Union internationale des télécommunications

UIT-T G.873.1

(03/2006)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

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

Réseaux numériques – Réseaux de transport optiques

Réseau de transport optique: protection linéaire

Recommandation UIT-T G.873.1

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
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.600–G.699
EQUIPEMENTS TERMINAUX NUMÉRIQUES	G.700–G.799
RÉSEAUX NUMÉRIQUES	G.800–G.899
Généralités	G.800–G.809
Objectifs de conception pour les réseaux numériques	G.810–G.819
Objectifs de qualité et de disponibilité	G.820–G.829
Fonctions et capacités du réseau	G.830–G.839
Caractéristiques des réseaux à hiérarchie numérique synchrone	G.840–G.849
Gestion du réseau de transport	G.850–G.859
Intégration des systèmes satellitaires et hertziens à hiérarchie numérique synchrone	G.860–G.869
Réseaux de transport optiques	**G.870–G.879**
SECTIONS NUMÉRIQUES ET SYSTÈMES DE LIGNES NUMÉRIQUES	G.900–G.999
QUALITÉ DE SERVICE ET DE TRANSMISSION – ASPECTS GÉNÉRIQUES ET ASPECTS LIÉS À L'UTILISATEUR	G.1000–G.1999
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.6000–G.6999
DONNÉES SUR COUCHE TRANSPORT – ASPECTS GÉNÉRIQUES	G.7000–G.7999
ASPECTS RELATIFS AU PROTOCOLE ETHERNET SUR COUCHE TRANSPORT	G.8000–G.8999
RÉSEAUX D'ACCÈS	G.9000–G.9999

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

Recommandation UIT-T G.873.1

Réseau de transport optique: protection linéaire

Résumé

La présente Recommandation définit le protocole de commutateur de protection automatique (APS, *automatic protection switch*) et l'opération de commutation de protection pour les systèmes de protection linéaire du réseau de transport optique au niveau des unités de données de canal optique (ODUk, *optical channel data unit k*). Les systèmes de protection examinés dans la présente Recommandation sont les suivants:

– protection de connexion de sous-réseau par unité ODUk avec surveillance intrinsèque (1+1, 1:n);
– protection de connexion de sous-réseau par unité ODUk avec surveillance non intrusive (1+1);
– protection de connexion de sous-réseau par unité ODUk avec surveillance de sous-couche (1+1, 1:n).

Source

La Recommandation UIT-T G.873.1 a été approuvée le 29 mars 2006 par la Commission d'études 15 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

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

Recommandation UIT-T G.873.1

Réseau de transport optique: protection linéaire

1 Domaine d'application

La présente Recommandation définit le protocole de commutateur de protection automatique (APS, *automatic protection switching*) et l'opération de commutation de protection pour les systèmes de protection linéaire du réseau de transport optique au niveau des unités de données de canal optique k (ODUk). Les systèmes de protection examinés dans la présente Recommandation sont les suivants:

– protection de connexion de sous-réseau par unité ODUk avec surveillance intrinsèque (1+1, 1:n);

– protection de connexion de sous-réseau par unité ODUk avec surveillance non intrusive (1+1);

– protection de connexion de sous-réseau par unité ODUk avec surveillance de sous-couche (1+1, 1:n).

Le protocole de commutation APS et l'opération de commutation de protection pour la protection annulaire d'un réseau OTN sont actuellement à l'étude.

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. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– Recommandation UIT-T G.709/Y.1331 (2003), *Interfaces pour le réseau de transport optique*.

– Recommandation UIT-T G.798 (2004), *Caractéristiques des blocs fonctionnels des équipements à hiérarchie numérique du réseau de transport optique*.

– Recommandation UIT-T G.805 (2000), *Architecture fonctionnelle générique des réseaux de transport*.

– Recommandation UIT-T G.806 (2006), *Caractéristiques des équipements de transport – Méthodologie de description et fonctionnalité générique*.

– Recommandation UIT-T G.808.1 (2006), *Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux*.

– Recommandation UIT-T G.841 (1998), *Types et caractéristiques des architectures de protection des réseaux à hiérarchie numérique synchrone*.

– Recommandation UIT-T G.872 (2001), *Architecture des réseaux de transport optiques*.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 canal de protection APS: voir la Rec. UIT-T G.870/Y.1352.

3.2 entité: voir la Rec. UIT-T G.870/Y.1352.

3.3 signal de trafic supplémentaire: voir la Rec. UIT-T G.870/Y.1352.

3.4 tête de réseau: voir la Rec. UIT-T G.870/Y.1352.

3.5 signal de trafic normal: voir la Rec. UIT-T G.870/Y.1352.

3.6 signal vide: voir la Rec. UIT-T G.870/Y.1352.

3.7 canal de communication de protection: voir la Rec. UIT-T G.870/Y.1352.

3.8 groupe de protection: voir la Rec. UIT-T G.870/Y.1352.

3.9 signal: voir la Rec. UIT-T G.870/Y.1352.

3.10 extrémité distante: voir la Rec. UIT-T G.870/Y.1352.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

APS commutateur de protection automatique (*automatic protection switching*)

DNR ne pas inverser (*do not revert*)

EXER exercice

FS commutation forcée (*forced switch*)

LO verrouillage pour protection (*lockout for protection*)

MS commutation manuelle (*manual switch*)

NR absence de demande (*no request*)

ODUk unité de données de canal optique k (*optical channel data unit k*)

OTN réseau de transport optique (*optical transport network*)

OTUk unité de transport de canal optique k (*optical channel transport unit k*)

PCC canal de communication de protection (*protection communication channel*)

RR demande d'inversion (*reverse request*)

SD dégradation du signal (*signal degrade*)

SF panne de signal (*signal fail*)

WTR attente de rétablissement (*wait to restore*)

5 Caractéristiques de protection

5.1 Méthodes et conditions de surveillance

La commutation de protection interviendra sur la base de la détection de certains défauts dans les entités de transport (de trafic et de protection) du domaine protégé. La façon dont ces défauts sont détectés fait l'objet des Recommandations relatives aux équipements (par exemple, Recommandations UIT-T G.806 et G.798). Du point de vue du contrôleur de commutation de protection, une entité située dans le domaine protégé possède un état d'absence de défaut = OK, un état dégradé (dégradation du signal = SD), ou un état défaillant (panne de signal = SF).

Les méthodes de surveillance habituelles sont les suivantes:

Surveillance inhérente – La commutation de protection est déclenchée par des défauts détectés dans la connexion de liaison d'unités ODUk (par exemple, extrémité de couche serveur et fonction d'adaptation serveur/ODUk). Aucune détection de défaut n'est effectuée dans la couche d'unités ODUk proprement dite.

NOTE – Contrairement à la protection inhérente de connexion de sous-réseau (SNC/I) de la hiérarchie SDH, la protection SNC/I des unités ODUk ne peut s'étendre que sur une seule connexion de liaison car le défaut FDI qui résulte d'autres défauts de couche serveur en amont n'est pas détecté par la fonction d'adaptation de serveur/ODUk.

Surveillance non intrusive – La commutation de protection est déclenchée par un moniteur non intrusif de la couche ODUkP ou des sous-couches ODUkT à l'extrémité distante du groupe de protection.

