par une primitive MDU-LAI. Il appartient à la gestion-systèmes de demander la procédure d'identification de liaison. La gestion-systèmes peut avoir d'autres déclencheurs pour demander cette procédure. La gestion-systèmes ne peut demander qu'une seule fois la procédure d'identification de liaison pour toutes les interfaces V5 du réseau d'accès ou du commutateur local.

C.21 Réaction au résultat d'identification de liaison

Il appartient à la gestion-systèmes d'effectuer l'opération qui s'impose dès réception d'une information de la machine FSM de commande de liaison (par exemple, primitives MDU-IDRej, MDU-AI, MDU-EIg) à la suite d'une procédure d'identification de liaison que la gestion-systèmes a demandé à la machine FSM de commande de liaison.

C.22 Blocage de liaison et reprofilage

Il n'est pas nécessaire de bloquer les liaisons à 2048 kbit/s avant le reprofilage. Une fois le reprofilage achevé, les liaisons à 2048 kbit/s peuvent passer à l'état opérationnel; le déblocage de liaison devient alors inutile.

Tableau C.1/G.965 – Temporisateur de l'entité de gestion-systèmes

Tempo-risateur	Valeur de temporisation	Cause de démarrage	Arrêt normal	A expiration	Référence
TR1	100 secondes	MDU-CTRL (demande de redémarrage) à toutes les machines FSM du protocole RTPC	MDU-CTRL (accusé de réception de redémarrage) de toutes les machines FSM du protocole RTPC	Abandon de la procédure de redémarrage RTPC	C.14
TR2	120 secondes	MDU-CTRL (demande de redémarrage) envoyée à ou reçue de COMMON CONTROL	MDU-CTRL (redémarrage achevé) en provenance de COMMON CONTROL	Abandon du processus de redémarrage RTPC	C.14
TC1	15 secondes	Anomalie de liaison de données détectée pour la sous-couche CONTROL_DL	Réception de ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION en provenance de CONTROL-DL	Lancer le temporisateur TC2	C.17
TC2	60 secondes	Expiration du temporisateur TC1	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION en provenance de CONTROL-DL	Initialiser le redémarrage du système en lançant le temporisateur TC8	C.17
TC3	15 secondes	Anomalie de liaison de données détectée pour la sous-couche RTPC_DL	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION en provenance de RTPC-DL	Bloquer tous les points d'accès RTPC	C.17
TC4	15 secondes	Anomalie de liaison de données détectée pour la sous-couche LINK_CONTROL_DL	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION en provenance de LINK_CONTROL_DL	Lancer le temporisateur TC5	C.17

Tableau C.1/G.965 – Temporisateur de l'entité de gestion-systèmes

Tempo-risateur	Valeur de temporisation	Cause de démarrage	Arrêt normal	A expiration	Référence
TC5	60 secondes	Expiration du temporisateur TC4	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION de LINK_CONTROL_DL	Lancer le temporisateur TC8	C.17
TC6	15 secondes	Anomalie de liaison de données détectée pour la sous-couche BCC_DL	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION de BCC_DL	Lancer le temporisateur TC7	C.17
TC7	60 secondes	Expiration du temporisateur TC6	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH_INDICATION de BCC_DL	Lancer le temporisateur TC8	C.17
TC8	20 secondes	Expiration des temporisateurs TC2, TC5 ou TC7	Ce temporisateur arrive toujours à expiration	Initialiser le démarrage du système	C.29
TC9	95 secondes	Arrêt ou mise sous tension (c'est-à-dire redémarrage à froid) de l'interface V5	Ce temporisateur arrive toujours à expiration	Initialiser le démarrage du système si nécessaire	C.29
TC10	30 secondes	Réception de MDL-ESTABLISH-CONFIRM ou MDL-ESTABLISH-INDICATION en provenance de la première de toutes les liaisons de données LAPV5 en cours de démarrage	Passage à l'état normal (selon C.13) ou commutation de protection demandée par le côté distant	Voir C.32	C.32
TV1	15 secondes	MDU-CTRL (demande d'identité de variante et d'interface) envoyée à COMMON CONTROL	MDU-CTRL (identité de variante et d'interface) reçue de COMMON CONTROL	Mise en œuvre spécifique, voir le paragraphe de référence	C.30
TU1A	100 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RTPC et RNIS pertinents) envoyée	MDU-CTRL (acceptation du déblocage de tous les points d'accès RTPC et RNIS pertinents) reçue	Abandonner le processus	C.28
TU2A	60 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RTPC et RNIS pertinents) reçue ou envoyée	MDU-CTRL (achèvement du déblocage de tous les points d'accès RTPC et RNIS pertinents) reçue	Débloquer les points d'accès RTPC et RNIS pertinents	C.28

Tableau C.1/G.965 – Temporisateur de l'entité de gestion-systèmes

Tempo-risateur	Valeur de temporisation	Cause de démarrage	Arrêt normal	A expiration	Référence
TU1B	100 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RTPC pertinents) envoyée	MDU-CTRL (acceptation du déblocage de tous les points d'accès RTPC pertinents) reçue	Abandonner le processus	C.28
TU2B	60 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RTPC pertinents) reçue ou envoyée	MDU-CTRL (achèvement du déblocage de tous les points d'accès RTPC pertinents) reçue	Débloquer les points d'accès RTPC pertinents	C.28
TU1C	100 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RNIS pertinents) envoyée	MDU-CTRL (acceptation du déblocage de tous les points d'accès RNIS pertinents) reçue	Abandonner le processus	C.28
TU2C	60 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RNIS pertinents) reçue ou envoyée	MDU-CTRL (achèvement du déblocage de tous les points d'accès RNIS pertinents) reçue	Débloquer les points d'accès RNIS pertinents	C.28
TU1D	100 secondes	MDU-CTRL (demande de blocage de tous les points d'accès RTPC) envoyée	MDU-CTRL (acceptation du blocage de tous les points d'accès RTPC) reçue	Abandonner le processus	C.28
TU2D	60 secondes	MDU-CTRL (demande de blocage de tous les points d'accès RTPC) reçue ou envoyée	MDU-CTRL (achèvement du blocage de tous les points d'accès RTPC) reçue	Bloquer les points d'accès RTPC	C.28
TU1E	100 secondes	MDU-CTRL (demande de blocage de tous les points d'accès RNIS) envoyée	MDU-CTRL (acceptation du blocage de tous les points d'accès RNIS) reçue	Abandonner le processus	C.28
TU2E	60 secondes	MDU-CTRL (demande de déblocage de tous les points d'accès RNIS) reçue ou envoyée	MDU-CTRL (achèvement du blocage de tous les points d'accès RNIS) reçue	Bloquer les points d'accès RNIS	C.28

C.23 Configuration à liaison unique et mécanisme de protection

Dans une interface V5.2 ne comportant qu'une seule liaison, le protocole de protection ne sera pas mis en œuvre. La gestion-systèmes ne doit pas invoquer l'établissement de la liaison de données de protection et doit le cas échéant ignorer une primitive d'indication MDL-RELEASE provenant d'une liaison de données de protection.

C.24 Rétablissement de liaisons de données après commutation de protection

En cas de commutation de protection de voies C pour le protocole RTPC, la commande commune et la commande de point d'accès, la commande de liaison ou le protocole BCC, la gestion-systèmes du commutateur local doit demander le rétablissement de la ou des liaisons de données pertinentes en envoyant une primitive de demande MDL-ESTABLISH.

C.25 Initialisation V5.2 et données de protocole

Pendant l'initialisation de l'interface V5.2, c'est-à-dire pendant ou après le reprofilage, toutes les données destinées au protocole de protection, au protocole BCC, au protocole de commande de liaison et au protocole de commande commun doivent être remises à la valeur par défaut. Ceci n'est pas nécessaire pour la partie commande de point d'accès car tous les points d'accès sont bloqués avant le début du reprofilage et doivent être débloqués un à un après. La procédure de redémarrage définie dans l'UIT-T G.964 [8] s'applique pour le protocole RTPC.

C.26 Traitement des rejets d'affectation BCC par la gestion-systèmes

La gestion-systèmes doit enregistrer les informations fournies par le gestionnaire de ressource BCC que le système opérationnel peut retrouver pour l'identification du niveau de performance. Des rejets d'affectation fréquents peuvent par ailleurs entraîner l'envoi d'une indication autonome au système d'exploitation afin d'attirer l'attention du fournisseur de service sur la situation. D'autres mesures peuvent alors être prises à un niveau supérieur.

C.27 Erreur du mécanisme de protection de couche 3 du protocole de commande de liaison

La réception d'une "indication d'erreur" émanant du mécanisme de protection de couche 3 du protocole de commande de la liaison, peut indiquer qu'il y a défaut d'alignement entre les machines FSM de commande de liaison du réseau d'accès et du commutateur local. Il sera peut-être utile d'effectuer les opérations de gestion suivantes:

– vider la file d'attente de messages pour le protocole de commande de liaison;
– vérifier l'état (opérationnel) en envoyant la primitive "débloquer";
– pour les liaisons pour lesquelles l'état ne peut être précisé, forcer le réalignement à l'aide des séquences normales "bloquer/débloquer".

C.28 Procédures de verrouillage accéléré

Les procédures d'alignement accélérées permettent l'alignement de l'état des points d'accès sans envoyer de messages de blocage et déblocage pour chaque point d'accès individuel. Les procédures sont définies comme suit:

a) débloquer tous les points d'accès RTPC et RNIS pertinents:

a1) lorsque l'alignement de déblocage est nécessaire pour tous les points d'accès RTPC et tous les points d'accès de base et primaires RNIS de l'interface, une primitive MDU-CTRL (demande de déblocage de tous les points d'accès RTPC et RNIS pertinents) doit être envoyée à l'entité de protocole de commande. Le temporisateur TU1A doit être lancé.

A réception d'une primitive MDU-CTRL (acceptation de déblocage de tous les points d'accès RTPC et RNIS pertinents) en provenance de l'entité de protocole de commande commune, le temporisateur TU1A doit être arrêté. Tous les points d'accès RTPC et RNIS pertinents doivent passer directement à l'état débloqué sans aucune négociation avec l'entité homologue, excepté ceux qui sont considérés comme impropres à l'état débloqué (le dernier doit être bloqué à nouveau pour le réalignement mutuel à la fin de la procédure). Une primitive MDU-CTRL (achèvement du déblocage de tous les points

d'accès RTPC et RNIS pertinents) doit être envoyée à l'entité de protocole de commande commune, et le temporisateur TU2A doit être lancé.

A réception d'une primitive MDU-CTRL (achèvement du déblocage de tous les points d'accès RTPC et RNIS pertinents) en provenance de l'entité de protocole de commande commune, le temporisateur TU2A doit être arrêté. La primitive MPH-BI doit être envoyée à celles des machines FSM d'état de point d'accès RTPC dont les points d'accès sont considérés comme impropres à l'état de blocage. A réception d'une primitive MDU-CTRL (rejet du déblocage de tous les points d'accès RTPC et RNIS pertinents), le temporisateur TU1A doit être arrêté et le processus abandonné. Cela doit être notifié à l'entité de maintenance.

A expiration du temporisateur TU1A, le processus doit être abandonné. Cela doit être notifié à l'entité de maintenance.

A expiration du temporisateur TU2A, une primitive MPH-BI doit être envoyée à celles des machines FSM d'état de point d'accès RTPC dont les points d'accès sont considérés comme impropres à l'état de blocage.

a2) A réception d'une primitive MDU-CTRL (demande du déblocage de tous les points d'accès RTPC et RNIS pertinents), une primitive MDU-CTRL (acceptation du déblocage de tous les points d'accès RTPC et RNIS pertinents) doit être envoyée à l'entité de protocole de commande commune. Après avoir débloqué tous les points d'accès RTPC et RNIS pertinents, une primitive MDU-CTRL (achèvement du déblocage de tous les points d'accès RTPC et RNIS pertinents) doit être envoyée à l'entité de protocole de commande commune et le temporisateur TU2A doit être lancé.

a3) Si, après avoir envoyé une primitive MDU-CTRL (demande du déblocage de tous les points d'accès RTPC et RNIS pertinents), le côté réseau d'accès ou commutateur local reçoit une primitive MDU-CTRL (demande du déblocage de tous les points d'accès RTPC et RNIS pertinents) avant une primitive MDU-CTRL (acceptation du déblocage de tous les points d'accès RTPC et RNIS pertinents), il doit alors envoyer une primitive MDU-CTRL (acceptation du déblocage de tous les points d'accès RTPC et RNIS pertinents) à l'entité de protocole de commande commune.

b) Débloquer tous les points d'accès RTPC pertinents:

la procédure débloquer tous les points d'accès RTPC pertinents se fait selon la procédure débloquer tous les points d'accès RTPC et RNIS pertinents avec les exceptions suivantes:

- le type de point d'accès à utiliser est uniquement RTPC;
- les temporisateurs TU1B et TU2B doivent être utilisés au lieu des temporisateurs TU1A et TU2A.

c) Débloquer tous les points d'accès RNIS pertinents (accès de base RNIS et accès primaire RNIS):

la procédure débloquer tous les points d'accès RNIS pertinents se fait selon la procédure débloquer tous les points d'accès RTPC avec les exceptions suivantes:

- le type de point d'accès à utiliser est l'accès de base RNIS et l'accès primaire RNIS;
- les temporisateurs TU1C et TU2C doivent être utilisés au lieu des temporisateurs TU1A et TU2A.

d) Bloquer tous les points d'accès RTPC:

d1) lorsque l'alignement de blocage est nécessaire pour tous les points d'accès RTPC de l'interface, une primitive MDU-CTRL (demande de blocage de tous les points d'accès RTPC) doit être envoyée à l'entité de protocole de commande. Le temporisateur TU1D doit être lancé.

A réception d'une primitive MDU-CTRL (acceptation de blocage de tous les points d'accès RTPC) en provenance de l'entité de protocole de commande commune, le temporisateur TU1D doit être arrêté. Tous les points d'accès RTPC doivent passer directement à l'état bloqué sans aucune négociation avec l'entité homologue, y compris ceux qui sont considérés comme impropres (le dernier doit être débloqué à nouveau à l'initiative du côté qui a fait la demande, à la fin de la procédure). Une primitive MDU-CTRL (achèvement du blocage de tous les points d'accès RTPC) doit être envoyée à l'entité de protocole de commande commune, et le temporisateur TU2D doit être lancé.

A réception d'une primitive MDU-CTRL (achèvement du blocage de tous les points d'accès RTPC) en provenance de l'entité de protocole de commande commune, le temporisateur TU2D doit être arrêté. La primitive MPH-UBR doit être envoyée à celles des machines FSM d'état de point d'accès RTPC dont les points d'accès sont considérés comme impropres à l'état de blocage. A réception d'une primitive MDU-CTRL (rejet du blocage de tous les points d'accès RTPC), le temporisateur TU1D doit être arrêté et le processus abandonné. Cela doit être notifié à l'entité de maintenance.

A expiration du temporisateur TU1D, le processus doit être abandonné. Cela doit être notifié à l'entité de maintenance.

A expiration du temporisateur TU2D, une primitive MPH-UBR doit être envoyée à celles des machines FSM d'état de point d'accès RTPC dont les points d'accès sont considérés comme impropres à l'état de blocage.

d2) A réception d'une primitive MDU-CTRL (demande de blocage de tous les points d'accès RTPC), une primitive MDU-CTRL (acceptation du blocage de tous les points d'accès RTPC) doit être envoyée à l'entité de protocole de commande commune. Après avoir bloqué tous les points d'accès RTPC, une primitive MDU-CTRL (achèvement du blocage de tous les points d'accès RTPC) doit être envoyée à l'entité de protocole de commande commune et le temporisateur TU2D doit être lancé.

d3) Si, après avoir envoyé une primitive MDU-CTRL (demande de blocage de tous les points d'accès RTPC), le côté réseau d'accès ou commutateur local reçoit une primitive MDU-CTRL (demande de blocage de tous les points d'accès RTPC) avant une primitive MDU-CTRL (acceptation du blocage de tous les points d'accès RTPC), il doit alors envoyer une primitive MDU-CTRL (acceptation du blocage de tous les points d'accès RTPC) à l'entité de protocole de commande commune.

e) Bloquer tous les points d'accès RNIS:

la procédure bloquer tous les points d'accès RNIS se fait selon la procédure bloquer tous les points d'accès RTPC avec les exceptions suivantes:

- le type de point d'accès à utiliser est l'accès de base RNIS et l'accès au débit primaire RNIS au lieu du point d'accès de type RTPC;
- les temporisateurs TU1E et TU2E doivent être utilisés au lieu des temporisateurs TU1D et TU2D.

f) Réalisation simultanée des procédures d'alignement accéléré:

les procédures d'alignement accéléré sont symétriques et peuvent s'appliquer d'un côté ou de l'autre de l'interface V5.2. L'alignement accéléré initialisé par le commutateur local a priorité sur la procédure initialisée par le réseau d'accès dans le cas de collision de demandes en provenance de l'accès réseau et du commutateur local. Cette priorité ne s'applique que lorsque les demandes d'alignement venant du commutateur local et du réseau d'accès sont de natures différentes (c'est-à-dire si ces demandes sont incompatibles ou contradictoires). La procédure reste symétrique si les demandes du réseau d'accès et du commutateur local sont identiques.

La procédure débloquer tous les points d'accès RTPC et RNIS pertinents ne doit pas être accomplie en parallèle avec aucune des autres procédures d'alignement accéléré décrites ci-dessus.

La procédure débloquer tous les points d'accès RTPC pertinents et la procédure débloquer tous les points d'accès RNIS pertinents peuvent être accomplies en parallèle.

La procédure bloquer tous les points d'accès RTPC et la procédure bloquer tous les points d'accès RNIS peuvent être accomplies en parallèle.

La procédure bloquer tous les points d'accès RTPC ne doit pas être accomplie en parallèle avec la procédure débloquer tous les points d'accès RTPC pertinents.

La procédure bloquer tous les points d'accès RNIS ne doit pas être accomplie en parallèle avec la procédure débloquer tous les points d'accès RNIS pertinents.

La procédure bloquer tous les points d'accès RTPC et la procédure débloquer tous les points d'accès RNIS pertinents peuvent être accomplies en parallèle.

La procédure bloquer tous les points d'accès RNIS et la procédure débloquer tous les points d'accès RTPC pertinents peuvent être accomplies en parallèle.

C.29 Traitement des temporisateurs TC8 et TC9

Ces temporisateurs sont utilisés pour commander la réinitialisation du démarrage d'un système.

Le temporisateur TC8 déclenche le démarrage du système dans le cas d'anomalies de liaison de données. Il est nécessaire pour garantir qu'après un échec d'établissement de liaison de données, les deux côtés sont retournés au profil par défaut. La temporisation TC9 est le temps minimal pendant lequel un système doit être arrêté avant de retourner en service. Elle est lancée lorsque le système s'est arrêté pour une raison quelconque pendant le démarrage du système ou pendant le fonctionnement normal. Elle doit aussi courir avant l'invocation du redémarrage du système lors de la réalisation d'un démarrage à froid.

A l'expiration des temporisateurs TC2, TC5 ou TC7, on applique ce qui suit:

– l'interface doit être amenée à un état dans lequel il n'existe pas de liaison de données LAPV5 établie;

– lancement du temporisateur TC8;

– à expiration du temporisateur TC8, le démarrage du système doit s'accomplir.

Si le système est arrêté par une demande du système opérationnel, on applique ce qui suit:

– arrêt du temporisateur TC9;

– le démarrage du système ne peut s'accomplir qu'après l'expiration du temporisateur TC9.

Si pour une autre raison un des côtés (réseau d'accès ou commutateur local) détermine le besoin de réinitialiser un démarrage de système, on applique ce qui suit:

– l'interface doit être amenée à un état dans lequel il n'existe pas de liaison de données LAPV5 établie;

– lancement du temporisateur TC9;

– à expiration du temporisateur TC9, le démarrage du système doit s'accomplir.

C.30 Traitement du temporisateur TV1

Ce temporisateur est utilisé pour commander la vérification d'identité de la variante et d'interface.

Le temporisateur TV1 doit être lancé dès l'envoi du message MDU (demande d'identité de variante et d'interface). A la première expiration du temporisateur TV1, le message MDU (demande d'identité de variante et d'interface) doit être répété et le temporisateur TV1 relancé. Si le temporisateur TV1

arrive à expiration pour la seconde fois, cela doit être notifié à l'entité de gestion et le système doit être redémarré ou la vérification d'identité de variante et d'interface doit être répétée périodiquement. Le temporisateur TV1 doit être arrêté lorsque l'identité de variante et d'interface est reçue de l'entité homologue.

C.31 Harmonisation du blocage/déblocage entre protocoles de commande et RTPC

Le contenu du présent paragraphe est identique à celui du C.23/G.964 [8].

C.32 Traitement du temporisateur TC10

Ce temporisateur est utilisé pour commander l'activation du mécanisme de commutation de protection pour le démarrage du groupe 1 de protection et pour définir une anomalie de liaison de données pour une liaison de données qui n'a pas encore été établie lors du démarrage réel.

Le temporisateur TC10 doit être lancé à réception de la primitive de confirmation MDL-Establish ou d'indication MDL-Establish venant de la première de toutes les liaisons de données V5.2 en cours de démarrage, et il ne doit pas être permis de demander la procédure de commutation de protection pour le groupe 1 de protection pendant la durée du temporisateur TC10. Il doit être arrêté à l'entrée dans l'état normal (conformément au C.13) ou à réception d'une demande de procédure de commutation de protection venant du côté distant.

A expiration du temporisateur TC10, on applique ce qui suit:

- activation du mécanisme de commutation de protection pour le groupe 1 de protection;
- évaluation des états des liaisons de données, détection de toute anomalie de liaison de données (voir C.17/G.964 [8]);
- vérifier toute cause de commutation de protection existante pour le groupe 1 de protection qui serait suivie des actions décrites au paragraphe 18.

Si le temporisateur TC10 est arrêté à réception d'une demande de procédure de commutation de protection en provenance du côté distant, on applique ce qui suit:

- activation du mécanisme de commutation de protection pour le groupe 1 de protection, c'est-à-dire accomplir la procédure demandée;
- évaluation des états des liaisons de données, détection de toute anomalie de liaison de données (voir C.17/G.964 [8]).

Si le temporisateur TC10 au passage à l'état normal, on applique ce qui suit:

- activation du mécanisme de commutation de protection pour le groupe 1 de protection;
- évaluation des états des liaisons de données, détection de toute anomalie de liaison de données (voir C.17/G.964 [8]);
- vérifier toute cause de commutation de protection existante pour le groupe 1 de protection qui serait suivie des actions décrites au paragraphe 18.

ANNEXE D

Architecture de protocole pour la commande du point d'accès utilisateur RTPC et RNIS (accès de base et accès au débit primaire)

D.1 Domaine d'application

La présente annexe décrit l'architecture de protocole pour le transfert de l'information de commande de l'état des points d'accès utilisateur RNIS (accès de base et accès au débit primaire) et RTPC.

D.2 Commande d'état du point d'accès RNIS-accès de base

Le contenu du présent paragraphe est identique à celui du D.2/G.964 [8].

D.3 Commande d'état du point d'accès utilisateur RNIS au débit primaire

D.3.1 Séparation fonctionnelle entre commutateur local et réseau d'accès

Pour les points d'accès RNIS au débit primaire qui ne sont pas directement reliés au commutateur local mais auxquels on peut avoir accès à distance via un réseau d'accès, les fonctions de couche 1 de l'ET sont réparties entre le commutateur local et le réseau d'accès.

En principe, le commutateur local ne sera informé que de la disponibilité de la couche 1 du point d'accès utilisateur (opérationnelle/non opérationnelle).

Etant donné que la maintenance de la section numérique d'accès et des lignes d'abonné relève du réseau d'accès, le fonctionnement des essais en boucle ou d'autres essais sur la section numérique ne sera contrôlé que par le réseau d'accès. Ainsi, aucune information concernant ces fonctions n'est transmise au commutateur local (FE-A-FE-Y). L'identification correcte de l'état du point d'accès relève de la machine FSM du point d'accès du réseau d'accès qui doit indiquer cet état au commutateur local.

D.3.2 Transfert d'information entre le commutateur local et le réseau d'accès

La Figure D.1 illustre le modèle d'architecture de protocole propre aux fonctions de commande du point d'accès utilisateur RNIS au débit primaire.

Pour le transfert bidirectionnel de l'information entre les deux machines FMS des points d'accès d'utilisateur (RNIS au débit primaire) du réseau d'accès et du commutateur local on utilise les éléments fonctionnels (FE20x). Ils sont transportés sur le protocole de commande de couche 3. Ce protocole comprend une procédure d'accusé de réception pour éviter la perte de trames individuelles.

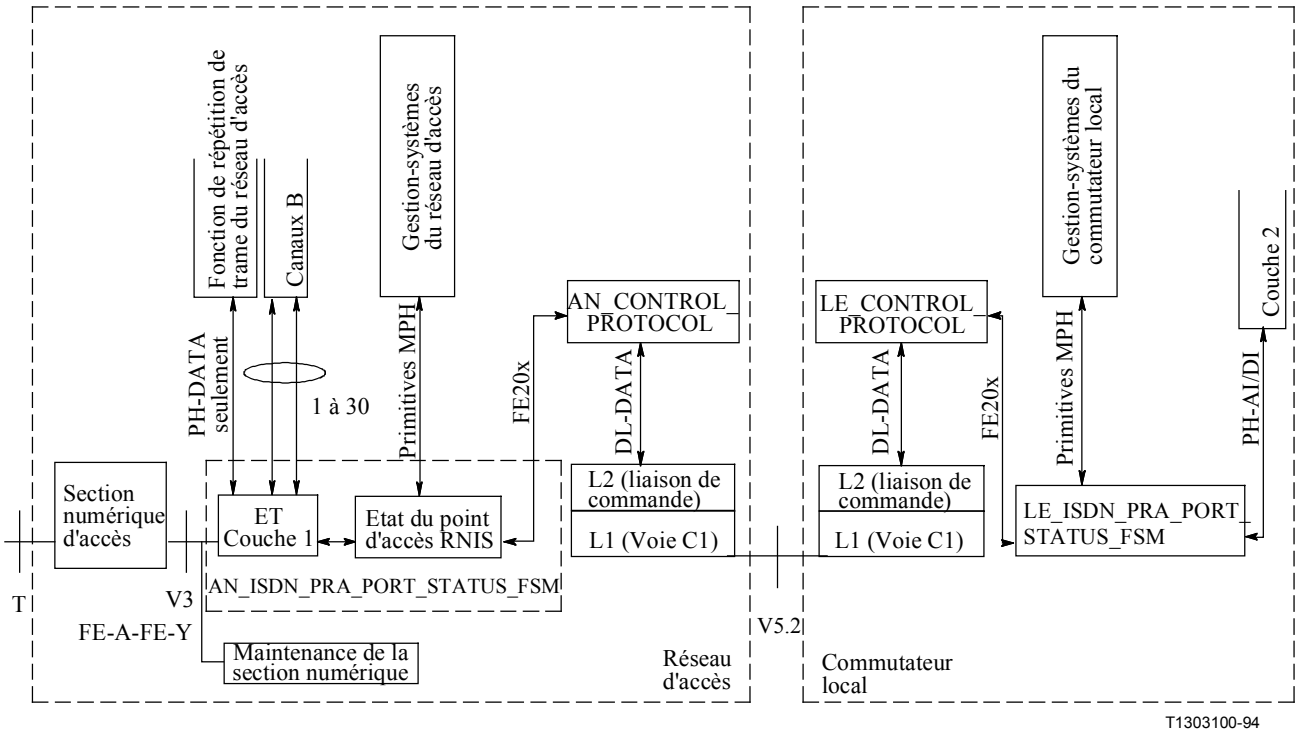


Figure D.1/G.965 – Architecture de protocole propre aux fonctions de commande du point d'accès RNIS – Accès au débit primaire

D.3.3 Activation/désactivation

Etant donné que les points d'accès RNIS au débit primaire sont activés en permanence, il n'y a pas de procédure d'activation/ désactivation, c'est-à-dire que les éléments fonctionnels relatifs à l'activation/désactivation (FE10x) ne sont pas utilisés à l'interface V5.2 pour les points d'accès utilisateur RNIS au débit primaire.

La couche 2 et la gestion-systèmes du commutateur local ne sont informées que de l'état opérationnel du point d'accès utilisateur RNIS au débit primaire par l'envoi de primitives PH-AI/DI et MPH-AI/DI, respectivement.

D.4 Commande de point d'accès utilisateur RTPC

Le contenu du présent paragraphe est identique à celui du D.3/G.964 [8].

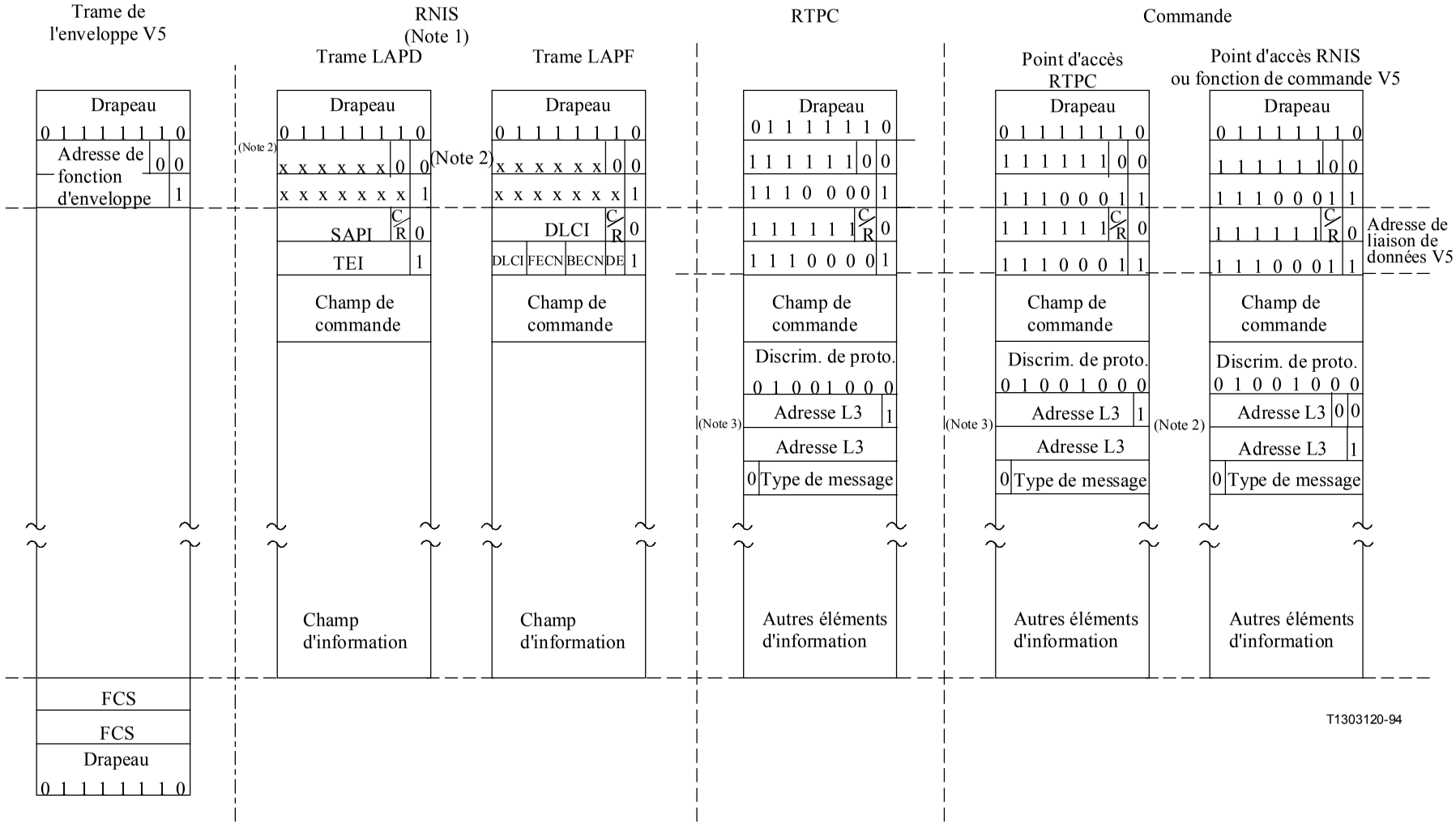
ANNEXE E

Structures de trame, points de code de messages et schéma d'adressage pour l'interface V5.2

Les Figures E.1 et E.2 illustrent les structures possibles des trames transportées dans les divers voies et protocoles de communication.

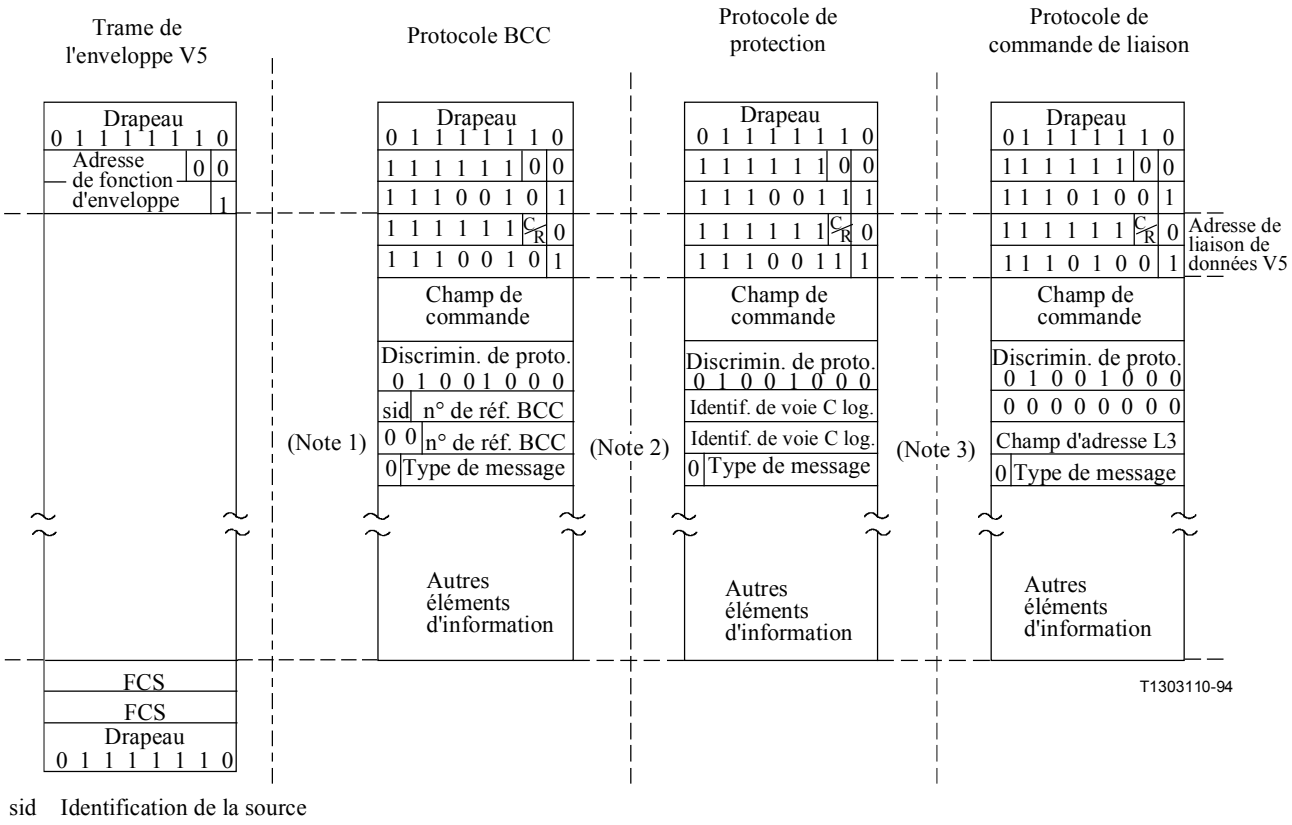
Le Tableau E.1 montre les types de messages affectés à l'interface V5.2.

Le Tableau E.2 montre les éléments d'information affectés à l'interface V5.2.



NOTE 1 – Dans le cas du RNIS, les champs d'adresse, de commande et d'information des trames de couche 2 RNIS ne sont pas modifiées à l'interface V5.2.
NOTE 2 – Pour un point d'accès RNIS donné, les champs d'adresse ont la même valeur.
NOTE 3 – Pour un point d'accès RTPC donné, les champs d'adresse ont la même valeur.

Figure E.1/G.965 – Formats de trame utilisés dans l'interface V5.2



sid Identification de la source

NOTE 1 – Le numéro de référence BCC identifie un processus de protocole BCC particulier.
NOTE 2 – L'identification de la voie C logique identifie une voie de communication logique particulière.
NOTE 3 – Le champ d'adresse L3 identifie une liaison de couche 1 particulière.