Surveillance de sous-couche – La commutation de protection est déclenchée par des défauts détectés dans le chemin de sous-couche (TCM) d'unités ODUkT. Un chemin de sous-couche d'unités ODUkT est établi pour chaque entité de trafic et de protection. La commutation de protection n'est donc déclenchée que lors de défauts du domaine protégé.

Le contrôleur de commutateur de protection ne tient pas compte de la méthode de surveillance qui est utilisée, du moment qu'il peut recevoir des informations (OK, SD, SF) concernant les entités de transport se trouvant dans le domaine protégé. Certains moniteurs ou certaines couches Réseau peuvent ne pas disposer d'une méthode de détection de l'état SD. Dans ce cas, il n'est pas nécessaire d'utiliser un protocole de commutation APS différent: il se passerait simplement qu'un état SD ne serait pas émis par un équipement qui ne peut pas le détecter. Lorsqu'un protocole de commutation APS est utilisé, l'implémentation ne devrait pas empêcher que l'extrémité distante déclare un état SD sur le canal de commutation APS, même si le moniteur situé à l'extrémité locale ne peut pas détecter l'état SD.

6 Commandes de groupe de protection

6.1 Commandes et états de bout en bout

Le présent paragraphe décrit les commandes qui s'appliquent au groupe de protection dans son ensemble. Lorsqu'une commutation APS est présente, ces commandes sont signalées à l'extrémité distante de la connexion. En commutation dans les deux sens, ces commandes affectent le dérivateur et le sélecteur aux deux extrémités.

Verrouillage de protection – Cette commande empêche un signal de trafic d'être sélectionné dans l'entité de protection, ce qui désactive pratiquement le groupe de protection. Si un signal de trafic supplémentaire est présent dans l'entité de protection, ce signal est rejeté.

Commutation forcée sur protection du signal de trafic normal n° n – Cette commande force le signal de trafic normal n° n à être sélectionné dans l'entité de protection dès que le dérivateur requis est présent.

Commutation forcée de signal vide – Dans les architectures à protection alternée, cette commande commute le signal vide vers l'entité de protection, à moins qu'une commande de commutation ayant une priorité égale ou supérieure ne soit en cours. Un signal de trafic normal présent dans l'entité de protection est transféré vers et sélectionné dans son entité de trafic. Dans les architectures à protection doublée, cette commande choisit le signal de trafic normal dans l'entité de trafic.

Commutation forcée de signal de trafic supplémentaire – Cette commande commute le signal de trafic supplémentaire vers l'entité de protection, à moins qu'une commande de commutation ayant une priorité égale ou supérieure ne soit en cours. Un signal de trafic normal présent dans l'entité de protection est transféré vers et sélectionné dans son entité de trafic.

Commutation manuelle sur protection du signal de trafic normal n° n – En l'absence de défaillance d'une entité de trafic ou de protection, cette commande force le signal de trafic normal n° n à être sélectionné dans l'entité de protection dès que le dérivateur requis est présent.

Commutation manuelle de signal vide – Dans les architectures à protection alternée, cette commande commute le signal vide vers l'entité de protection, à moins qu'un état de dérangement n'existe dans d'autres entités ou qu'une commande de commutation ayant une priorité égale ou supérieure ne soit en cours. Un signal de trafic normal présent dans l'entité de protection est transféré vers et sélectionné dans son entité de trafic. Dans les architectures à protection doublée, cette commande choisit le signal de trafic normal dans l'entité de trafic.

Commutation manuelle de signal de trafic supplémentaire – Cette commande commute un signal de trafic supplémentaire vers l'entité de protection, à moins qu'un état de dérangement n'existe dans d'autres entités ou qu'une commande de commutation ayant une priorité égale ou supérieure ne soit en cours. Un signal de trafic normal présent dans l'entité de protection est transféré vers et sélectionné dans son entité de trafic.

Attente de rétablissement du signal de trafic normal n° n – En commutation réversible, après la relève d'un état SF ou SD dans une entité de trafic n° n, cette commande maintient le signal de trafic normal n° n comme étant sélectionné dans l'entité de protection jusqu'à l'expiration d'un temporisateur d'attente de rétablissement. Si cette expiration intervient avant tout autre évènement ou toute autre commande, l'état sera changé en NR. Cela afin de prévenir un fonctionnement fréquent du sélecteur dans le cas de défaillances intermittentes.

Exercice du signal n° n – Commande d'application du protocole de commutation APS. Le signal est choisi de façon à ne pas modifier le sélecteur.

Ne pas inverser le signal de trafic normal n° n – En commutation irréversible, cette commande sert à maintenir un signal de trafic normal sélectionné dans l'entité de protection.

Absence de demande – Tous les signaux de trafic normal sont sélectionnés dans leurs entités correspondantes de transport de trafic. L'entité de protection transporte soit le signal vide, soit le signal de trafic supplémentaire, ou une dérivation de l'unique signal de trafic normal dans un groupe de protection doublée.

Suppression – Cette commande supprime les commandes de verrouillage de protection, de commutation forcée, de commutation manuelle, d'état d'attente WTR, ou d'exercice dans l'extrémité locale qui est active.

6.2 Commandes locales

Ces commandes ne s'appliquent qu'à l'extrémité locale du groupe de protection. Lorsqu'une commutation APS est présente, ces commandes ne sont pas signalées à l'extrémité distante via le canal de commutation APS.

Gel – Cette commande gèle l'état du groupe de protection. Les commandes additionnelles d'extrémité locale sont rejetées jusqu'à ce que le gel soit relevé. Les changements d'état et les octets de commutation APS reçus sont ignorés. Lorsque la commande de gel est relevée, l'état du groupe de protection est recalculé sur la base des octets APS reçus.

Suppression du gel

Verrouillage hors protection du signal de trafic normal n° n – Cette commande empêche le signal de trafic normal n° n d'être sélectionné dans l'entité de protection. Les commandes visant le signal de trafic normal n° n seront rejetées. Les états SF ou SD seront ignorés pour le signal de trafic normal n° n. En commutation alternée dans les deux sens, les demandes de dérivation distante pour le signal de trafic normal n° n continueront à être honorées afin d'éviter des défaillances de protocole. En conséquence, un signal de trafic normal doit être verrouillé hors protection aux deux extrémités afin d'empêcher qu'il soit sélectionné dans l'entité de protection à la suite d'une

commande ou d'une défaillance à une des deux extrémités. Plusieurs de ces commandes peuvent coexister pour différents signaux de trafic normal.

Suppression du verrouillage hors protection du signal de trafic normal n° n.

7 Architectures de protection

En architecture de protection linéaire, la commutation de protection intervient aux deux extrémités distinctes d'un chemin protégé ou d'une connexion de sous-réseau protégée. Entre ces extrémités, il y aura des entités "de trafic" comme de "protection".

Dans un certain sens de transmission, la "tête de réseau" du signal protégé est capable de remplir une fonction de dérivation, qui placera une copie d'un signal de trafic normal dans une entité de protection lorsque requis. "L'extrémité distante" remplira une fonction de sélecteur si elle est capable de choisir un signal de trafic normal soit dans son entité de trafic habituelle, ou dans une entité de protection. En transmission dans les deux sens, où les deux sens de transmission sont protégés, les deux extrémités du signal protégé rempliront normalement les deux fonctions, de dérivateur et de sélecteur.

Les architectures suivantes sont possibles:

architecture doublée (1+1) – En architecture doublée, un seul signal de trafic normal est protégé par une seule entité de protection. Le dérivateur situé en tête de réseau est permanent. La commutation intervient entièrement à l'extrémité distante.