Figure E.2/G.965 – Autres formats de trame utilisés dans l'interface V5.2

Tableau E.1/G.965 – Points de code de message utilisés dans l'interface V5.2

Bits							Types de messages
7	6	5	4	3	2	1	
0	0	0	–	–	–	–	Types de messages du protocole RTPC
0	0	0	0	0	0	0	ESTABLISH
0	0	0	0	0	0	1	ESTABLISH ACKNOWLEDGE
0	0	0	0	0	1	0	SIGNAL
0	0	0	0	0	1	1	SIGNAL ACKNOWLEDGE
0	0	0	1	0	0	0	DISCONNECT
0	0	0	1	0	0	1	DISCONNECT COMPLETE
0	0	0	1	1	0	0	STATUS ENQUIRY
0	0	0	1	1	0	1	STATUS
0	0	0	1	1	1	0	PROTOCOL PARAMETER

Tableau E.1/G.965 – Points de code de message utilisés dans l'interface V5.2

Bits							Types de messages
7	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	1	0	–	–	–	Types de messages du protocole de commande
0	0	1	0	0	0	0	PORT CONTROL
0	0	1	0	0	0	1	PORT CONTROL ACKNOWLEDGE
0	0	1	0	0	1	0	COMMON CONTROL
0	0	1	0	0	1	1	COMMON CONTROL ACKNOWLEDGE
0	0	1	1	–	–	–	Types de message du protocole de protection
0	0	1	1	0	0	0	SWITCH-OVER REQUEST
0	0	1	1	0	0	1	SWITCH-OVER COMMAND
0	0	1	1	0	1	0	OS SWITCH-OVER COMMAND
0	0	1	1	0	1	1	SWITCH-OVER ACKNOWLEDGE
0	0	1	1	1	0	0	SWITCH-OVER REJECT
0	0	1	1	1	0	1	PROTOCOL ERROR
0	0	1	1	1	1	0	RESET SN COMMAND
0	0	1	1	1	1	1	RESET SN ACKNOWLEDGE
0	1	0	–	–	–	–	Types de messages du protocole BCC
0	1	0	0	0	0	0	ALLOCATION
0	1	0	0	0	0	1	ALLOCATION COMPLETE
0	1	0	0	0	1	0	ALLOCATION REJECT
0	1	0	0	0	1	1	DE-ALLOCATION
0	1	0	0	1	0	0	DE-ALLOCATION COMPLETE
0	1	0	0	1	0	1	DE-ALLOCATION REJECT
0	1	0	0	1	1	0	AUDIT
0	1	0	0	1	1	1	AUDIT COMPLETE
0	1	0	1	0	0	0	AN FAULT
0	1	0	1	0	0	1	AN FAULT ACKNOWLEDGE
0	1	0	1	0	1	0	PROTOCOL ERROR
0	1	1	0	–	–	–	Types de messages du protocole de commande de liaison
0	1	1	0	0	0	0	LINK CONTROL
0	1	1	0	0	0	1	LINK CONTROL ACK
NOTE – Toutes les autres valeurs sont réservées.							

Tableau E.2/G.965 – Eléments d'information attribués à l'interface V5.2

Bits (Note 1)								**Protocole**	**Elément d'information**	**Référence** (Note 2)
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**			
0	–	–	–	–	–	–	–		Eléments d'information à longueur variable	
0	0	0	0	0	0	0	0	RTPC	Numéro de séquence	14 (13.4.7.1)
0	0	0	0	0	0	0	1	RTPC	Retour d'appel cadencé	14 (13.4.7.2)
0	0	0	0	0	0	1	0	RTPC	Signal pulsé	14 (13.4.7.3)
0	0	0	0	0	0	1	1	RTPC	Signal stable	14 (13.4.7.4)
0	0	0	0	0	1	0	0	RTPC	Signal numérique	14 (13.4.7.5)
0	0	0	1	0	0	0	0	RTPC	Durée de reconnaissance	14 (13.4.7.6)
0	0	0	1	0	0	0	1	RTPC	Activation d'accusé de réception autonome	14 (13.4.7.7)
0	0	0	1	0	0	1	0	RTPC	Désactivation d'accusé de réception autonome	14 (13.4.7.8)
0	0	0	1	0	0	1	1	RTPC	Cause	14 (13.4.7.9)
0	0	0	1	0	1	0	0	RTPC	Ressource indisponible	14 (13.4.7.10)
0	0	1	0	0	0	1	0	RTPC	Capacité de mesure	14 (13.4.7.11)
0	0	1	0	0	0	1	1	RTPC	Rapport de mesure	14 (13.4.7.12)
0	0	1	0	0	1	0	0	RTPC	Affaiblissement	14(13.4.7.13)
0	0	1	0	0	0	0	0	Commande	Elément de fonction de commande	15.4 (14.4.2.5.4)
0	0	1	0	0	0	0	1	Commande	Identification de fonction de commande	15.4 (14.4.2.5.5)
0	0	1	0	0	0	1	0	Commande	Variante	15.4 (14.4.2.5.6)
0	0	1	0	0	0	1	1	Commande	Identification d'interface	15.4 (14.4.2.5.7)
0	0	1	1	0	0	0	0	Commande de liaison	Fonction de commande de liaison	16.3.2.2
0	1	0	0	0	0	0	0	BCC	Identification de point d'accès utilisateur	17.4.2.1
0	1	0	0	0	0	0	1	BCC	Identification d'intervalle de temps de point d'accès RNIS	17.4.2.2
0	1	0	0	0	0	1	0	BCC	Identification d'intervalle de temps V5	17.4.2.3
0	1	0	0	0	0	1	1	BCC	Mappage d'intervalles de temps multiples	17.4.2.4
0	1	0	0	0	1	0	0	BCC	Cause du rejet	17.4.2.5
0	1	0	0	0	1	0	1	BCC	Cause d'erreur de protocole	17.4.2.6
0	1	0	0	0	1	1	0	BCC	Connexion inachevée	17.4.2.7
0	1	0	1	0	0	0	0	Protection	Numéro de séquence	18.5.2
0	1	0	1	0	0	0	1	Protection	Identification de la voie C physique	18.5.3
0	1	0	1	0	0	1	0	Protection	Cause du rejet	18.5.4
0	1	0	1	0	0	1	1	Protection	Cause d'erreur de protocole	18.5.5
1	–	–	–	–	–	–	–		Eléments d'information à octet unique	
1	0	0	0	X	X	X	X	RTPC	Information de ligne	14 (13.4.6.2)
1	0	0	1	X	X	X	X	RTPC	Etat	14 (13.4.6.3)

Tableau E.2/G.965 – Eléments d'information attribués à l'interface V5.2

Bits (Note 1)								**Protocole**	**Elément d'information**	**Référence** (Note 2)
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**			
1	0	1	0	X	X	X	X	RTPC	Séquence de signalisation autonome	14 (13.4.6.4)
1	0	1	1	X	X	X	X	RTPC	Réponse à séquence	14 (13.4.6.5)
1	1	0	0	0	0	0	0	RTPC	Notification de l'impulsion	14 (13.4.6.1)
1	1	1	0	X	X	X	X	Commande	Niveau de performance	15.4 (14.4.2.5.2)
1	1	1	1	X	X	X	X	Commande	Cause du rejet	15.4 (14.4.2.5.1)
NOTE 1 – Toutes les autres valeurs sont réservées. NOTE 2 – Les références entre parenthèses se réfèrent aux paragraphes pertinents de l'UIT-T G.964 [8].										

ANNEXE F

Conception et spécifications de la transformation d'une interface V5.1 en une interface V5.2

Le contenu de la présente annexe est identique à celui de l'Annexe F/G.964 [8].

ANNEXE G

Spécifications du réseau d'accès pour la numérotation par impulsions

Le contenu de la présente annexe est identique à celui de l'Annexe H/G.964 [8].

ANNEXE H

Procédures de détection des erreurs dans la couche 3

Le contenu de la présente annexe est identique à celui de l'Annexe K/G.964 [8].

ANNEXE J

Protocole de protection – Notes explicatives et flux d'information

J.1 Complément d'information sur les principes régissant le protocole de protection

Le réseau d'accès ne peut que demander une commutation mais la commande de commutation (message SWITCH-OVER COM ou OS-SWITCH-OVER COM) proviendra toujours du côté commutateur local. Dès réception de la commande de commutation, la gestion-systèmes du réseau d'accès se bornera à vérifier si les ressources nécessaires à la réussite de la commutation sont ou non disponibles. Le résultat sera communiqué au commutateur local à l'aide d'un message SWITCH-OVER ACK ou SWITCH-OVER REJECT. Le réseau d'accès ne peut pas vérifier la bonne exécution de la commutation. Si pour une raison quelconque, des problèmes liés à la procédure de commutation sont signalés ultérieurement, le réseau d'accès peut en informer le commutateur local en lui envoyant une nouvelle demande.

Avant que le commutateur local n'envoie une commande SWITCH-OVER au réseau d'accès, la gestion-systèmes/le gestionnaire de ressources du commutateur local vérifie si la commutation est en principe possible. Si pour une raison quelconque, des problèmes liés à la procédure de commutation sont signalés ultérieurement, le commutateur local peut lancer une nouvelle commutation en envoyant une nouvelle commande SWITCH-OVER au réseau d'accès.

Si un message SWITCH-OVER ACK envoyé par le côté réseau d'accès se perd, le temporisateur TSO1 ou TSO2 expirera et le commutateur local retransmettra le message SWITCH-OVER COM ou OS-SWITCH-OVER COM. Etant donné que la commutation dans le réseau d'accès a déjà été effectuée, le réseau d'accès répondra par un message SWITCH-OVER REJECT indiquant la cause "l'affectation demandée existe déjà". La gestion-systèmes du commutateur local considèrera ce message comme un accusé de réception de la commutation effectuée dans le réseau d'accès et, en conséquence, devra effectuer la commutation dans le commutateur local.

Les processus de commutation ne doivent pas être simultanés. Ainsi, si le commutateur local envoie une commande de commutation au réseau d'accès, le côté commutateur local doit attendre la réponse avant de pouvoir envoyer une commande SWITCH-OVER, même si des problèmes liés à la commande précédente SWITCH-OVER sont signalés entre-temps par le commutateur local.

Si une anomalie est détectée presque simultanément, le côté commutateur local et le côté réseau d'accès peuvent demander une procédure de commutation en même temps. Dans ce cas, il n'y a pas de conflit d'utilisation dans le commutateur local étant donné que ce dernier est le responsable de la commutation (voir Figure J.7).

J.2 Flux d'information

Les Figures J.1 à J.7 montrent plusieurs exemples de flux d'information du protocole de protection.

La Figure J.1 illustre une commutation déclenchée de façon autonome par le commutateur local à la suite de la détection d'une anomalie ou par intervention de l'exploitant.

La Figure J.2 illustre une commutation de protection déclenchée de façon autonome par le réseau d'accès à la suite de la détection d'une anomalie ou par intervention de l'exploitant.

La Figure J.3 illustre le rejet par le réseau d'accès d'une commutation déclenchée par le commutateur local.

La Figure J.4 illustre le rejet par le commutateur local d'une commutation déclenchée par le réseau d'accès.

La Figure J.5 illustre une commutation déclenchée par le commutateur local, avec retransmissions dues à une perte de message.

La Figure J.6 illustre une commutation déclenchée par le commutateur local, avec retransmissions dues à une perte de message.

La Figure J.7 illustre une commutation déclenchée simultanément par le côté commutateur local et le côté réseau d'accès.

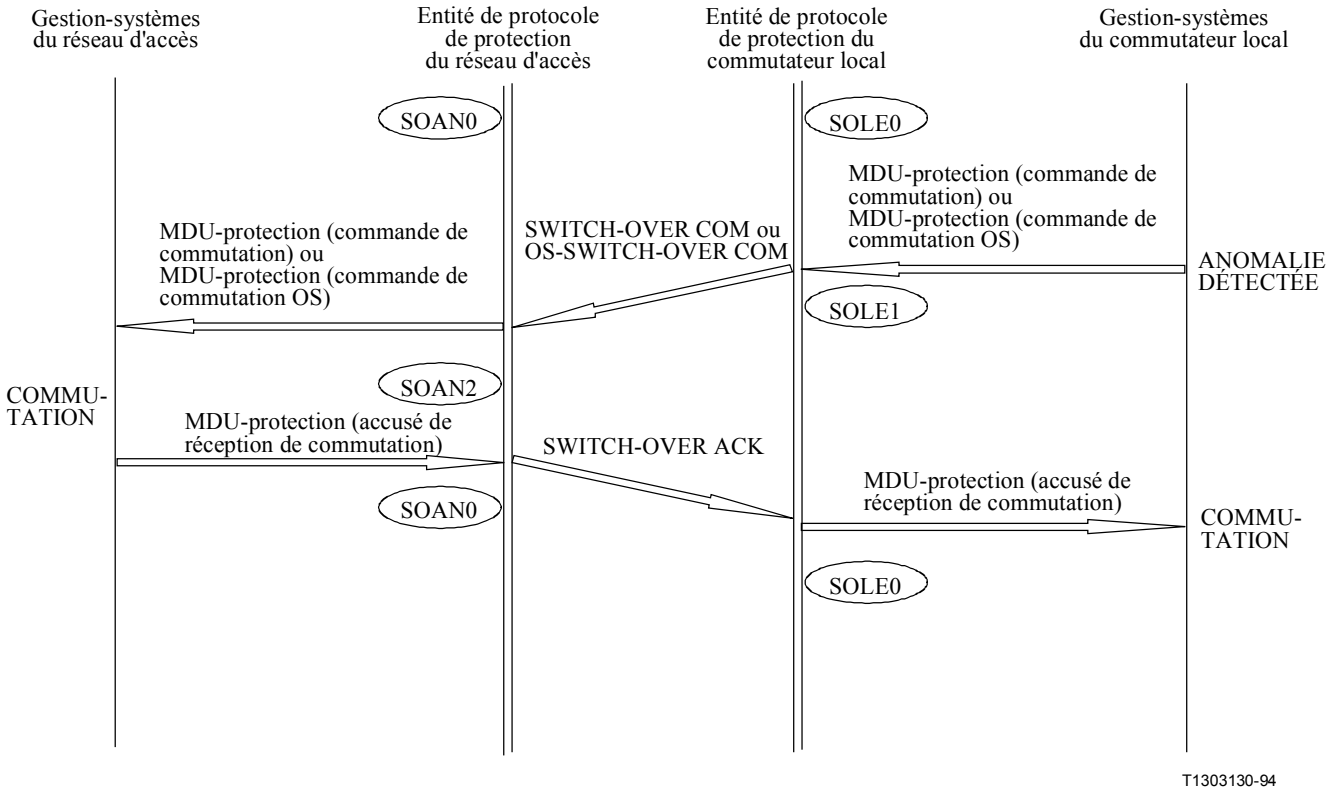


Figure J.1/G.965 – Commutation de protection autonome lancée par le commutateur local entre voies C physiques

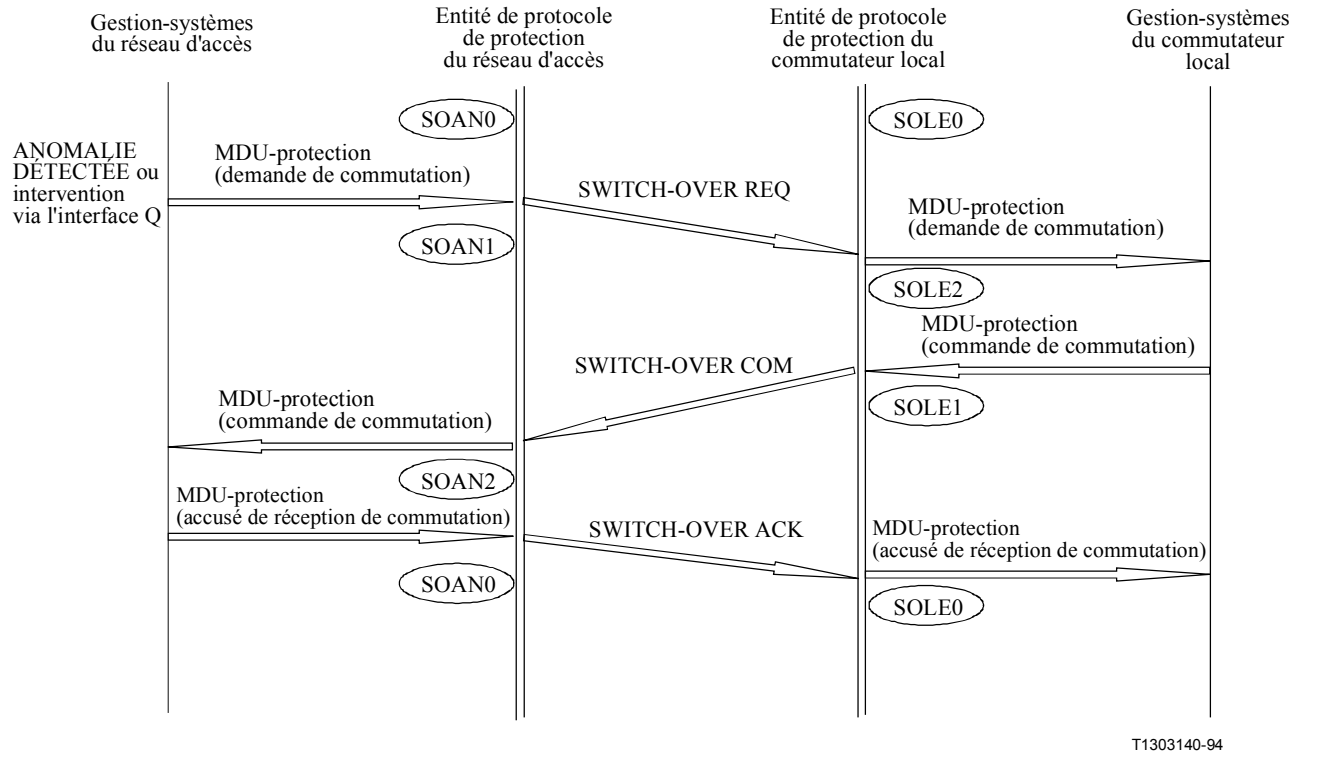


Figure J.2/G.965 – Commutation de protection autonome lancée par le réseau d'accès