Architecture alternée (1:n) – En architecture alternée, un ou plusieurs signaux de trafic normal sont protégés par une seule entité de protection. Le dérivateur situé en tête de réseau n'est pas établi avant qu'une commutation de protection soit requise. Si $n > 1$, on ne peut pas savoir, avant qu'un défaut ait été détecté sur un des signaux protégés, lequel des divers signaux de trafic normal devrait être dérivé vers l'entité de protection. Les architectures à protection alternée sont capables de transporter un signal de trafic supplémentaire (de basse priorité et réservable) dans l'entité de protection lorsque ce signal n'est pas en cours d'utilisation afin de protéger un quelconque signal de trafic normal. Une architecture alternée peut être utilisée même pour $n = 1$ (1:1 ou protection partagée). Cette architecture peut être choisie à la place de la très simple architecture doublée (qui ne nécessite aucune action de tête de réseau par l'algorithme de protection) étant donné que la protection partagée (1:1) est capable de transporter du trafic supplémentaire lorsque la protection doublée (1+1) ne le peut pas.

Architecture multi-alternée (m:n) – Dans cette architecture, m entités de protection sont utilisées afin de protéger n entités de trafic. Cette architecture fera l'objet d'un complément d'étude.

Dans l'hypothèse d'un très grand canal de commutation APS, le codage concernant l'entité numéro "n" utilisera un octet entier plutôt que les quelques bits de la hiérarchie SDH. Deux des 256 valeurs sont réservées: 0 sert à indiquer un signal vide ou l'entité de protection, et 0xFF (255) sert à indiquer le trafic supplémentaire.

L'architecture de chaque extrémité de la connexion doit toujours être adaptée à celle de l'autre extrémité.

7.1 Commutation dans un seul sens et dans les deux sens

Dans le cas de la transmission dans les deux sens, il est possible de choisir une commutation dans un seul sens ou dans les deux sens. En commutation dans un seul sens, les sélecteurs situés à chaque extrémité sont entièrement indépendants. En commutation dans les deux sens, l'on essaie de coordonner les deux extrémités de façon qu'elles aient toutes les deux les mêmes réglages de dérivateur et de sélecteur, même pour une défaillance dans un seul sens. La commutation dans les deux sens nécessite toujours un canal APS et/ou PCC afin de coordonner les deux extrémités. La

commutation dans un seul sens peut protéger deux défaillances en sens opposé dans des entités différentes.

7.2 Nécessité d'un canal APS/PCC

Le seul type de commutation type qui ne nécessite PAS de canal APS et/ou PCC est la commutation doublée dans un seul sens. Si un dérivateur permanent est présent dans la tête de réseau et qu'il ne soit pas nécessaire de coordonner les positions du sélecteur aux deux extrémités, le sélecteur d'extrémité distante peut être exploité entièrement en fonction des défauts et commandes reçus à l'extrémité distante.

La commutation dans les deux sens nécessite toujours un canal de commutation APS. La commutation alternée (1:n) dans un seul sens nécessite un canal de commutation APS afin de coordonner le dérivateur en tête de réseau avec le sélecteur d'extrémité distante.

7.3 Commutation réversible et irréversible

En commutation réversible, le trafic est rétabli vers les entités de trafic après qu'un motif de commutation a été relevé. Dans le cas de la relève d'une commande (par exemple, la commutation forcée), ce rétablissement intervient immédiatement. Dans le cas de la relève d'un défaut, ce rétablissement intervient généralement après l'expiration d'une temporisation "d'attente de rétablissement" qui sert à éviter un broutement des sélecteurs dans le cas de défauts intermittents.

En commutation irréversible, le trafic normal est autorisé à rester dans l'entité de protection même après que le motif de commutation a été relevé. Cette autorisation est généralement obtenue par remplacement de la précédente demande de commutation par une demande "Ne pas inverser (DNR, *do not revert*)" qui est de basse priorité.

La protection doublée est souvent préconfigurée comme étant irréversible car cette protection est de toute façon entièrement spécialisée: cela évitera l'envoi d'une seconde alerte de "panne aléatoire" du trafic. Il peut, cependant, y avoir des raisons pour préconfigurer la protection comme étant réversible (par exemple, de façon que le trafic utilise le sens "court" autour d'un anneau sauf en conditions de défaillance. Certaines politiques d'opérateur imposent également la commutation réversible même en protection doublée).

Habituellement, la protection alternée est réversible. Il est certain que si un signal de trafic supplémentaire est transporté par l'entité de protection, l'opération sera toujours réversible de sorte que le signal de trafic supplémentaire réservé pourra être rétabli. Il est certainement possible de définir le protocole de façon à permettre une commutation irréversible en protection alternée, mais l'on a jugé préférable d'inverser la commutation et de signaler la panne aléatoire du trafic lorsque l'entité de trafic est réparée plutôt que lorsqu'une autre entité du groupe tombe en panne, ce qui oblige à utiliser l'entité de protection afin de transporter un autre signal de trafic normal.

En général, le choix d'une protection réversible/irréversible sera le même aux deux extrémités du groupe de protection. Cependant, une discordance de ce paramètre n'empêche pas l'interfonctionnement – il sera seulement un peu difficile pour un côté de passer en temporisation WTR pour la relève des commutations lancées par ce côté tandis que l'autre côté passe en commande DNR (ne pas inverser) pour ses commutations. Voir également § 8.4.

7.4 Discordances de préconfiguration

Avec toutes les options de préconfiguration des groupes de protection, il existe des opportunités de discordances entre les préconfigurations des deux extrémités. Ces discordances de préconfiguration prennent une des diverses formes suivantes:

– discordances où un fonctionnement correct n'est pas possible;

– discordances où un des côtés ou les deux côtés peuvent adapter leur fonctionnement afin d'offrir un degré élevé d'interfonctionnement malgré la discordance;

– discordances qui n'empêchent pas l'interfonctionnement, comme la discordance réversible/irréversible examinée au § 8.4.

Toutes les discordances de préconfiguration ne peuvent pas être acheminées et détectées par informations transmises dans le canal de commutation APS. Compte tenu d'un nombre maximal possible de 254 entités de trafic dans un groupe de protection alternée (1:n), il y a en fait un trop grand nombre de combinaisons valides d'entités pour offrir facilement une visibilité totale de toutes les options de configuration. Ce qui est désirable, cependant, est d'offrir la visibilité concernant la catégorie médiane, où les côtés peuvent adapter leur fonctionnement de façon à interfonctionner malgré la discordance. Par exemple, un équipement préconfiguré pour la commutation dans les deux sens pourrait se replier sur la commutation dans un seul sens afin de permettre l'interfonctionnement. Un équipement préconfiguré pour la commutation doublée avec canal de commutation APS pourrait se replier sur le fonctionnement en commutation doublée dans un seul sens sans canal de commutation APS. L'utilisateur pourra continuer à être informé de la discordance de préconfiguration, mais un niveau de protection pourra encore être offert par l'équipement.

8 Protocole de commutation APS

8.1 Format du canal de commutation APS

Un canal de commutation APS est transporté par les trois premiers octets du champ APS/PCC de l'en-tête d'unité ODUk. Le quatrième octet du champ APS/PCC est réservé. Huit canaux de commutation APS indépendants sont disponibles afin d'assurer la protection au niveau ODUkP, aux six niveaux ODUkT (TCM) et à l'unique niveau de protection par connexion SNC/I d'unités ODUk, comme défini au § 15.8.2.4/G.709/Y.1331.

Le format des quatre octets APS proprement dits dans chaque trame est défini dans la Figure 1. Les valeurs de champ concernant les canaux de commutation APS sont définies dans le Tableau 1.

1								2								3								4							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Demande/ état				Type de protection				Signal demandé								Signal dérivé								Réservé							
				A	B	D	R																								

Figure 1/G.873.1 – Format du canal de protection APS

Tableau 1/G.873.1 – Valeurs de champ pour canal de protection APS

Champ		Valeur	Description
Demande/état		1111	Verrouillage de protection (LO)
		1110	Commutation forcée (FS)
		1100	Panne de signal (SF)
		1010	Dégradation du signal (SD)
		1000	Commutation manuelle (MS)
		0110	Attente de rétablissement (WTR)
		0100	Exercice (EXER)
		0010	Demande d'inversion (RR)
		0001	Ne pas inverser (DNR)
		0000	Absence de demande (NR)
		Autres	Réservé pour future normalisation internationale
Type de protection	A	0	Aucun canal de protection APS
		1	Canal de protection APS
	B	0	Doublée (dérivation permanente)
		1	Alternée (aucune dérivation permanente)
	D	0	Commutation dans un seul sens
		1	Commutation dans les deux sens
	R	0	Commutation irréversible
		1	Commutation réversible
Signal demandé		0	Signal vide
		1-254	Signal de trafic normal 1-254
		255	Signal de trafic supplémentaire
Signal dérivé		0	Signal vide
		1-254	Signal de trafic normal 1-254
		255	Signal de trafic supplémentaire

8.2 Transmission et acceptation de protocole de commutation APS

Le protocole APS/PCC est transmis via l'entité de protection. Bien qu'il puisse également être transmis de la même façon via les entités de trafic, les récepteurs ne devraient pas en faire l'hypothèse et devraient avoir la capacité d'ignorer ces informations dans les entités de trafic.

A chacun des huit niveaux, un processus d'acceptation indépendant doit être effectué. Comme le protocole de commutation APS est transporté au moyen des trois premiers octets des quatre APS/PCC, seuls ces trois octets sont pris en compte pour le processus d'acceptation. Une nouvelle valeur de protocole de commutation APS doit être acceptée si une valeur identique est reçue consécutivement dans ces trois octets d'un même niveau.

NOTE – Comme le quatrième octet du message APS message est "réservé", il n'a pas à être pris en compte dans le processus d'acceptation d'octets APS.

8.3 Type de demande

Les types de demande qui peuvent être reflétés dans les octets APS sont les types "normaux" qui sont traditionnellement pris en charge par la commutation de protection dans les hiérarchies SONET et SDH. Ces demandes reflètent la condition, la commande ou l'état ayant la priorité la plus élevée (voir Tableaux 2 et 3). Dans le cas de la commutation dans un seul sens, il s'agit de la valeur de priorité la plus élevée qui a été déterminée d'après la seule extrémité locale. En commutation dans les deux sens, la demande locale ne sera indiquée que si elle est égale ou supérieure à une quelconque demande reçue de l'extrémité distante par le canal de commutation APS. En commutation dans les deux sens, lorsque la demande de l'extrémité distante a la priorité la plus élevée, l'extrémité locale signale une demande d'inversion.

Tableau 2/G.873.1 – Priorités de demande/d'état avec protocole de commutation APS

Demande/état	Priorité
Verrouillage de protection (LO)	1 (la plus élevée)
Panne de signal (SF) – protection	2 (voir § 8.9)
Commutation forcée (FS)	3
Panne de signal (SF) – trafic	4
Dégradation du signal (SD)	5
Commutation manuelle (MS)	6
Attente de rétablissement (WTR)	7
Exercice (EXER)	8
Demande d'inversion (RR)	9
Ne pas inverser (DNR)	10
Absence de demande (NR)	11 (la moins élevée)

Tableau 3/G.873.1 – Demande/état priorités sans protocole de commutation APS

Demande/état	Priorité
Verrouillage de protection (LO)	1 (la plus élevée)
Commutation forcée (FS)	2
Panne de signal (SF)	3
Dégradation du signal (SD)	4
Commutation manuelle (MS)	5
Attente de rétablissement (WTR)	6
Ne pas inverser (DNR)	7
Absence de demande (NR)	8 (la moins élevée)

8.4 Types de protection

Les types de protection valides sont les suivants:

000x doublée dans un seul sens sans APS

100x doublée dans un seul sens avec APS

101x doublée dans les deux sens avec APS

110x alternée dans un seul sens avec APS

111x alternée dans les deux sens avec APS

Les valeurs sont choisies de façon que la valeur de dérangement (séquence de zéros) corresponde au seul type de protection qui peut fonctionner sans APS (protection doublée dans un seul sens).

Noter que les valeurs 010x, 001x, et 011x sont non valides car la protection alternée et dans les deux sens nécessite le protocole APS.

Si le bit "B" bit ne correspond pas, le sélecteur est libéré car les protections doublée et alternée sont incompatibles. Une alarme en résultera.

En admettant que le bit "B" corresponde:

Si le bit "A" ne correspond pas, le côté qui attend le protocole APS se repliera sur la commutation doublée dans un seul sens sans APS.

NOTE 1 – Si un nœud ne prend pas en charge le canal de commutation APS, une séquence de zéros sera présente dans le champ APS/PCC champ comme spécifié au § 15/G.709Y.1331.

Si le bit "D" ne correspond pas, le côté à commutation dans les deux sens se repliera sur la commutation dans un seul sens.

Si le bit "R" ne correspond pas, un des côtés libérera les commutations sur la temporisation "WTR" et l'autre émettra la commande "DNR". Les deux côtés interfonctionneront et le trafic sera protégé.

NOTE 2 – Chaque côté signale toujours ses possibilités maximales dans le champ de type de protection même s'il se replie sur un fonctionnement avec moins de possibilités (c'est-à-dire qu'un côté qui prend en charge la commutation dans les deux sens se replie sur un fonctionnement dans un seul sens en cas d'interfonctionnement avec un côté qui ne prend en charge la commutation que dans un seul sens, mais continue à signaler "1" dans le bit "D").

NOTE 3 – Le compte rendu de conditions de discordance fera l'objet d'un complément d'étude.

8.5 Signal demandé

Cet octet indique le signal que l'extrémité locale demande à faire transporter par l'entité de protection. Pour la demande NR, il s'agit soit du signal vide (0) ou du signal de trafic supplémentaire (255). Pour la demande LO, il ne peut s'agir que du signal vide (0). Pour la demande d'exercice, ce peut être le signal vide (0) ou le signal de trafic supplémentaire (255) lorsque l'exercice remplace la demande NR, ou le numéro d'un signal de trafic normal si l'exercice remplace la demande DNR. Pour la demande SF ou SD, il s'agira du numéro d'un signal de trafic normal, ou le signal vide (0) afin d'indiquer que la protection est défaillante ou dégradée. Pour toutes les autres demandes, il s'agira du numéro du signal de trafic normal dont le transport par l'entité de protection a été demandé.