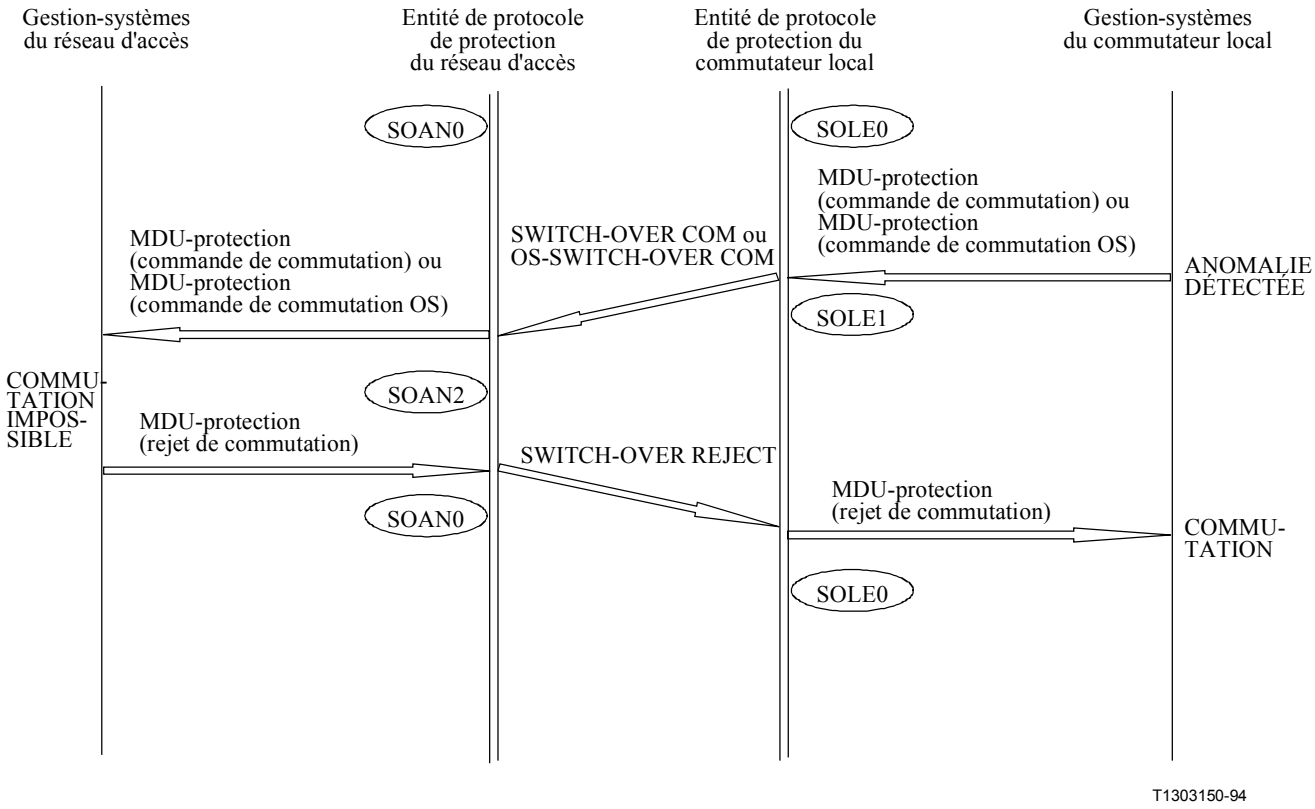


Figure J.3/G.965 – Rejet par le réseau d'accès d'une commutation de protection déclenchée par le commutateur local

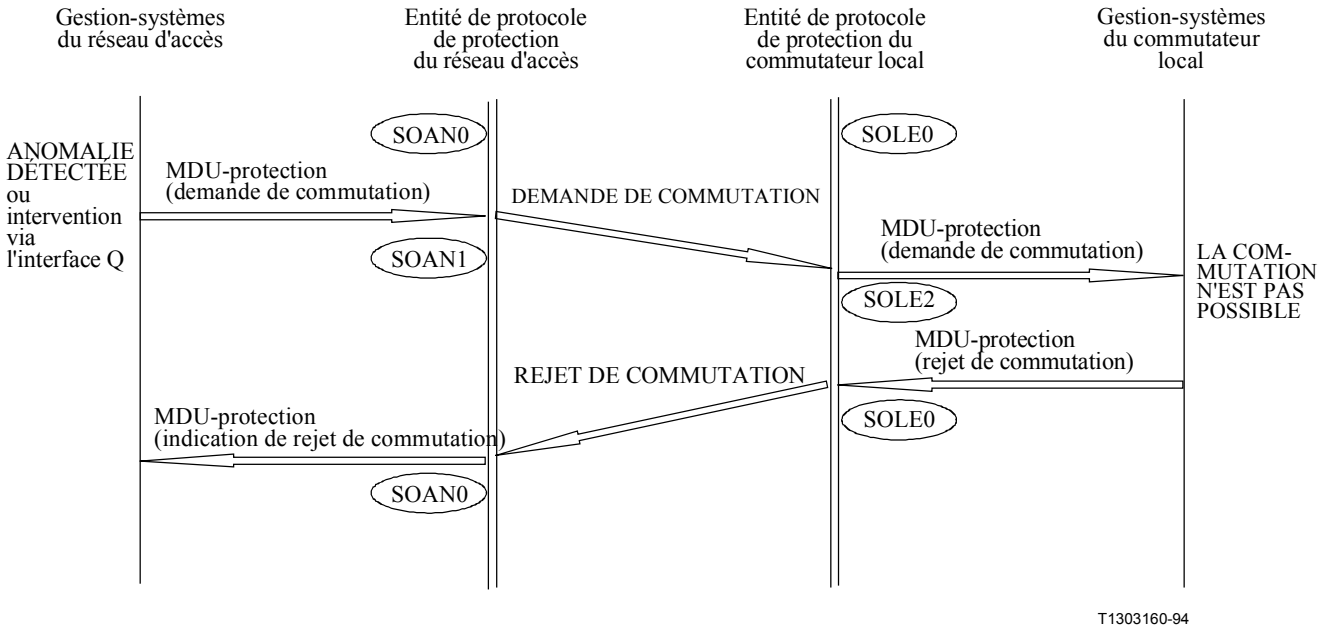
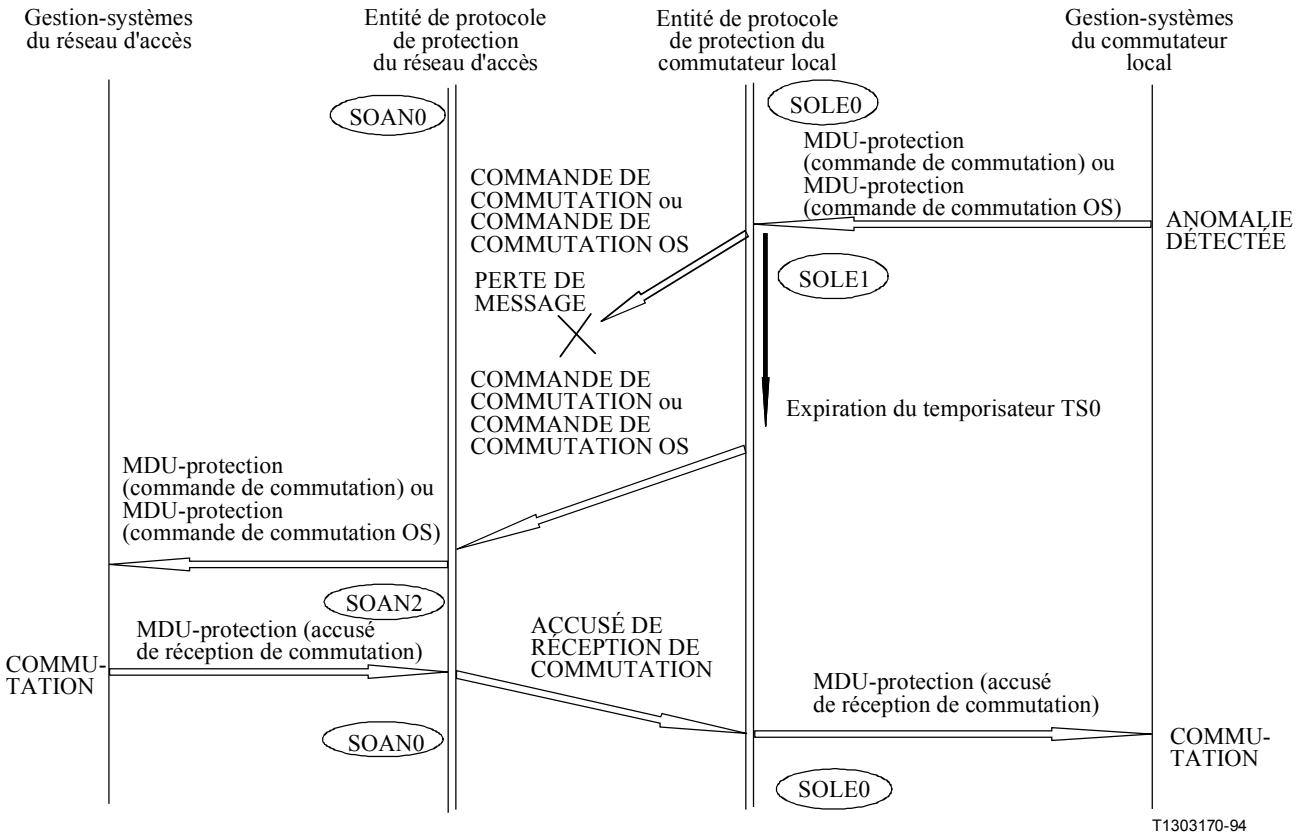
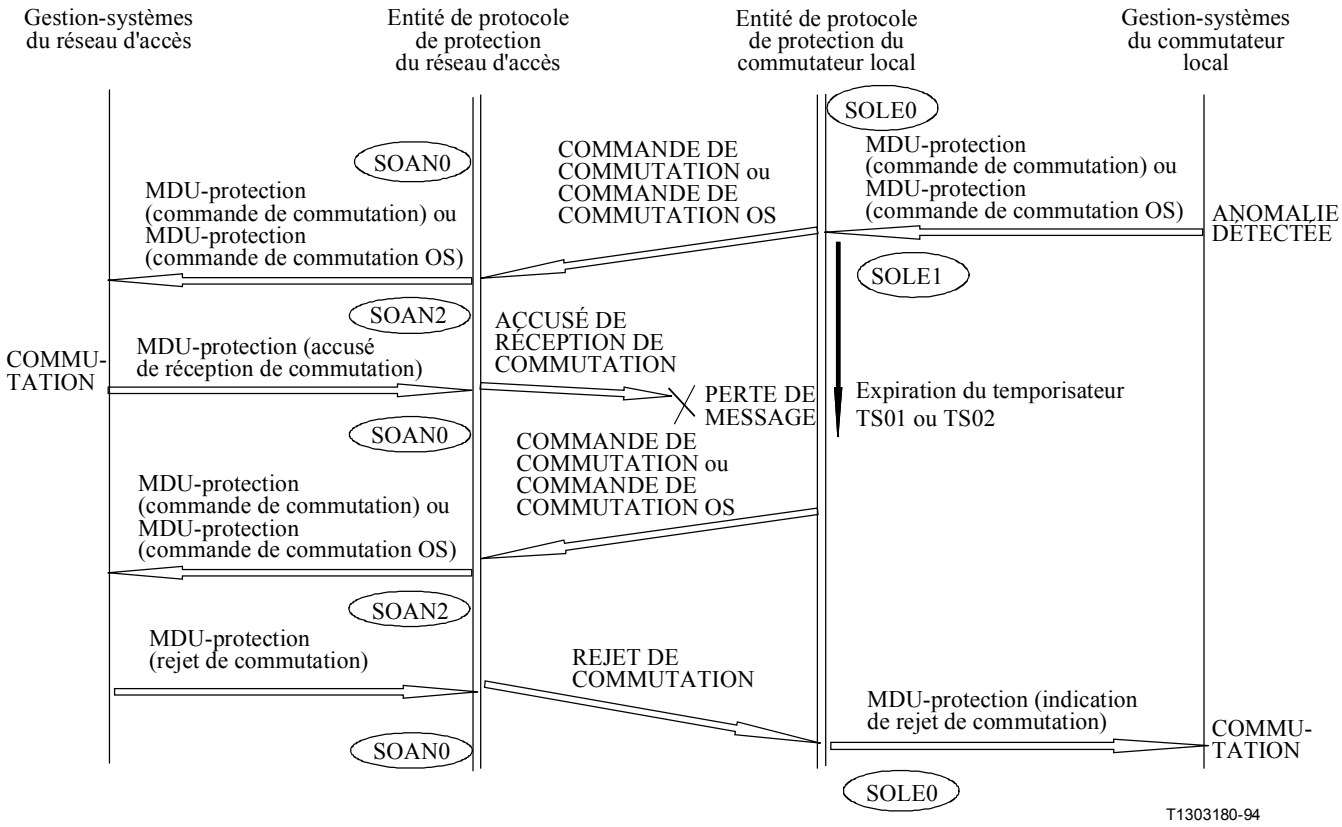


Figure J.4/G.965 – Rejet par le commutateur local d'une commutation de protection déclenchée par le réseau d'accès



NOTE – La figure illustre le cas où il n'y a pas de retransmissions dans la couche 2 (L2) en raison de l'anomalie détectée.

Figure J.5/G.965 – Commutation de protection déclenchée par le commutateur local avec retransmissions (perte de message)



NOTE – La figure illustre le cas où il n'y a pas de retransmissions dans la couche 2 (L2) en raison de l'anomalie détectée.

Figure J.6/G.965 – Commutation de protection déclenchée par le commutateur local (retransmissions dues à une perte de message)

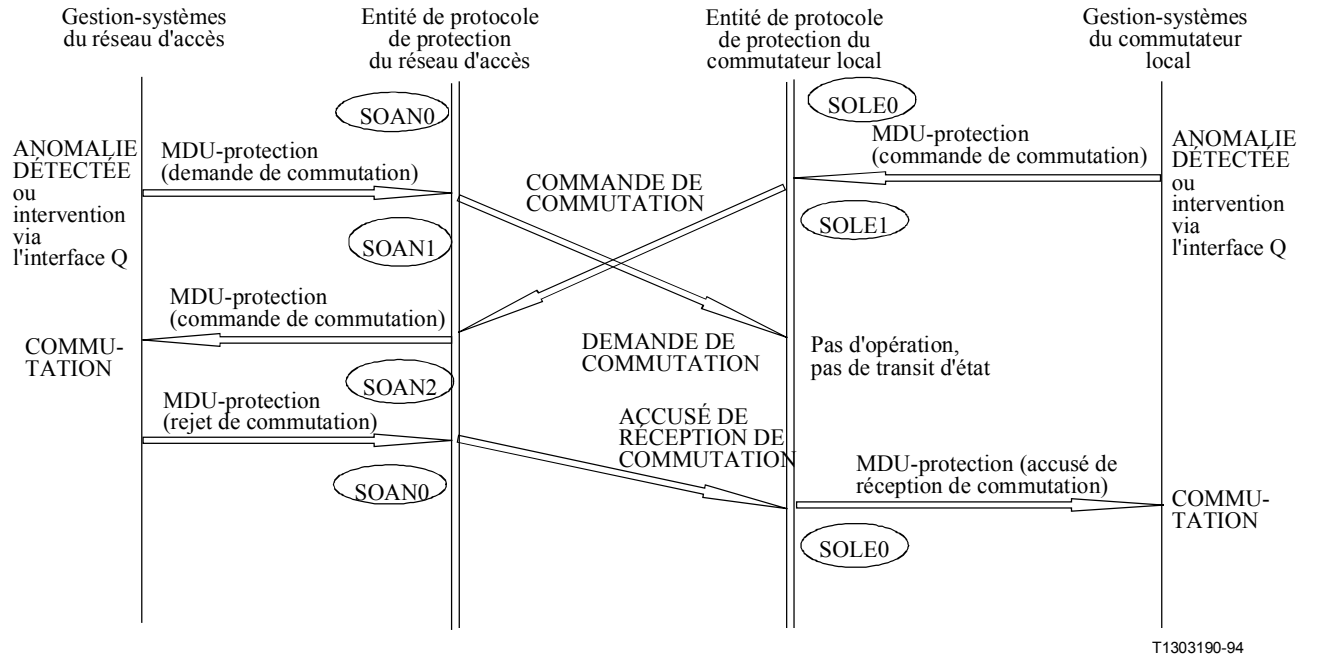


Figure J.7/G.965 – Commutation de protection déclenchée simultanément par le réseau d'accès et le commutateur local

ANNEXE K

Principes d'utilisation du protocole BCC

K.1 Introduction

La présente annexe donne des précisions normatives sur les modalités d'utilisation du protocole BCC par le réseau d'accès et le commutateur local afin de satisfaire les exigences de service au niveau de l'interface V5.2.

Les entités de gestion des ressources gèrent les ressources utilisées lors de la mise en œuvre de connexions de canal support (intervalles de temps, points d'accès utilisateur et voies de point d'accès utilisateur RNIS) à l'aide du protocole BCC. Les fonctions sont partagées entre différentes entités comme suit:

– les entités de gestion des ressources du commutateur local et du réseau d'accès sont responsables de la maintenance des ressources disponibles pour la fourniture des connexions de canal support et de leur état (affectées ou désaffectées);

– la commande du protocole BCC (échange de messages entre le commutateur local et le réseau d'accès) relève de l'entité de protocole BCC;

– les entités de gestion des ressources recevront des demandes de service émanant de différentes entités et du commutateur local (par exemple, protocole national RTPC, protocole national DSS1, système de gestion) mais la relation qui existe entre les entités de gestion des ressources et celles demandant des services BCC ne relève pas de la présente Recommandation.

Le protocole BCC offre les moyens permettant d'assurer divers types de services d'utilisateur:

a) service commuté, dans lequel l'entité de gestion des ressources affecte des connexions commutées pour la prise en charge des appels d'utilisateur; ces connexions seront disponibles pendant toute la durée de l'appel. Les processus d'affectation et de désaffectation, qui sont du ressort de l'entité de gestion de ressources, sont déclenchés par des entités nationales RTPC ou DSS1;

b) service de lignes semi-permanentes louées, dans lequel l'entité de gestion des ressources affecte les connexions commutées nécessaires à la prise en charge de ces connexions d'utilisateur longue durée. Les processus d'affectation et de désaffectation, qui sont du ressort de l'entité de gestion des ressources, sont déclenchés par la gestion-systèmes à la suite d'une demande via l'interface Q_{CL}.

   L'utilisation du protocole BCC pour l'établissement de ce type de connexions garantit que l'entité de gestion des ressources est pleinement informée de l'état de ces connexions de canal support. Lorsque la liaison à 2048 kbit/s sur laquelle est fournie la ligne semi-permanente présente une anomalie, l'entité de gestion des ressources établit un autre trajet.

c) Service de canaux supports préconnectés, dans lequel l'entité de gestion des ressources affecte des connexions commutées pour fournir à l'utilisateur la largeur de bande sous forme de canaux supports à 64 kbit/s ou leurs multiples. Les processus d'affectation et de désaffectation, qui sont du ressort de l'entité de gestion des ressources, sont déclenchés par la gestion-systèmes à la suite d'une demande via l'interface Q_{CL}.