8.6 Signal dérivé

Cet octet indique le signal qui est dérivé vers l'entité de protection. En protection doublée, cet octet devrait toujours indiquer le signal de trafic normal 1, qui reflète précisément le dérivateur permanent. Cela permet une commutation en deux plutôt qu'en trois phases dans le cas d'une architecture doublée. En protection alternée, cet octet indiquera le signal qui est effectivement dérivé vers l'entité de protection (c'est-à-dire soit le signal vide (0), soit le signal de trafic

supplémentaire (255) ou le numéro d'un signal de trafic normal). Il s'agira généralement du dérivateur demandé par l'extrémité distante.

8.7 Commande du dérivateur

Dans les architectures à protection doublée, le signal de trafic normal est dérivé de façon permanente vers la protection. Le signal de trafic normal numéro "1" sera toujours indiqué dans le champ de signal dérivé du canal de commutation APS.

Dans les architectures à protection alternée, le dérivateur sera réglé à celui qui est indiqué par le champ "signal demandé" du canal de commutation APS entrant. Une fois que le dérivateur a été établi, cela est indiqué dans le champ "signal dérivé" du canal de commutation APS sortant.

8.8 Commande du sélecteur

Dans les architectures doublées dans un seul sens (avec ou sans APS), le sélecteur est réglé entièrement selon la demande locale de priorité la plus élevée. Il s'agit d'une commutation à phase unique.

Dans les architectures doublées dans les deux sens, le signal de trafic normal est sélectionné dans l'entité de protection lorsque le "signal demandé" sortant et le "signal dérivé" entrant indiquent tous les deux un signal de trafic normal "1" (le "signal dérivé" entrant devrait toujours indiquer "1" dans cette architecture.) Il s'agit d'une commutation à deux phases, car l'extrémité distante ne commute pas avant l'arrivée des octets APS indiquant qu'une commutation dans les deux sens a été demandée par l'extrémité locale.

Dans les architectures alternées dans un seul sens ou dans les deux sens, un signal de trafic normal "n" ou le signal de trafic supplémentaire 255 sera sélectionné dans l'entité de protection lorsque le même numéro "n" (ou 255) apparaît dans les deux champs de "signal demandé" et de "signal dérivé" entrant. Il en résulte généralement une commutation en trois phases.

8.9 Panne de signal dans l'entité de protection

Une panne de signal dans l'entité de protection a une priorité plus élevée qu'un quelconque défaut qui provoquerait la sélection d'un signal de transport normal dans l'entité de protection. Si un signal APS est en cours d'utilisation, un défaut SF dans l'entité de protection (par laquelle le signal APS est routé) a priorité sur la commutation forcée. Une commande de verrouillage a une priorité plus élevée qu'un défaut SF. Pendant les conditions de défaillance, l'état du verrouillage doit être maintenu actif.

8.10 Demandes équiprioritaires

En général, une fois qu'une commutation a été effectuée à la suite d'une demande, elle n'est pas neutralisée par une autre demande de même priorité (comportement de premier arrivé, premier servi). Lorsque des demandes équiprioritaires apparaissent simultanément, le conflit est résolu en faveur de la demande ayant le plus petit numéro d'entité. En commutation dans les deux sens, une demande reçue par le canal de commutation APS avec un numéro d'entité inférieur aura toujours priorité sur une demande locale de priorité identique contenant un numéro d'entité plus élevé. Deux demandes équiprioritaires concernant le même numéro d'entité, provenant des deux côtés d'un groupe de protection dans les deux sens, sont considérées l'une et l'autre comme valides et équivalant à la réception d'une commande "RR" issue d'un nœud de traitement local.

8.11 Acceptation et rétention de commande

Les commandes CLEAR, LO, FS, MS et EXER sont acceptées ou rejetées en fonction des précédentes commandes, de l'état des entités de trafic et de protection dans le groupe de protection, et (en commutation dans les deux sens seulement) des octets APS reçus.

La commande CLEAR n'est valide que si une commande d'extrémité locale LO, FS, MS, ou EXER est en cours ou que si un état d'attente WTR est présent à l'extrémité locale. Si ce n'est pas le cas, cette commande est rejetée. Cette commande supprimera la commande d'extrémité locale ou l'état WTR, ce qui permet de valider la prochaine condition de priorité inférieure ou (en commutation dans les deux sens) la prochaine demande de protection APS doit être validée.

Les autres commandes sont rejetées à moins qu'elles n'aient une priorité supérieure à la commande, à la condition, ou (en commutation dans les deux sens) à la demande APS qui existait précédemment. Si une nouvelle commande est acceptée, toute commande précédente de priorité inférieure qui est neutralisée est négligée. Si une commande de priorité supérieure neutralise une condition ou (en commutation dans les deux sens) une demande APS de priorité inférieure, cette autre demande sera revalidée si elle existe encore au moment où la commande est supprimée.

Si une commande est neutralisée par une condition ou (en commutation dans les deux sens) par une demande APS, cette commande est négligée.

8.12 Temporisateur d'attente de protection

Afin de coordonner le rythme des commutations de protection dans de multiples couches ou dans des domaines de protection empilés, un temporisateur d'attente de protection peut être requis. Le but visé est soit de permettre à une commutation de protection en couche serveur d'avoir une chance de résoudre le problème avant la commutation vers une couche client, soit de permettre à un domaine de protection amont de commuter avant un domaine aval (par exemple, afin de permettre à un anneau amont de commuter avant l'anneau aval dans une configuration d'interconnexion à double nœud de sorte que la commutation intervienne dans le même anneau que la défaillance).

Chaque groupe de protection devrait avoir un temporisateur d'attente de protection préconfigurable. L'étendue et les valeurs suggérées sont les suivantes: 0, 20 ms, et de 100 ms à 10 s par échelons de 100 ms (précision de ±5 ms conformément à la Rec. UIT-T G.808.1).

Le fonctionnement du temporisateur d'attente de protection utilise la méthode "de double lecture en mémoire" spécifiée dans les normes de la hiérarchie SDH. Plus précisément, lorsqu'un défaut nouveau ou plus grave se produit (nouvel état SD ou SF, ou SD devenant SF), cet évènement n'est pas signalé immédiatement à la commutation de protection si la valeur préconfigurée du temporisateur d'attente de protection est différente de zéro. En revanche, le temporisateur d'attente de protection est lancé. Lorsque la temporisation d'attente de protection expire, l'on vérifie si un défaut existe encore sur le chemin qui a lancé le temporisateur. Si tel est le cas, ce défaut est signalé à la commutation de protection. Le défaut peut ne pas être le même que celui qui a lancé le temporisateur.

8.13 Exercice préalable

L'exercice est une commande visant à vérifier si le canal de commutation APS fonctionne correctement. Il a une priorité inférieure à toute demande de commutation "réelle". Il n'est valide qu'en commutation dans les deux sens, car celle-ci est le seul environnement dans lequel l'on peut effectuer un essai significatif en recherchant une réponse.

La commande d'exercice doit être émise avec les mêmes numéros d'entité demandée et dérivée que dans la demande NR ou DNR qu'elle remplace. La réponse valide sera une commande RR avec les numéros correspondants d'entité demandée et dérivée. Afin de permettre la détection de la commande RR, la réponse normalisée à la commande DNR devrait être DNR plutôt que RR. Lorsque la commande d'exercice est supprimée, elle est remplacée par NR si le numéro de l'entité demandée est 0 ou 255, et par DNR pour tout signal de trafic normal de numéro 1 à 254.

NOTE – L'exercice préalable pour réseau OTN a été défini différemment de l'exercice préalable défini pour la hiérarchie SDH.

8.14 Alarme de canal de protection APS

Les situations de "défaillance de protocole" dans les groupes nécessitant une commutation APS sont les suivantes:

– préconfiguration entièrement incompatible (discordance du bit "B", décrite au § 8.4);

– absence de réponse à une demande de dérivation (c'est-à-dire pas de correspondance entre message "entité demandée" émis et un message "entité dérivée" reçu) pendant une durée > 50 ms.

Si une demande inconnue ou une demande de numéro non valide d'entité est reçue, elle est ignorée. C'est à l'extrémité distante qu'il appartient d'émettre l'alarme de non-réponse en provenance de l'extrémité locale.

Appendice I

Exemples de fonctionnement

I.1 Commutation de protection doublée dans un seul sens

Le protocole APS peut être ou ne pas être présent. Même si le protocole APS n'est pas présent, la dérivation est censée être permanente, de sorte que les commutations sont effectuées immédiatement en réponse à la demande locale. Les octets APS, s'ils sont présents, n'ont qu'une valeur d'information et ne commandent pas le fonctionnement du groupe de protection. S'ils sont présents, un équipement peut permettre une recherche concernant l'état de l'extrémité distante.

Cet exemple montre la superposition de demandes SF et SD issues des côtés opposés. A titre d'illustration, l'exemple de la Figure I.1 montre une préconfiguration montée en discordance, avec côté A irréversible et un côté B réversible.

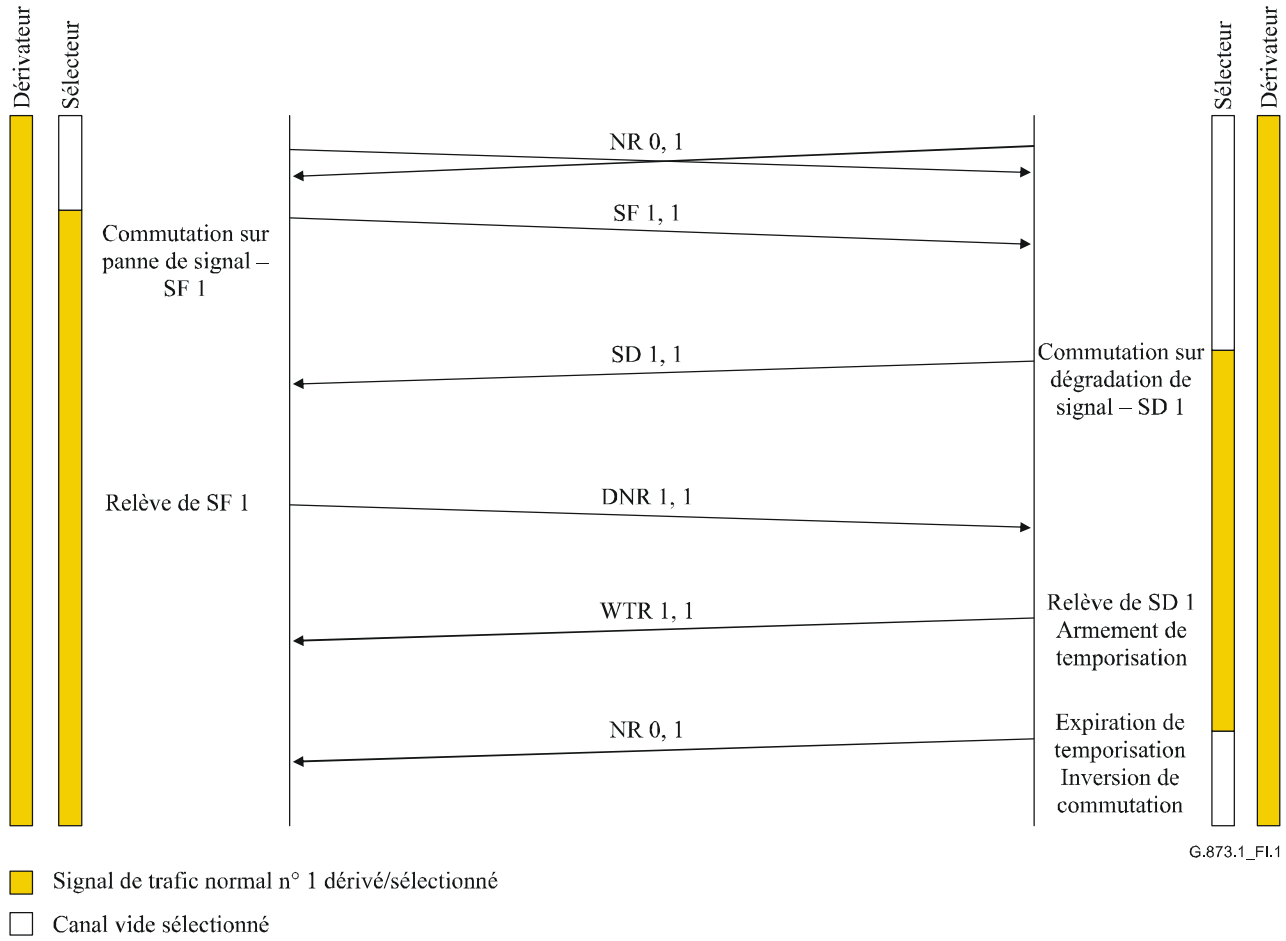

Figure I.1/G.873.1 – Exemple de flux de messages APS pour commutation doublée dans un seul sens

I.2 Commutation de protection doublée dans les deux sens

L'exemple de la Figure I.2 décrit une commutation de protection doublée dans les deux sens et irréversible. Comme le dérivateur permanent est indiqué dans les octets APS dès le départ, la commutation peut être en deux phases au lieu d'être en trois phases.