   Ce service fournit à l'utilisateur des connexions permanentes entre le commutateur local et le point d'accès utilisateur via l'interface V5.2. Il convient de l'utiliser lorsqu'il est important que le facteur de concentration fourni par l'interface V5.2 ne risque pas d'entraîner le blocage de services essentiels (par exemple, le service téléphonique pour les pompiers).

L'utilisation du protocole BCC pour l'établissement de ce type de connexion garantit que l'entité de gestion des ressources est pleinement informée de l'état de ces connexions de canal support. Si la liaison à 2048 kbit/s sur laquelle le canal support préconnecté est fourni présente une anomalie, l'entité de gestion des ressources établit un autre trajet et rend compte de l'opération via l'interface Q_{CL}.

K.2 Possibilités d'utilisation des intervalles de temps

Les intervalles de temps 1 à 14 et 17 à 30 de toutes les liaisons à 2048 kbit/s d'une interface V5.2 doivent être disponibles pour être affectés comme canaux supports.

Lorsque les intervalles de temps 15, 16 ou 31 d'une liaison à 2048 kbit/s ne sont pas profilés pour être utilisés comme une voie C physique, ils doivent être utilisables comme canal support.

Les canaux supports à l'interface V5.2 doivent être disponibles pour n'importe quel service (canal support RTPC, canal B-RNIS, canal H-RNIS). Des canaux supports, groupes de canaux supports ou des liaisons à 2048 kbit/s ne peuvent pas être affectés à des types de service ou de canal.

K.3 Règles d'affectation et de désaffection des intervalles de temps

K.3.1 Généralités

Le commutateur local et, s'il y a lieu, le réseau d'accès doivent appliquer les règles suivantes pour l'affectation des intervalles de temps de l'interface V5.2 à des connections supports:

a) le commutateur local est le seul responsable de l'affectation des intervalles de temps;

b) le réseau d'accès peut rejeter une demande de connexion à la suite d'une anomalie ou d'une erreur ou bien encore en raison d'un blocage interne au réseau d'accès;

c) l'entité de protocole RTPC national du commutateur local ou l'entité de protocole RNIS national peuvent demander une nouvelle affectation des intervalles de temps;

d) il n'est pas possible de désaffecter une connexion de canal support pour laquelle toutes les données qui doivent figurer dans le message DE-ALLOCATION ne sont pas fournies.

   Lorsque le commutateur local ne connaît pas toutes les données utiles permettant d'identifier une connexion de canal support avant d'engager le processus de désaffectation, il demande le complément d'information au réseau d'accès à l'aide de la procédure d'audit.

   Si, à la suite de la procédure d'audit, il est établi que cette connexion n'existe pas, le commutateur local efface au niveau interne l'enregistrement de la connexion de canal support BCC;

e) le ou les voies B des points d'accès utilisateur RNIS-accès de base ou au débit primaire, nécessaires à l'établissement d'un appel, sont réservés au niveau interne par l'entité de protocole DSS1 avant que le ou les intervalles de temps de l'interface V5 soient structurés à l'aide du protocole BCC. Ensuite, à l'aide des procédures DSS1, le ou les voies B seront affectés, ce dont sera averti l'abonné RNIS dans le message DSS1 approprié. Un nouveau réarrangement des voies B, sous le contrôle de l'abonné, peut être nécessaire.

   La capacité de service DSS1 est ainsi maintenue et la demande de connexion BCC peut transmettre l'identité complète des deux extrémités de la connexion du réseau d'accès;

f) lorsqu'il affecte les intervalles de temps, le commutateur local applique une séquence de connexions, c'est-à-dire qu'il affecte des connexions aux liaisons à 2048 kbit/s d'une interface V5.2 dans un ordre préférentiel. Les liaisons à 2048 kbit/s ayant plus d'une voie C physique sont prioritaires. Ces règles s'appliquent à toutes les connexions, afin de minimiser le risque d'encombrement dans le cas de connexions à intervalles de temps multiples.

La séquence de connexions multiplie les incidences que des anomalies non détectées peuvent avoir sur le service, en particulier lorsque le volume de trafic est faible. On peut remédier à cette situation en n'ayant pas une préférence fixe unique, ce qui se traduit en général par un compromis entre le nombre d'anomalies et le nombre d'encombrements sur des connexions à intervalles de temps multiples. Il convient d'en tenir compte lorsqu'on met en œuvre le commutateur local pour prendre en charge des interfaces V5.2;

g) la gestion-systèmes du commutateur local réaffecte les connexions semi-permanentes et les canaux supports préconnectés du réseau d'accès à d'autres liaisons à 2048 kbit/s (s'il en existe), si la liaison à 2048 kbit/s qui les achemine présente une anomalie ou si le protocole BCC signale une anomalie interne au réseau d'accès.

Les connexions supports commutées ne sont pas réaffectées à d'autres intervalles de temps de l'interface V5.2 en cas d'anomalie;

h) dans le cas d'appels à l'arrivée dans le RNIS (appels que le commutateur local présente au réseau d'accès), le commutateur local doit indiquer dans le message DSS1 SETUP qu'il enverra à l'accès RNIS, l'identification du canal B ou du canal H à utiliser pour l'appel.

Par conséquent, avant d'envoyer le message SETUP, le commutateur local doit s'assurer de la disponibilité des intervalles de temps nécessaires dans l'interface qui seront utilisés comme canaux supports; il doit également s'assurer que ces intervalles de temps sont affectés correctement au point d'accès RNIS. Une synchronisation de protocole est donc nécessaire car le processus d'affectation doit être terminé avant l'envoi du message DSS1 SETUP.

Si elle reçoit un message ALLOCATION REJECT, l'entité de protocole BCC du commutateur local en avertit l'entité de gestion des ressources à l'aide de la primitive MDU-BCC (indication de rejet d'affectation) et envoie également la notification adaptée à l'entité de protocole RNIS. Lorsqu'elle reçoit cette indication, l'entité de protocole RNIS peut demander une autre affectation de canal support avant d'envoyer le message RELEASE COMPLETE à l'abonné RNIS. Le nombre de nouvelles tentatives dépendra des décisions d'implémentation et des contraintes de synchronisation DSS1 qui relèvent de l'entité de protocole RNIS;

i) en cas d'appels au départ dans le RNIS (appels que le réseau d'accès présente au commutateur local), le commutateur local doit indiquer dans le message DSS1 qu'il envoie comme réponse au message SETUP reçu (ALERTING, CALL PROCEEDING, CONNECT) l'identification du canal B ou du canal H qui sera utilisé pour l'appel.

Par conséquent, avant d'envoyer la réponse qui convient au message SETUP reçu, le commutateur local doit s'assurer de la disponibilité des intervalles de temps de l'interface nécessaires qui seront utilisés comme canaux supports; il doit également s'assurer que ces intervalles de temps sont affectés correctement au point d'accès RNIS. Une synchronisation de protocole est donc nécessaire car le processus d'affectation doit être achevé avant d'envoyer le message DSS1 en réponse au message SETUP reçu;

j) en cas d'appels à l'arrivée dans un RTPC (appels que le commutateur local présente au réseau d'accès), le commutateur local doit, en règle générale, avant d'envoyer le signal "signal de sonnerie initial", s'assurer de la disponibilité d'une voie support pour l'appel. Il y a toutefois des cas où un trajet de signalisation RTPC est établi et où aucune affectation de voie support n'est nécessaire;

k) en cas d'appels au départ dans le RTPC (appels que le réseau d'accès présente au commutateur local), le commutateur local doit, en règle générale, avant d'envoyer la "tonalité de numérotation" s'assurer de la disponibilité d'un canal support pour l'appel. Il y a toutefois des cas où un trajet de signalisation RTPC est établi et où aucune affectation de canal support n'est nécessaire;

l) lorsqu'il libère des appels RNIS ou RTPC (lancés par l'utilisateur ou le réseau), le commutateur local lance en direction du réseau d'accès l'opération propre à libérer les ressources V5.2 affectées à cet appel particulier.

Lorsqu'il lance un processus de désaffectation concernant le point d'accès RNIS, le commutateur local peut déconnecter le canal support (intervalle de temps V5) de la connexion d'appel et passer à la libération de l'appel RNIS avant d'achever le processus de désaffectation (c'est-à-dire que la synchronisation entre le protocole DSS1 et le processus de désaffectation BCC n'est pas nécessaire);

m) le Tableau K.1 précise quand utiliser les différents types de causes de rejet des procédures de protocole BCC;

n) Indépendamment de l'affectation/la désaffectation possible des canaux supports, la fourniture de services complémentaires DSS1 ne nécessite pas la mise en œuvre d'autres fonctions du protocole BCC.

Tableau K.1/G.965 – Utilisation des types de causes de rejet

Cause	Description
Non spécifié	Une anomalie autre que celles figurant dans le présent tableau a été détectée.
Anomalie dans le réseau d'accès	Le processus d'affectation ou de désaffectation ne peut être achevé car une anomalie interne au réseau a été détectée.
Réseau d'accès bloqué (interne)	Le processus d'affectation ne peut être achevé car un blocage interne du réseau d'accès a été détecté.
Il existe déjà une connexion au point d'accès utilisateur RTPC à un intervalle de temps V5 différent	Le processus d'affectation ne peut être achevé car il existe déjà une connexion sur le point d'accès RTPC choisi à un intervalle de temps différent.
Il existe déjà une connexion aux intervalles de temps à un point d'accès différent ou intervalle de temps de point d'accès utilisateur RNIS différent	Le processus d'affectation ne peut être achevé car il existe déjà une connexion sur le ou les intervalles de temps V5.2 choisis à un point d'accès utilisateur différent ou à un intervalle de temps de point d'accès utilisateur différent.
Il existe déjà une connexion aux intervalles du point d'accès utilisateur RNIS à différents intervalles de temps	Le processus d'affectation ne peut être achevé car il existe déjà une connexion sur un ou des intervalles de temps de point d'accès d'utilisateur choisis à un/des intervalles de temps différents.
Point d'accès utilisateur non disponible (bloqué)	Le processus d'affectation ne peut être achevé car le point d'accès utilisateur choisi n'est pas disponible pour le service.
Le processus de désaffectation ne peut être achevé car le contenu de données est incompatible	Le processus de désaffectation ne peut être achevé car les données fournies concernant l'intervalle de temps, le point d'accès utilisateur et l'intervalle de temps de point d'accès utilisateur ne correspondent à aucune connexion de point d'accès utilisateur.
Le processus de désaffectation ne peut être achevé en raison d'une incompatibilité des données relatives aux intervalles de temps V5	Le processus de désaffectation ne peut être achevé car les données fournies concernant les intervalles de temps V5 ne correspondent à aucune donnée relative au réseau d'accès.

Tableau K.1/G.965 – Utilisation des types de causes de rejet

Cause	Description
Le processus de désaffectation ne peut être achevé en raison d'une incompatibilité des données relatives au point d'accès	Le processus de désaffectation ne peut être achevé car les données fournies concernant le point d'accès utilisateur ne correspondent à aucun point d'accès utilisateur du réseau d'accès.
Le processus de désaffectation ne peut être achevé en raison d'une incompatibilité des données relatives aux intervalles de temps de point d'accès utilisateur	Le processus de désaffectation ne peut être achevé car les données fournies concernant les intervalles de temps de point d'accès utilisateur ne correspondent pas à un/des point(s) d'accès utilisateur du réseau d'accès.
Point d'accès utilisateur non profilé	Le processus d'affectation ne peut être achevé car le point d'accès utilisateur identifié n'est pas profilé.
Identifications d'intervalles de temps V5 non valables	L'identification d'intervalle(s) de temps V5 ne correspond pas à une de celles disponibles pour être utilisées comme canaux supports.
Identification de liaison à 2048 kbit/s non valable	L'identification de la liaison à 2048 kbit/s à l'interface V5.2 ne correspond à aucune liaison disponible.
Identification(s) d'intervalle(s) de temps de point d'accès d'utilisateur non valable(s)	L'identification du/des intervalle(s) de temps de point d'accès utilisateur ne correspond à aucun des points d'accès utilisateur RNIS choisis.
Intervalles de temps V5 utilisés comme voies C physiques	Le processus ne peut être achevé car l'intervalle de temps V5 identifié est utilisé comme voie C physique.
NOTE – Aucune autre valeur applicable.	

K.3.2 Connexions à plusieurs intervalles de temps

Le commutateur local et, s'il y a lieu, le réseau d'accès, doivent appliquer les règles suivantes pour affecter des intervalles de temps d'interface V5.2 à des connexions supports à intervalles de temps multiples (par exemple, n × 64 kbit/s):

a) au début d'un appel (ou d'une affectation de canal support semi-permanente ou préconnecté) tous les intervalles de temps d'une connexion à intervalles de temps multiples sont affectés simultanément par un seul et même processus d'affectation BCC;

b) pendant un appel (ou une affectation de voie semi-permanente ou préconnectée) il est possible de libérer un à un les intervalles de temps constituant une connexion à intervalles de temps multiples ou de libérer simultanément une proportion quelconque des intervalles de temps. Cette fonction permet de réduire la largeur de bande affectée pour la partie restante d'un appel (ou d'une affectation de voie semi-permanente ou préconnectée).

c) à la fin d'un appel (ou d'une affectation de voie semi-permanente ou préconnectée) tous les intervalles de temps constituant une connexion à intervalles de temps multiples sont libérés simultanément;

d) les intervalles de temps multiples nécessaires pour une connexion à intervalles de temps multiples sont sélectionnés parmi des intervalles de temps libres (dans une liaison à 2048 kbit/s simple) et ne doivent pas être situés dans un bloc d'intervalles de temps contigus;

e) l'attribut structurel d'intégrité de séquence d'intervalles de temps (TSSI) s'applique à l'élément de connexion entre l'interface utilisateur-réseau et l'interface V5. Ainsi:

   – à l'interface utilisateur-réseau et à l'interface V5, les intervalles de temps sont implicitement ou explicitement délimités pour chaque voie d'un ensemble de voies;

- les éléments d'information provenant des intervalles de temps côté réception sont dans l'ordre où ils ont été envoyés côté émission;
- tous les intervalles de temps utilisés côté utilisateur sont dans la même interface RNIS-accès de base ou RNIS-accès à débit primaire;
- tous les intervalles de temps utilisés à l'interface V5 sont dans la même liaison à 2048 kbit/s;

f) l'attribut structurel d'intégrité à 8 kHz s'applique à l'élément de connexion entre l'interface utilisateur-réseau et l'interface V5. Ainsi:
   - à l'interface utilisateur-réseau et à l'interface V5, les intervalles de 125 µs sont implicitement ou explicitement délimités (par exemple, à l'aide de frontières de trame);
   - tous les bits transmis dans un intervalle délimité de 125 µs sont remis dans un intervalle de 125 µs délimité correspondant;

g) si la présence d'un canal support préconnecté n'est pas nécessaire pour assurer des services commutés à débit binaire multiple (H0 ou H12), contrairement à ce qui se passe pour des services à 64 kbit/s, on établit une connexion à n × 64 kbit/s pour assurer l'intégrité TSSI et l'intégrité à 8 kHz de ces services.

K.3.3 Capacité d'outrepassement

Pour mieux assurer certaines prestations de service utilisateur, le commutateur local, lorsqu'il affecte des connexions de canal support, peut utiliser la capacité d'outrepassement. Cette fonction permet de connecter le canal support connecté à un canal B d'un point d'accès utilisateur RNIS à un autre canal B du même point d'accès utilisateur RNIS.

La fonction d'outrepassement ne peut être utilisée que pour des processus d'affectation à un canal support à 64 kbit/s simple.

K.4 Règles régissant la procédure d'analyse

Le protocole BCC comprend les moyens nécessaires pour que le commutateur local puisse obtenir du réseau d'accès des informations concernant certaines connexions pour lesquelles il ne dispose pas de toutes les informations. Cette procédure doit respecter certaines règles:

a) le commutateur local ne lance d'analyse que lorsque aucun autre processus (affectation ou désaffectation) n'est en cours d'achèvement;

b) lorsqu'un processus d'analyse a été lancé, le commutateur local n'engage pas de processus d'affectation ou de désaffectation;

c) plusieurs processus d'analyse peuvent être lancés simultanément en utilisant différents numéros de référence BCC;

d) les processus d'analyse sont lancés par l'entité de gestion des ressources du commutateur local ou à la demande de la gestion-systèmes;

e) le Tableau K.2 précise quand utiliser les valeurs affectées aux différents causes donnés dans le protocole BCC.

Tableau K.2/G.965 – Utilisation des valeurs affectées aux différentes causes

Cause	Description
Non achevé, normal	Le processus d'analyse ne peut être achevé parce que la connexion n'existe pas.
Point d'accès utilisateur non profilé	Le processus d'analyse ne peut être achevé car le point d'accès utilisateur identifié n'est pas profilé.
Identification d'intervalle de temps V5 non valable	L'identification du canal support ne correspond pas à la voie disponible pour le canal support faisant l'objet de l'analyse.
Liaison à 2048 kbit/s non valable	L'identification de la liaison à 2048 kbit/s à l'interface V5.2 ne correspond pas à celle acheminant le canal support faisant l'objet de l'analyse.
Intervalle de temps utilisé comme voie C physique	Le processus ne peut être achevé car l'intervalle de temps identifié est utilisé comme voie C physique.

K.5 Règles de notification d'anomalie interne au réseau d'accès

Le protocole BCC comprend les moyens nécessaires pour que le réseau d'accès puisse avertir le commutateur local d'anomalies internes touchant les connexions internes assurant les canaux supports. Pour utiliser cette procédure il faut respecter les règles suivantes:

a) le réseau d'accès avertit toutes les connexions internes prenant en charge la connexion de canal support, en cas d'anomalie interne.

   Les anomalies internes ne touchant pas de canaux supports affectés ne seront pas signalées via le protocole BCC;

b) la notification d'anomalie interne au réseau d'accès se fait sur une connexion simple à 64 kbit/s; le processus est répété pour chaque notification;

c) lorsqu'il signale une anomalie interne le réseau d'accès fournit autant d'informations que possible pour que le commutateur local puisse identifier la connexion support. Toutefois s'il n'est pas en mesure de fournir toutes les informations nécessaires, le commutateur local obtiendra les informations complètes à partir de ses propres données internes sur la base des informations partielles reçues.

K.6 Règles à appliquer en cas d'anomalie interne au réseau d'accès

Lorsque le réseau d'accès signale une anomalie interne au commutateur local par un message AN FAULT contenant l'élément d'identification Identification de point d'accès d'utilisateur, et dans le cas d'un RNIS, l'élément d'information Identification de voie de point d'accès RNIS ainsi que l'élément d'information Identification d'intervalle de temps V5, toutes les ressources du réseau d'accès se rapportant à la connexion affectée sont libérées en interne. L'entité de gestion des ressources du commutateur local lance la procédure interne de désaffectation de la connexion de canal support notifiée. Elle signale par ailleurs l'événement à l'entité de protocole RTPC/RNIS afin que les mesures de service adéquates soient prises.

Lorsqu'une anomalie interne du réseau d'accès est notifiée par le réseau d'accès au commutateur local par un message AN FAULT contenant soit l'élément d'information Identification de point d'accès d'utilisateur et en cas d'un RNIS, l'élément d'information Identification de voie de point d'accès RNIS ou l'élément d'information Identification d'intervalle de temps V5, mais pas tous les éléments d'information mentionnés, l'entité de gestion des ressources dans le commutateur local doit initialiser la désaffectation pour la connexion de canal support notifiée envoyée, envoyer un message DE-ALLOCATION au réseau d'accès et notifier l'événement aux entités de protocole RTPC/RNIS pour que soient prises les actions de service appropriées.

Si l'entité de gestion des ressources du commutateur local s'aperçoit que la connexion de canal support touchée fait partie d'une configuration à intervalles de temps multiples, elle ne prend aucune mesure concernant le reste des connexions de canal support. Le déclenchement de la mesure à prendre (par exemple, désaffectation du reste des connexions de canal support) relève de la responsabilité de l'entité de protocole RNIS en fonction des besoins du service.

K.7 Erreurs de protocole BCC

Les entités de protocole BCC doivent pouvoir détecter trois catégories différentes d'erreurs de protocole:

a) erreurs portant sur un processus BCC en cours (dues par exemple à l'absence de réponse à un message ALLOCATION renvoyé). Ces erreurs sont signalées à l'entité de gestion des ressources;

b) erreurs portant sur un processus BCC non existant (dues par exemple à la réception d'un message ALLOCATION COMPLETE lorsque le commutateur local se trouve dans l'état Bcc0). Ces erreurs sont signalées à l'entité de gestion-systèmes;

c) erreurs portant sur les procédures de traitement des erreurs de protocole (voir 17.5.8). Elles sont signalées à la gestion-systèmes.

K.8 Diagrammes de flux – Exemples de coordination entre le protocole BCC et l'entité DSS1

K.8.1 Appel RNIS lancé par l'abonné

K.8.1.1 Procédure normale

La Figure K.1 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas d'un appel lancé par l'abonné (procédure normale).

En cas d'établissement d'un appel RNIS et d'affectation d'un canal support, il est nécessaire d'avoir une synchronisation de protocole; le processus d'affectation doit être achevé avant d'envoyer le message DSS1 en réponse au message SETUP reçu.

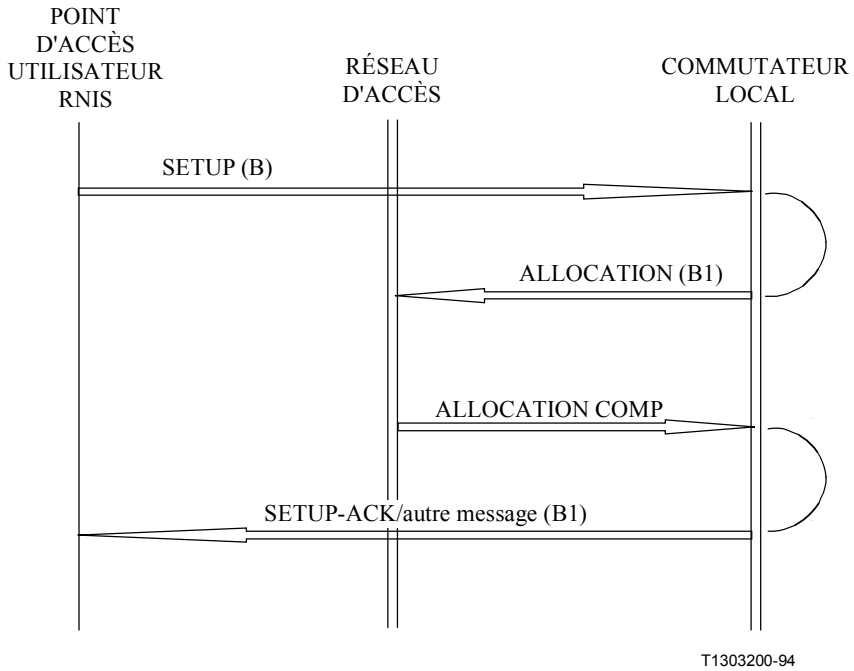


Figure K.1/G.965 – Appel RNIS lancé par l'abonné – Procédure normale

K.8.1.2 Procédure exceptionnelle

La Figure K.2 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas d'un appel lancé par l'abonné (procédure exceptionnelle).

K.8.1.3 Etablissement d'appels RNIS simultanés (en provenance du même point d'accès RNIS)

La Figure K.3 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas d'établissement d'appels RNIS simultanés depuis un point d'accès utilisateur.

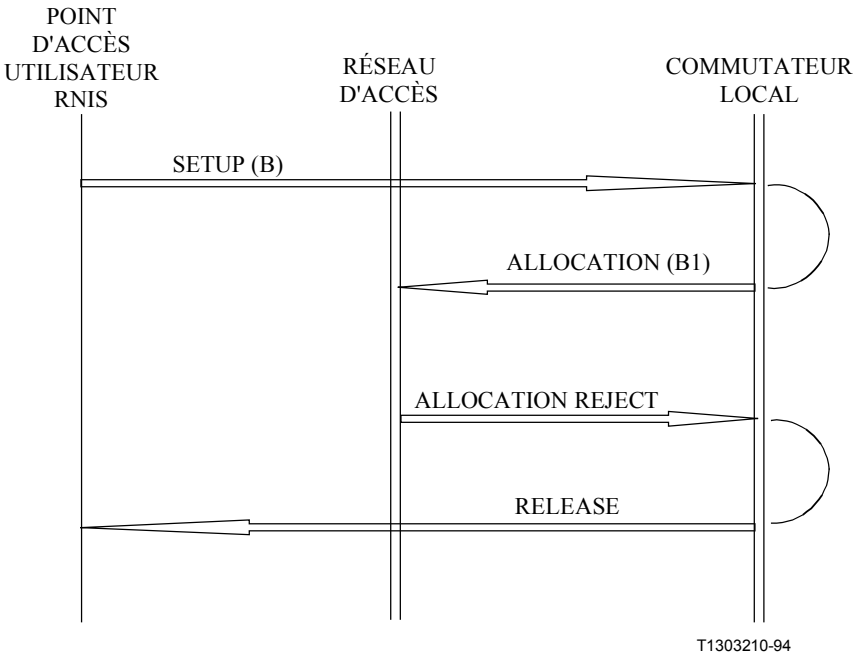


Figure K.2/G.965 – Appel RNIS lancé par l'abonné – Procédure exceptionnelle

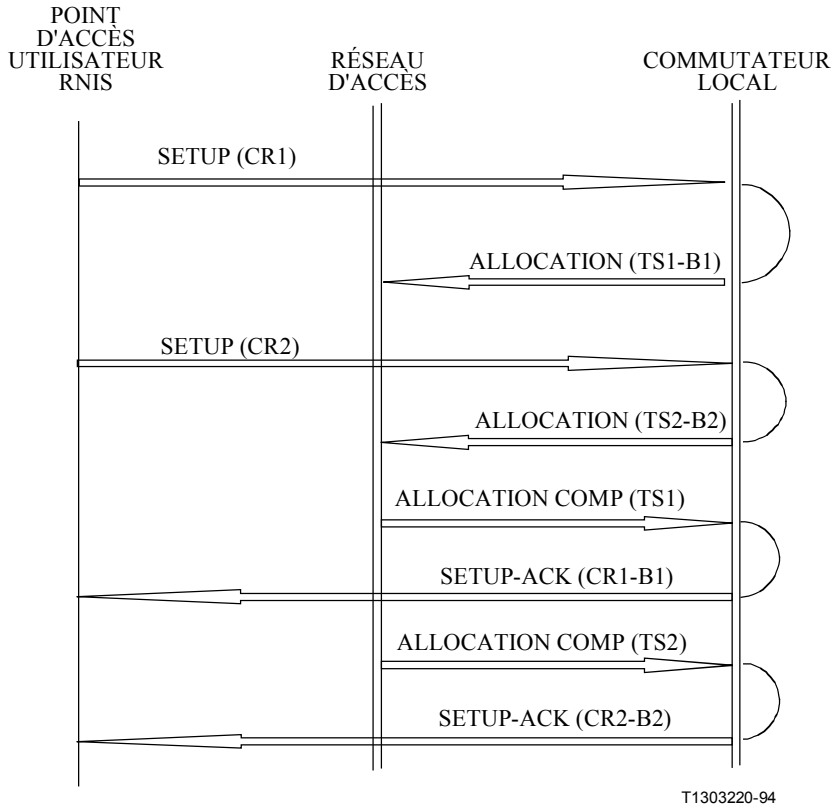


Figure K.3/G.965 – Etablissement d'appels simultanés RNIS depuis un point d'accès utilisateur RNIS

K.8.2 Appel RNIS lancé par le réseau

K.8.2.1 Négociation avec la voie B non autorisée (par exemple, configuration en bus passif)

La Figure K.4 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas d'un appel RNIS lancé par le réseau (négociation avec la voie B non autorisée).

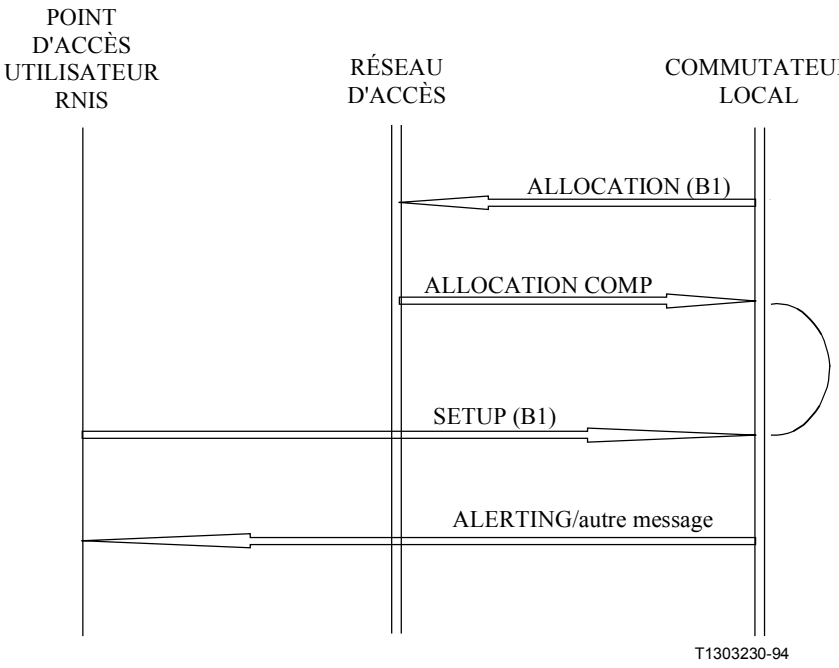


Figure K.4/G.965 – Appel RNIS lancé par le réseau – Négociation avec le canal B non autorisée

K.8.2.2 Négociation avec la voie B autorisée (par exemple, configuration point à point)

La Figure K.5 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas d'un appel RNIS lancé par le réseau (négociation avec la voie B autorisée).

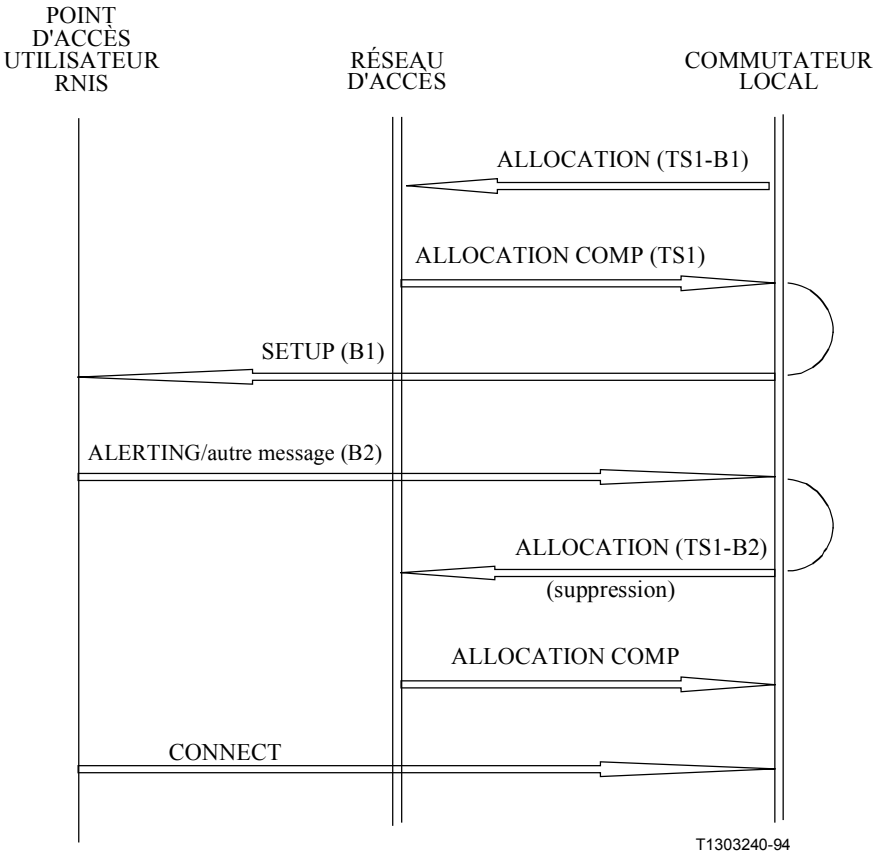


Figure K.5/G.965 – Appel RNIS lancé par le réseau – Négociation avec le canal B autorisée

K.8.2.3 Appel RNIS en attente de fourniture de service complémentaire

La Figure K.6 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas où aucun canal B n'est disponible à l'interface utilisateur-réseau.

Au point indiqué par un X) dans la Figure K.6, une réaffectation interne s'opère dans le commutateur local, les ressources (intervalle de temps et canal B) utilisées par un point d'accès pour un appel étant réaffectées à un nouvel appel qui doit aboutir au même point d'extrémité. La prise en charge de ce service complémentaire RNIS est une fonction interne du commutateur local concerné (entité de gestion des ressources du protocole BCC) sans qu'intervienne l'entité de protocole BCC.

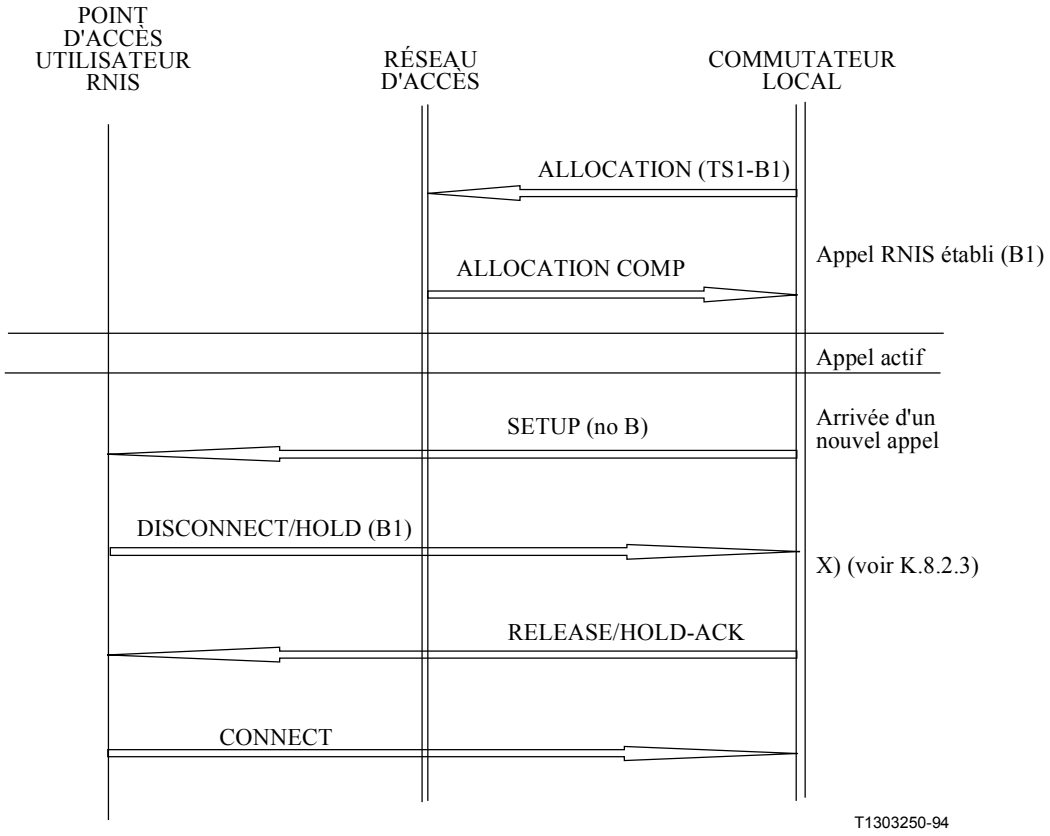


Figure K.6/965 – Appel RNIS lancé par le réseau, appel en attente de fourniture d'un service complémentaire

K.8.3 Libération d'un appel RNIS lancé par l'abonné

La Figure K.7 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité DSS1 dans le cas où la libération d'un appel est lancée par l'abonné.

En cas de libération d'un appel RNIS et de désaffectation du canal support, la synchronisation de protocole n'est pas nécessaire; l'envoi du message de réponse DSS1 au message DISCONNECT est donc dissocié de l'envoi du message DE-ALLOCATION.

K.8.4 Libération d'appel RNIS lancée par le réseau

La Figure K.8 illustre le diagramme de flux montrant l'interaction entre le protocole BCC et l'entité de signalisation DSS1 dans le cas où la libération d'un appel est lancée par le réseau.

En cas de libération d'un appel RNIS et de désaffectation du canal support, la synchronisation de protocole n'est pas nécessaire; l'envoi du message DE-ALLOCATION est donc dissocié de la réception du message DSS1 RELEASE.