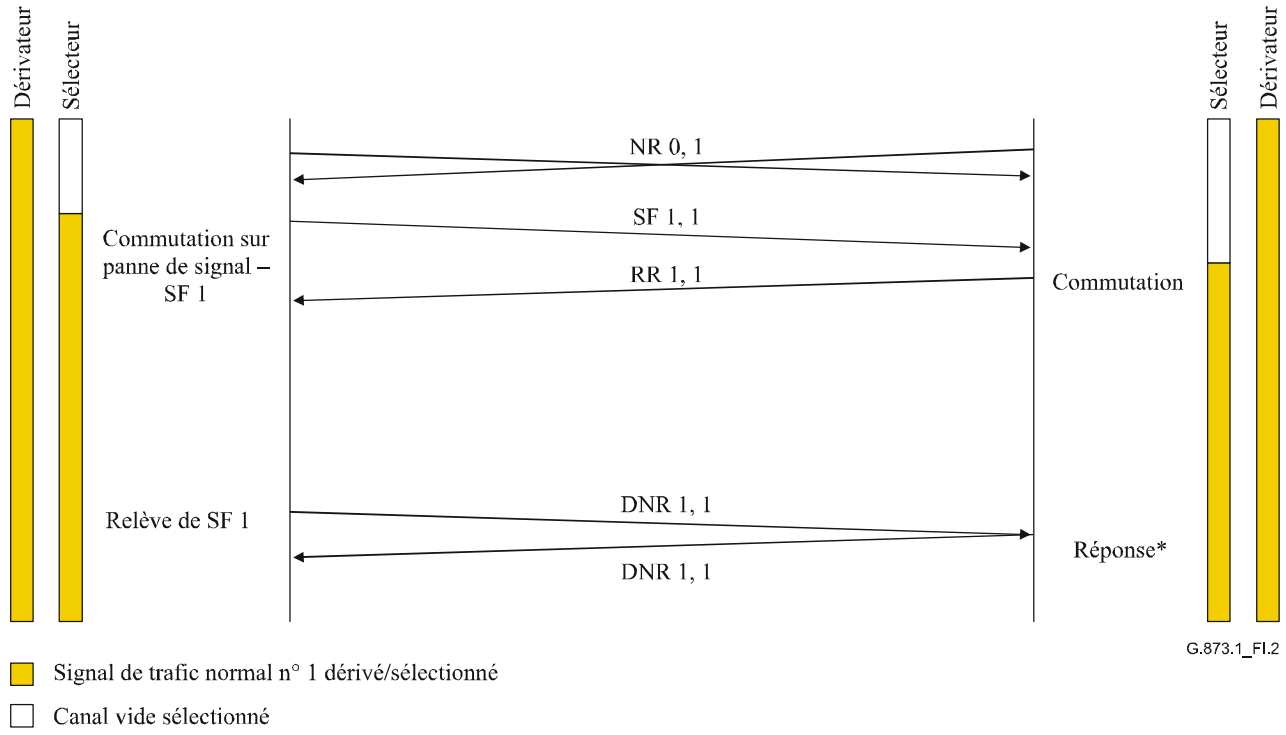

Figure I.2/G.873.1 – Exemple de flux de messages APS pour commutation doublée dans les deux sens

NOTE – Historiquement, la commande DNR a été acquittée au moyen de la commande RR. Dans ce cas, le fait de répondre à la commande DNR par un message DNR ne crée pas de différence fondamentale dans les états des deux côtés, et permet d'implémenter un exercice significatif.

I.3 Commutation alternée dans les deux sens

La Figure I.3 montre un exemple de commutation alternée dans les deux sens avec trafic supplémentaire. Ce qui est illustré est le cas où un état SD sur la voie de trafic n° 2 est réservé par un état SF sur la voie de trafic n° 3.

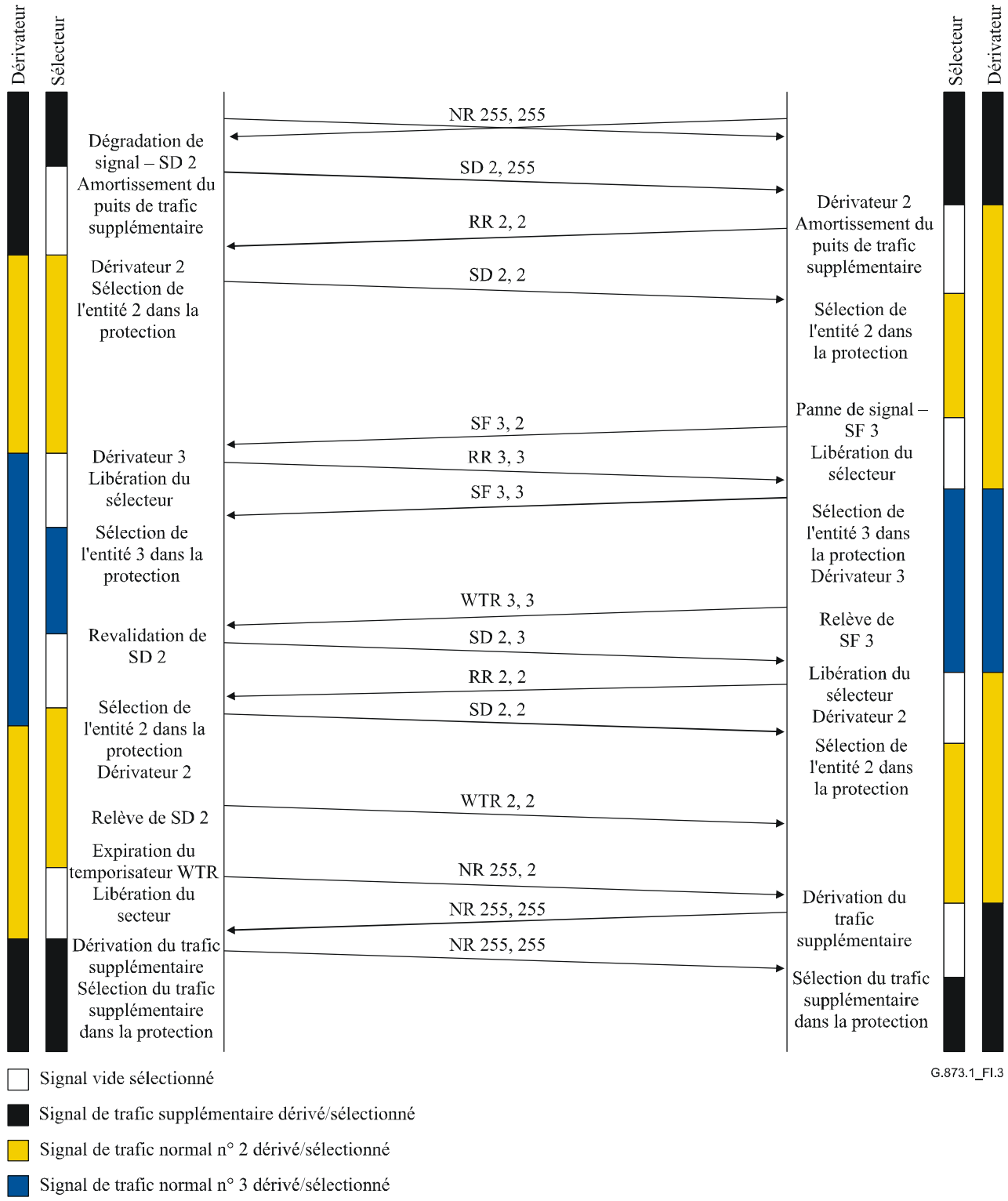

Figure I.3/G.873.1 – Exemple de flux de messages APS pour commutation alternée dans les deux sens

I.4 Fonctionnement de la commande d'exercice

La commande d'exercice vise à vérifier que l'extrémité distante répondra à une demande de canal de commutation APS dans les deux sens sans faire fonctionner le sélecteur. Cette commande est à basse priorité de façon à ne pas gêner le bon fonctionnement du groupe de protection. Elle n'est valide que lorsque la demande émise est NR ou DNR car elle a une priorité inférieure à toutes les autres demandes.

Les Figures I.4, I.5, I.6 et I.7 donnent des exemples de fonctionnement de la commande d'exercice. Dans tous les cas, ni le numéro d'entité demandée ni le numéro d'entité dérivée ne sont changés pour la commande d'exercice. Une réponse favorable consiste à recevoir une commande "RR" avec le même numéro d'entité. Noter qu'une réponse DNR à une commande DNR constitue une façon de vérifier que la commande d'exercice reçoit la réponse RR appropriée.