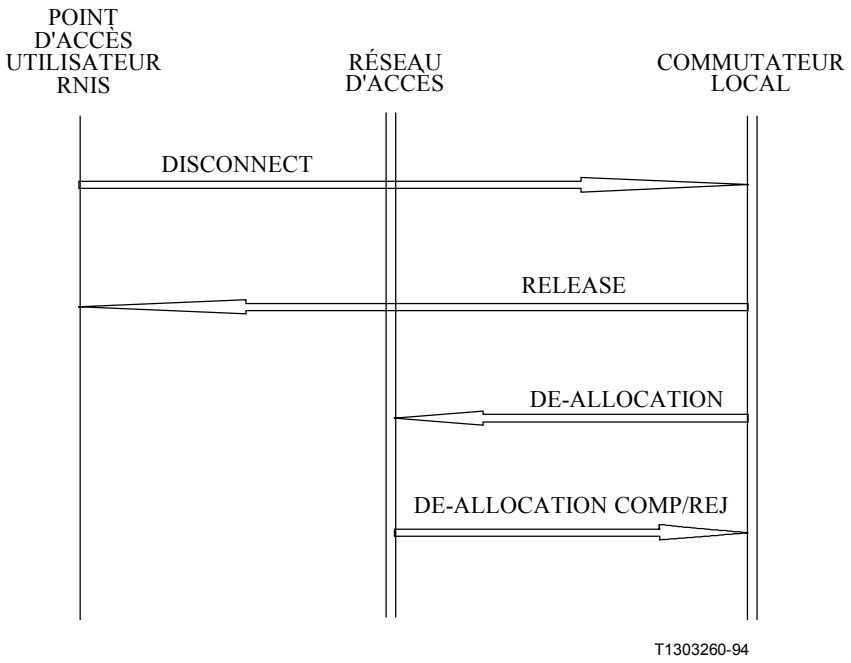


Figure K.7/G.965 – Libération d'un appel RNIS lancée par l'abonné

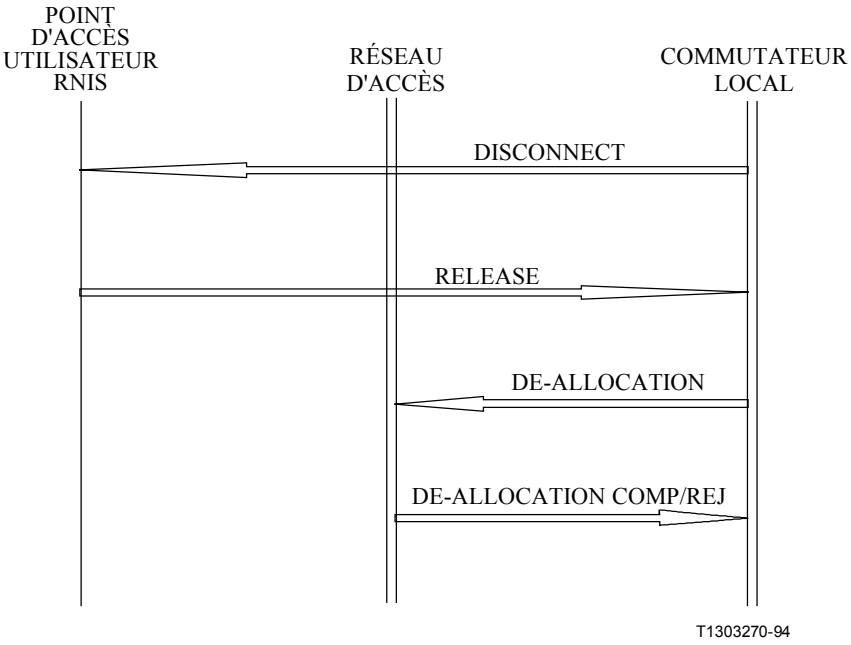


Figure K.8/G.965 – Libération d'un appel RNIS lancée par le réseau

K.8.5 Prise en charge du service complémentaire de portabilité de terminal

La Figure K.9 illustre le diagramme de flux montrant comment les messages DSS1 SUSPEND et RESUME doivent être pris en charge.

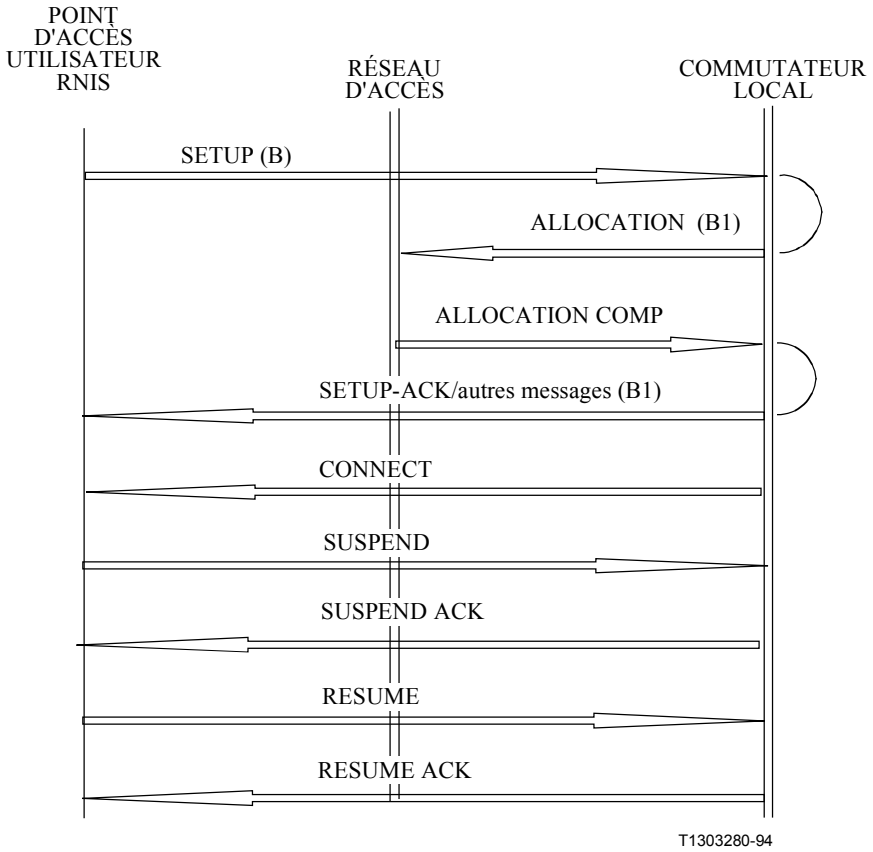


Figure K.9/G.965 – Service complémentaire de portabilité de terminal

K.9 Diagrammes de flux – Exemples de coordination de protocoles BCC et RTPC

Le présent paragraphe montre la coordination attendue entre le protocole BCC et les entités RTPC nationales. Il ne donne pas une liste complète des possibilités et n'a qu'un caractère purement informatif.

K.9.1 Appel RTPC lancé par l'abonné

K.9.1.1 Procédure normale

La Figure K.10 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'un appel lancé par l'abonné (procédure normale).

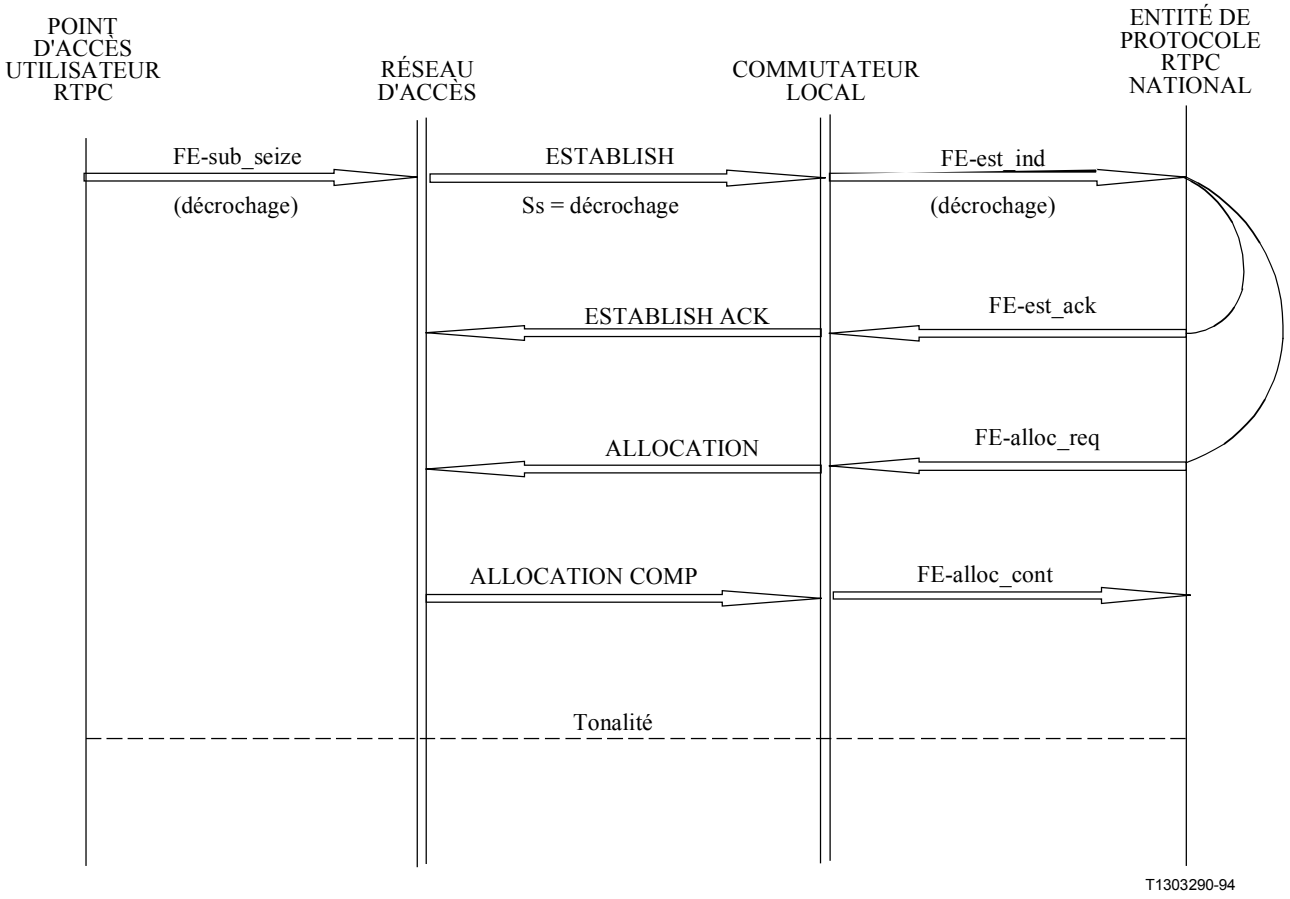


Figure K.10/G.965 – Appel RTPC lancé par l'abonné – Procédure normale

K.9.1.2 Procédure exceptionnelle

La Figure K.11 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'un appel lancé par l'abonné (procédure exceptionnelle). Après réception d'un message ALLOCATE REJECT en provenance du réseau d'accès, plusieurs tentatives d'affectation d'un canal support peuvent être faites (contrôlées par un temporisateur dans le protocole national).

K.9.2 Appel RTPC lancé par le réseau

La Figure K.12 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'un appel lancé par le réseau.

K.9.3 Collision d'appel

K.9.3.1 Collision d'appels – Priorité à l'appel de départ

La Figure K.13 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'une collision d'appels (priorité à l'appel de départ).

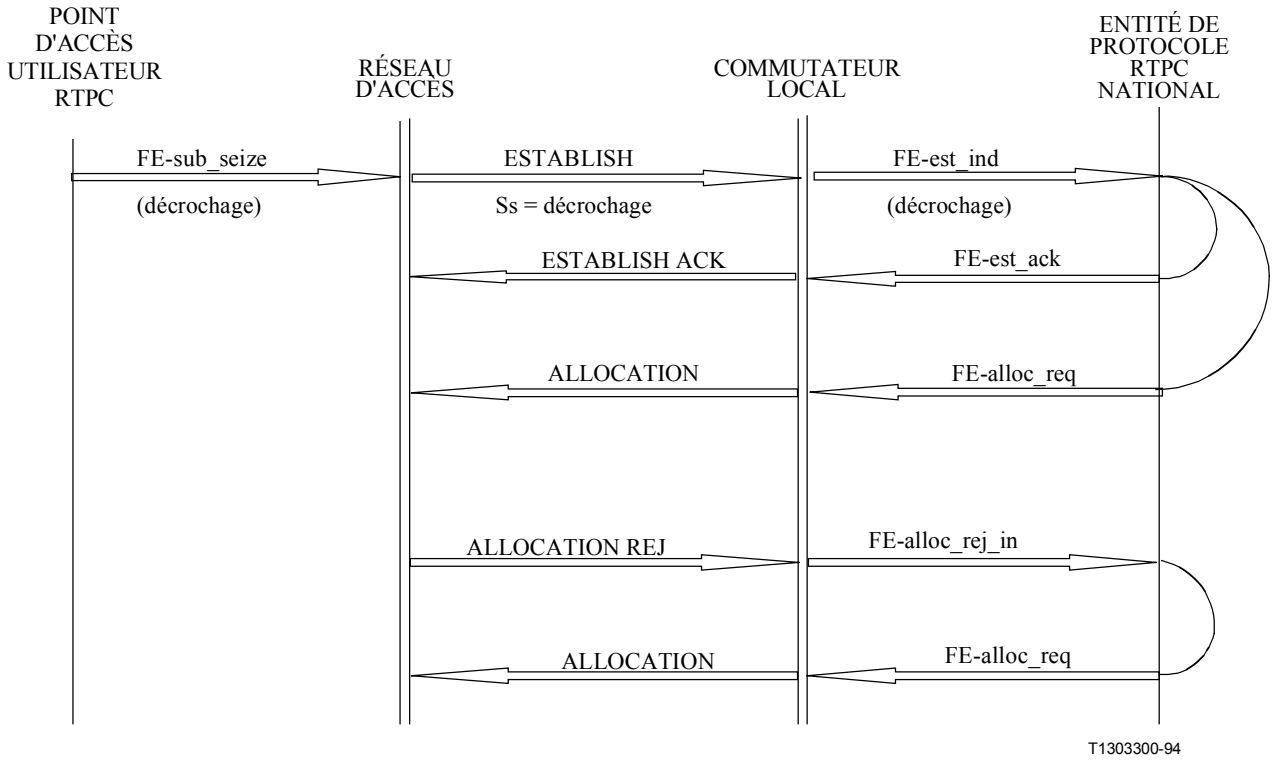


Figure K.11/G.965 – Appel RTPC lancé par l'abonné – Procédure exceptionnelle

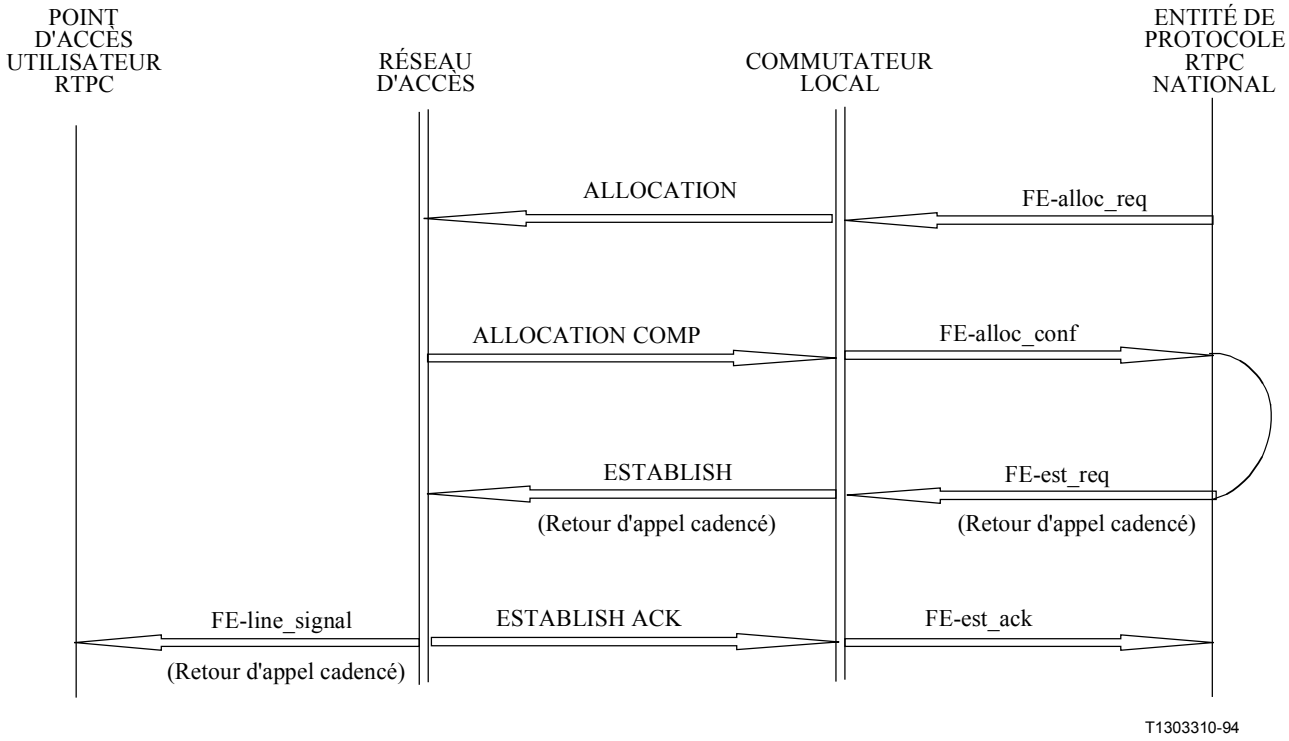


Figure K.12/G.965 – Appel RTPC lancé par le réseau

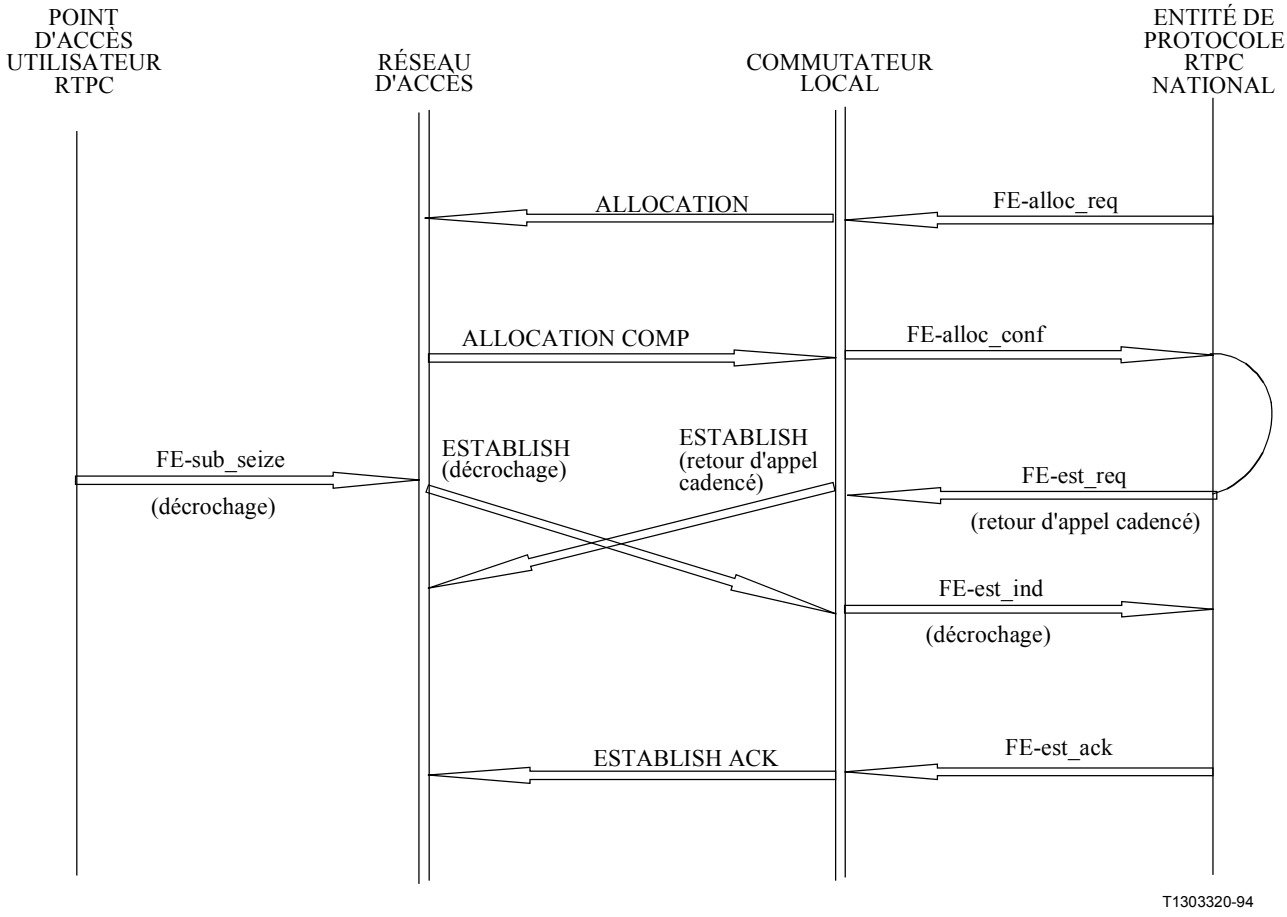


Figure K.13/G.965 – Collision d'appels RTPC – Priorité à l'appel de départ

K.9.3.2 Collision d'appels: priorité à l'appel d'arrivée

La Figure K.14 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'une collision d'appels (priorité à l'appel d'arrivée).

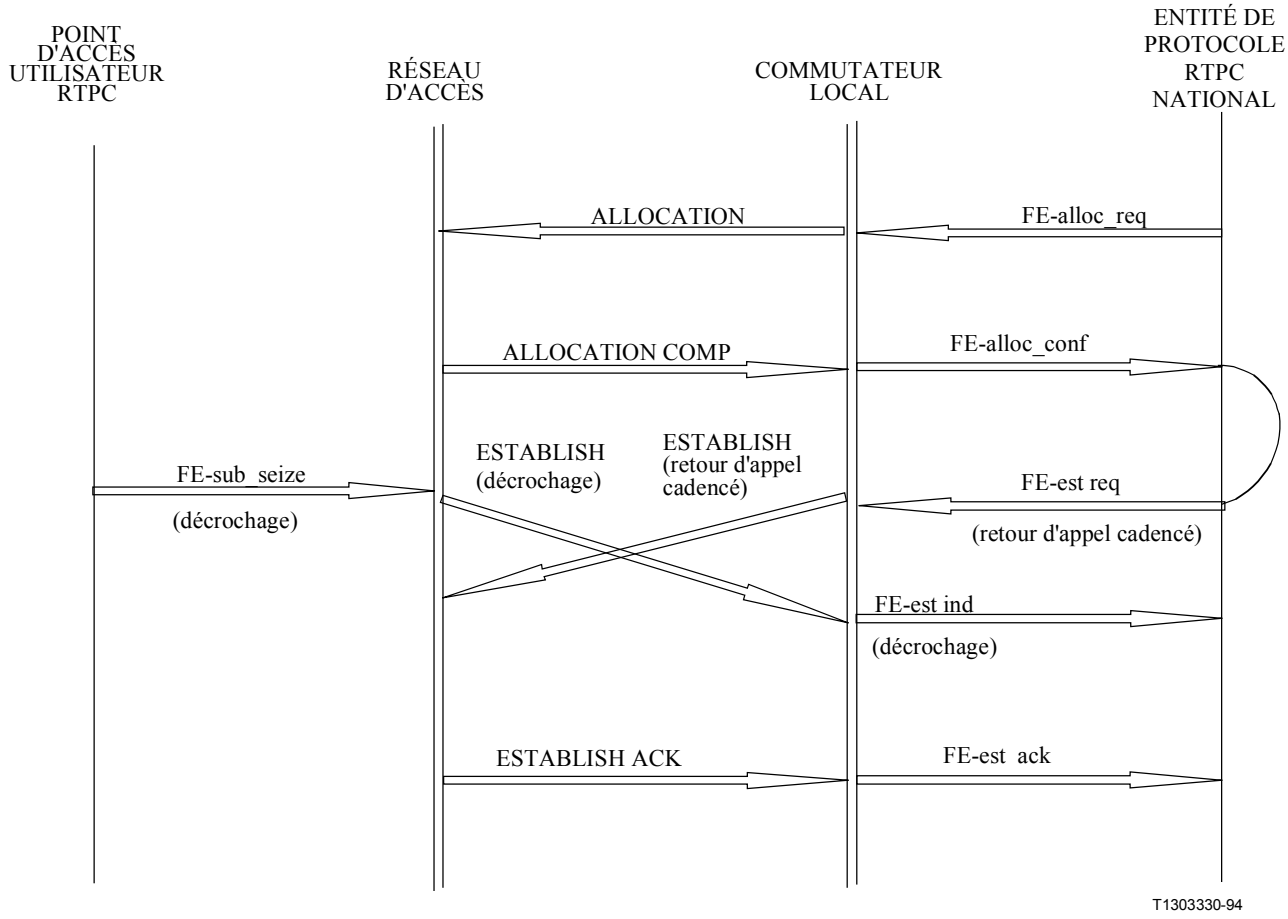


Figure K.14/G.965 – Collision d'appels RTPC – Priorité à l'appel d'arrivée

K.9.4 Libération d'appel

K.9.4.1 Libération d'appel lancée par l'abonné

La Figure K.15 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'une libération d'appel lancée par l'abonné.

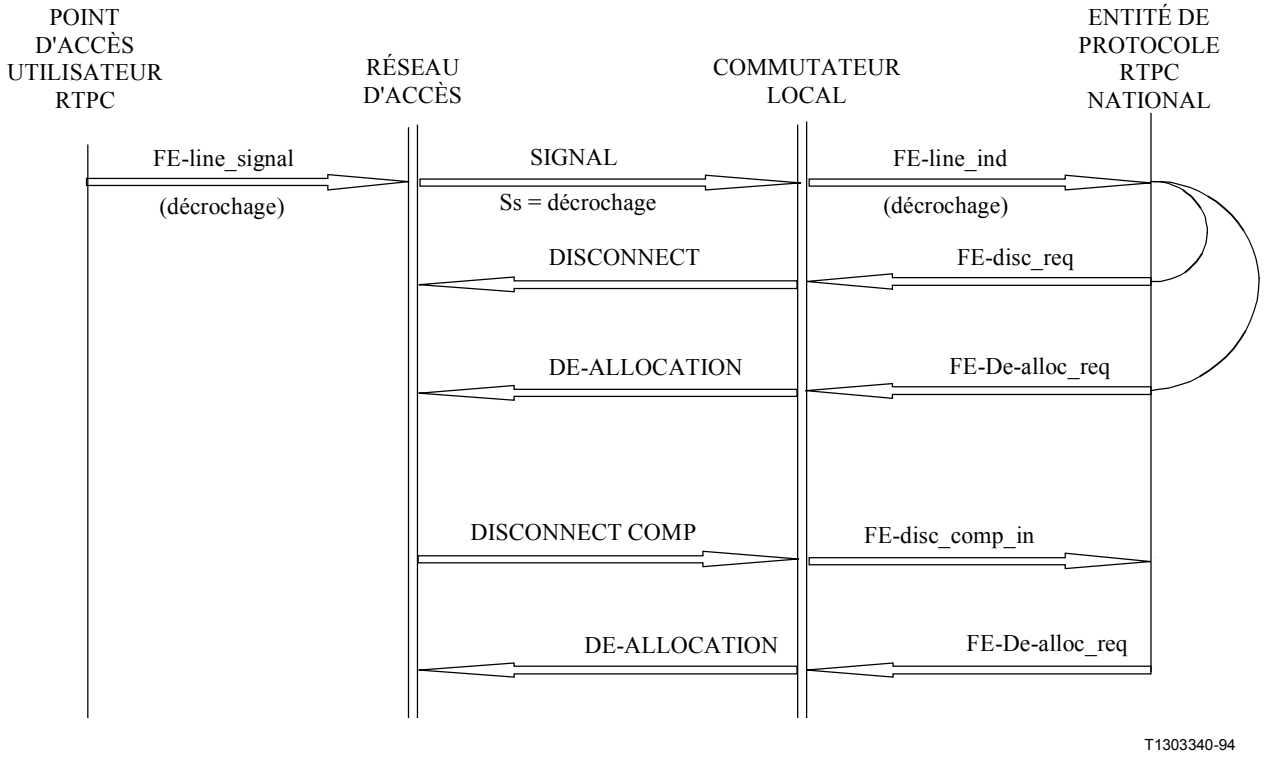


Figure K.15/G.965 – Libération d'appel RTPC lancée par l'abonné

K.9.4.2 Libération d'appel lancée par le réseau

La Figure K.16 illustre le diagramme de flux montrant un exemple d'interaction entre le protocole BCC et le protocole RTPC dans le cas d'une libération d'appel lancée par le réseau.

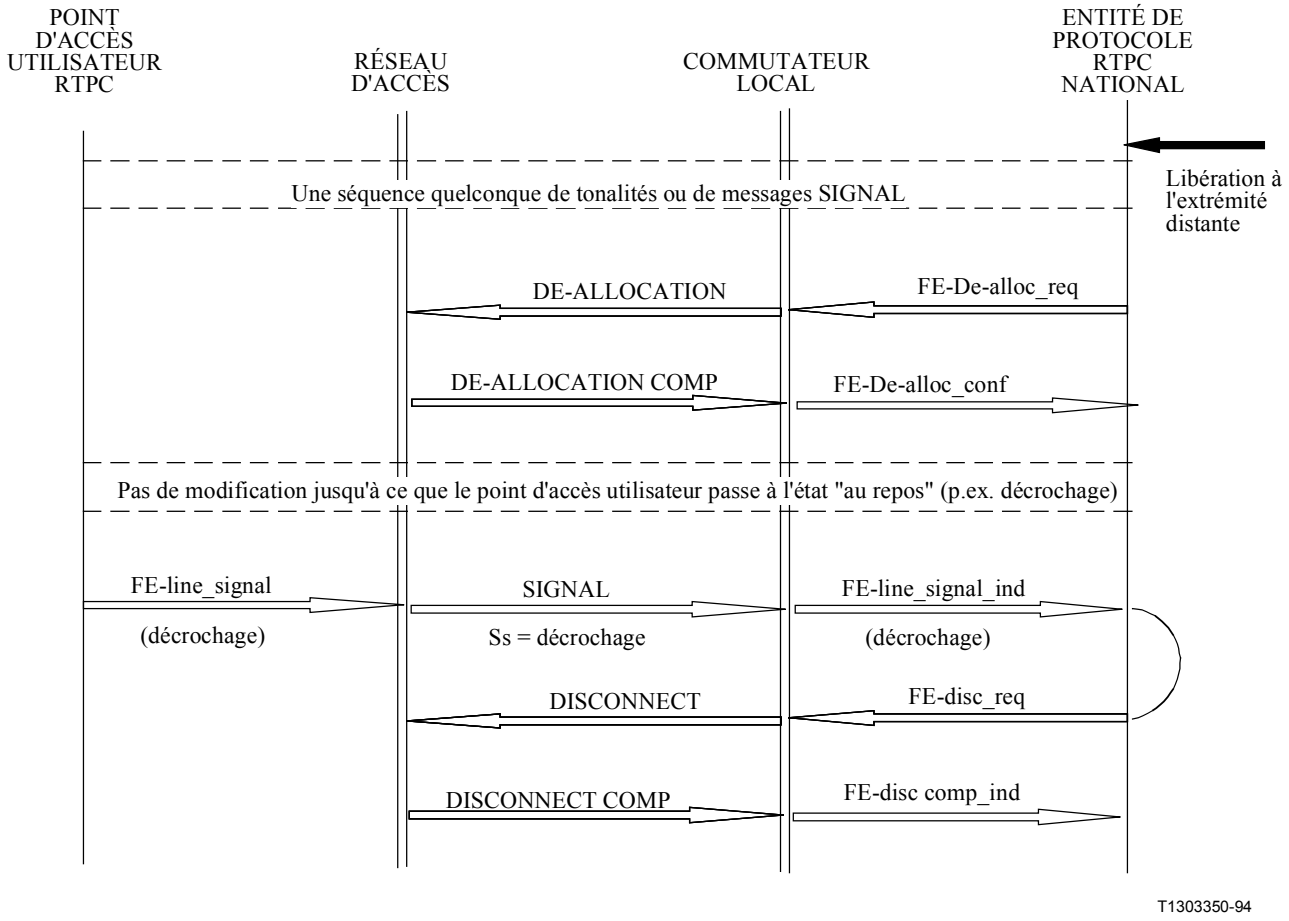


Figure K.16/G.965 – Libération d'appel RTPC lancée par le réseau

K.10 Règles des anomalies de liaison

Les anomalies de liaison persistantes, qui seront habituellement identifiées par les deux côtés, ne doivent pas être notifiées par le réseau d'accès comme étant des anomalies internes.

Si le commutateur local envoie une commande de blocage de liaison dans un message LINK CONTROL pour une liaison contenant des intervalles de temps affectés à des points d'accès (par exemple, dans le cas d'une anomalie de liaison reconnue), toutes les ressources du réseau d'accès qui se rapportent aux connexions affectées sont libérées en interne. L'entité de gestion des ressources du commutateur local doit initialiser la désaffectation interne pour la connexion de canal support notifiée et doit notifier l'événement aux entités de protocole RTPC/RNIS afin d'entreprendre les actions de service appropriées.

ANNEXE L

Exemples d'implémentation avec haute interopérabilité

La présente annexe donne des exemples des problèmes typiques qui surviennent dans l'interaction de systèmes mettant en œuvre des normes internationales telles que V5. Elle indique les précautions qui peuvent aider à atteindre un niveau élevé de compatibilité et d'interopérabilité. L'approche choisie se fonde sur des procédures qui doivent être réalisées en coopération. Il est bien connu que tous les systèmes n'acceptent pas l'ensemble complet des procédures définies. Ceci peut provenir des versions différentes des normes ou simplement des choix des fabricants. La présente annexe décrit aussi comment traiter ce problème de façon à garantir le plus haut degré de compatibilité possible.

L.1 Procédures non acceptées localement

La plupart des procédures facultatives offrent la possibilité d'être refusées par le côté qui reçoit la demande. Si un système n'accepte pas une procédure demandée de façon spécifique, il doit au moins implémenter le message de rejet approprié. Ceci permet d'informer correctement et aussitôt que possible le côté distant. De cette façon peuvent être évités les retards résultant de la surveillance des temporisateurs du côté d'origine.

L.2 Procédures non acceptées à distance

a) *refus reçu*

Le côté d'origine devrait toujours être prêt à recevoir un message de refus pour une procédure demandée. Il devrait prendre immédiatement les actions appropriées pour réaliser la tâche d'une autre façon si possible. Les refus ne devrait jamais avoir pour résultat des disfonctionnements du côté de réception, c'est-à-dire une réduction non nécessaire des services offerts;

b) *expiration locale de délais*

Si le côté d'origine ne reçoit aucune réponse à la demande mais qu'il y a un temporisateur local qui met fin à cette procédure, on devrait se comporter de la même manière que lors d'un refus.

L.3 Généralités sur la conception coopérative

a) *acceptation passive des procédures*

L'acceptation des procédures ne devrait pas être limitée sans nécessité. Un système devrait accepter une procédure dans la mesure du possible. Ceci s'applique même si – dans le cas de procédures symétriques – il n'est pas tout à fait prêt à se comporter comme partie active, c'est-à-dire, comme côté demandeur.

EXEMPLE 1: vérification d'identificateur de liaison, vérification d'identificateur de variante et d'interface, etc.

Ceci est particulièrement utile lorsque des implémentations correspondant à des versions différentes des spécifications V5 doivent coopérer, par exemple, lors du démarrage d'une interface.

Les demandes de procédures qui ne peuvent être refusées mais qu'on n'est pas prêt à accomplir devraient être sauvegardées et recevoir réponse aussitôt que les conditions ont changé et que la procédure peut s'appliquer.

EXEMPLE 2: procédure de redémarrage RTPC après une anomalie de sous-couche RTPC, lorsque le message Establish destiné à la sous-couche RTPC n'a pas encore été reçu localement mais que le côté distant demande déjà la procédure;

b) *implémentation de procédures symétriques réservées au maître*

Les implémentations réservées au maître devraient être évitées. Tout système acceptant une telle procédure (par exemple, des procédures d'alignement accéléré) devrait être prêt à être à la fois la partie active et la partie passive.

APPENDICE I

Références bibliographiques

– UIT-T G.921 (1988), *Sections numériques fondées sur la hiérarchie à 2048 kbit/s*.

– UIT-T G.961 (1993), *Système de transmission numérique en lignes locales métalliques pour accès RNIS au débit de base*.

– UIT-T M.3602 (1992), *Application des principes de maintenance aux installations d'abonné du RNIS*.

– UIT-T M.3603 (1992), *Application des principes de maintenance à l'accès de base du RNIS*.

– UIT-T M.3604 (1992), *Application des principes de maintenance à l'accès primaire du RNIS*.

– UIT-T O.162 (1992), *Appareil de surveillance en service de signaux à 2048, 8448, 34 368 et 139 264 kbit/s*.

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

– UIT-T Q.933 (1995), *Système de signalisation d'abonné numérique n° 1 – Spécification de la signalisation pour la commande et la surveillance de l'état des connexions virtuelles commutées et permanentes en mode trame*.

SÉRIES 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	Réseaux câblés et 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, circuits téléphoniques, télégraphie, télécopie 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 de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2002