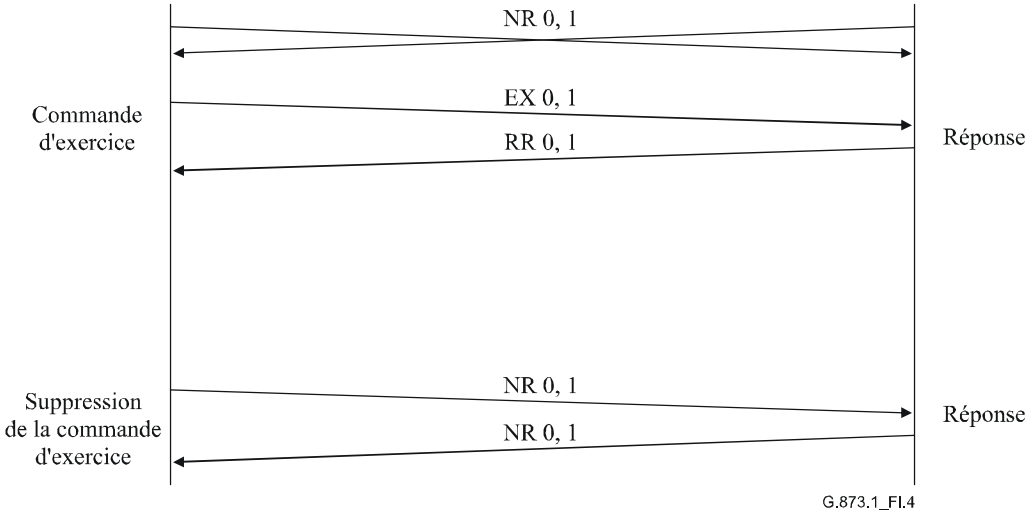

Figure I.4/G.873.1 – Exemple de commande d'exercice à partir de l'état NR en protection doublée

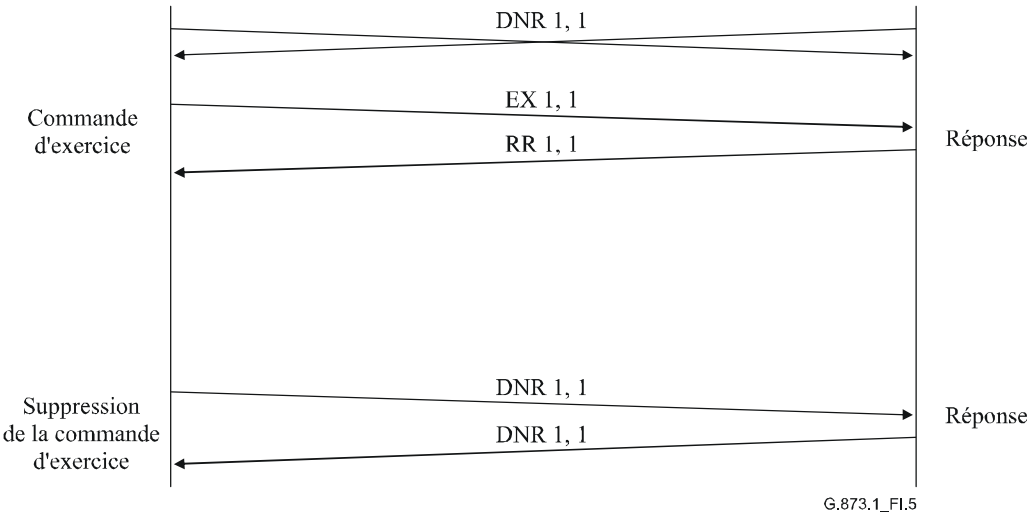

Figure I.5/G.873.1 – Exemple de commande d'exercice à partir de l'état DNR en protection doublée

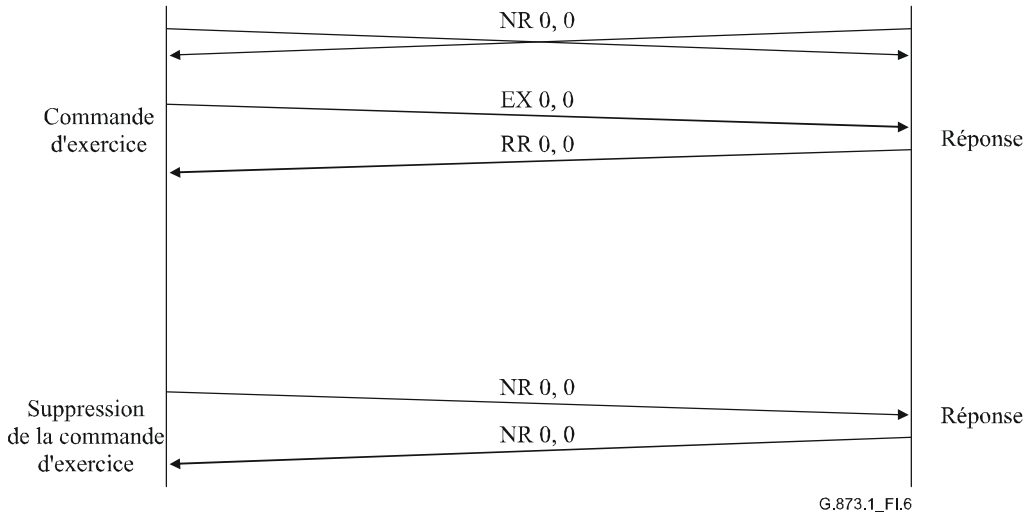

Figure I.6/G.873.1 – Exemple de commande d'exercice à partir de l'état NR en protection alternée sans trafic supplémentaire

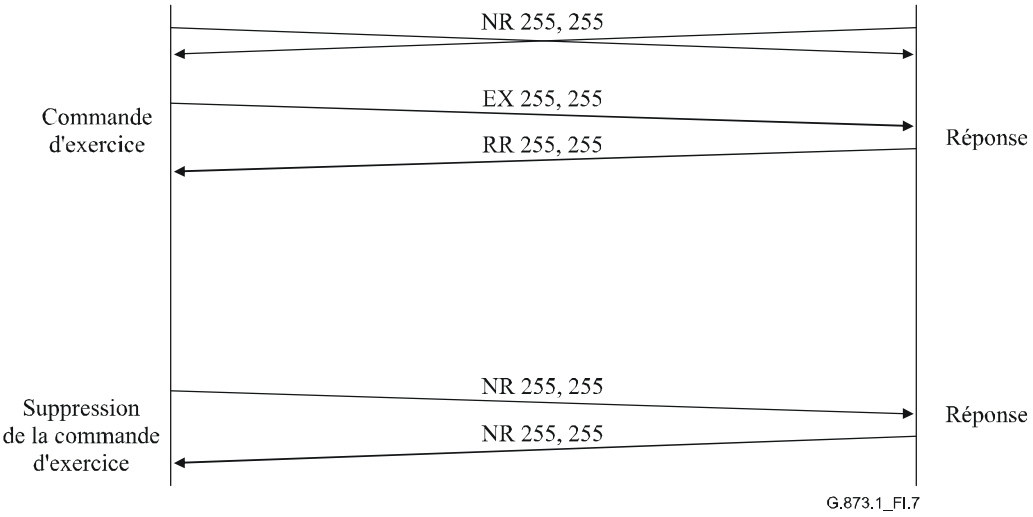

Figure I.7/G.873.1 – Exemple de commande d'exercice à partir de l'état NR en protection alternée avec trafic supplémentaire

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	Gestion des télécommunications y compris le RGT et maintenance des réseaux
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, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006