

UIT-T

G.8031/Y.1342

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(06/2006)

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

Aspects relatifs aux protocoles en mode paquet sur
couche Transport – Aspects relatifs au protocole Ethernet
sur couche Transport

SÉRIE Y: INFRASTRUCTURE MONDIALE DE
L'INFORMATION, PROTOCOLE INTERNET ET
RÉSEAUX DE PROCHAINE GÉNÉRATION

Aspects relatifs au protocole Internet – Transport

Commutation de protection Ethernet

Recommandation UIT-T G.8031/Y.1342

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
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 AUX PROTOCOLES EN MODE PAQUET SUR COUCHE TRANSPORT	G.8000–G.8999
Aspects relatifs au protocole Ethernet sur couche Transport	G.8000–G.8099
Aspects relatifs au protocole MPLS sur couche Transport	G.8100–G.8199
Objectifs de qualité et de disponibilité (suite de la série G.82x)	G.8200–G.8299
Gestion des services	G.8600–G.8699
RÉSEAUX D'ACCÈS	G.9000–G.9999

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

Recommandation UIT-T G.8031/Y.1342

Commutation de protection Ethernet

Résumé

La présente Recommandation décrit en détail la commutation de protection des signaux VLAN Ethernet, notamment en ce qui concerne les caractéristiques et les architectures de protection ETH et le protocole APS. Le mécanisme de protection considéré est le suivant:

- protection de connexion de sous-réseau Ethernet VLAN avec surveillance de sous-couche.

Source

La Recommandation UIT-T G.8031/Y.1342 a été approuvée le 6 juin 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 développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2007

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références normatives..... 1
3	Définitions 2
4	Abréviations..... 5
5	Conventions 6
	5.1 Représentation des champs..... 6
6	Introduction 6
7	Prescriptions 7
8	Caractéristiques de protection..... 8
	8.1 Méthodes et conditions de surveillance..... 8
9	Commandes de groupe de protection 9
	9.1 Commandes et états de bout en bout 9
	9.2 Commandes locales 9
10	Architectures de protection..... 10
	10.1 Commutation unidirectionnelle ou bidirectionnelle 10
	10.2 Nécessité d'une communication APS 11
	10.3 Commutation réversible ou non réversible..... 11
	10.4 Discordances de configuration 11
	10.5 Déclenchement de la commutation de protection 12
	10.6 Modèles de commutation de protection 12
11	Protocole APS..... 18
	11.1 Format du protocole APS 18
	11.2 Protocole APS à une phase..... 21
	11.3 Type de demande..... 23
	11.4 Type de protection..... 23
	11.5 Signal demandé 24
	11.6 Signal ponté 24
	11.7 Commande du pont..... 24
	11.8 Commande du sélecteur 24
	11.9 Défaillance du signal dans l'entité de transport de protection 25
	11.10 Demandes d'égale priorité 25
	11.11 Acceptation et rétention de commande 25
	11.12 Temporisateur d'attente de protection 25
	11.13 Temporisateur d'attente avant rétablissement..... 26
	11.14 Commande test 26
	11.15 Défauts de défaillance de protocole 26

	Page
Annexe A – Tableaux de transitions d'états pour la commutation de protection.....	27
A.1 Transitions d'états associées à la commutation bidirectionnelle 1:1 en mode réversible	27
A.2 Transitions d'états associées à la commutation bidirectionnelle 1:1 en mode non réversible	32
A.3 Transitions d'états associées à la commutation bidirectionnelle 1+1 en mode réversible	36
A.4 Transitions d'états associées à la commutation bidirectionnelle 1+1 en mode non réversible	41
A.5 Transitions d'états associées à la commutation unidirectionnelle 1+1 en mode réversible	46
A.6 Transitions d'états associées à la commutation unidirectionnelle 1+1 à mode non réversible	48
Appendice I – Exemple de fonctionnement du protocole APS à une phase.....	50
I.1 Introduction	50
I.2 Exemples de scénario	50
I.3 Exemples de protocole APS	51
Appendice II – Interaction entre la commutation de protection Ethernet et le protocole STP	53
Appendice III – Utilisation de points MIP dans un environnement de commutation de protection	55
III.1 Introduction	55
III.2 Généralités.....	55
III.3 Exemples de configuration	57

Recommandation UIT-T G.8031/Y.1342

Commutation de protection Ethernet

1 Domaine d'application

La présente Recommandation définit le protocole APS et les mécanismes de commutation de protection linéaires pour la connexion de sous-réseau ETH VLAN point à point dans les réseaux de transport Ethernet. Tous les autres mécanismes de protection, notamment point à multipoint et multipoint à multipoint, appellent un complément d'étude.

Les architectures de commutation de protection 1+1 et 1:1 linéaires à commutation unidirectionnelle ou bidirectionnelle sont définies dans la présente version de la Recommandation.

L'application du protocole APS et de la commutation de protection à toutes les autres architectures de réseau Ethernet (en anneau à réseau maillé par exemple, etc.) appelle un complément d'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.780/Y.1351 (2004), *Termes et définitions des réseaux à hiérarchie numérique synchrone (SDH)*.
- 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.870/Y.1352 (2004), *Termes et définitions pour les réseaux de transport optiques*.
- Recommandation UIT-T G.8010/Y.1306 (2004), *Architecture des réseaux de couche Ethernet*.
- Recommandation UIT-T G.8021/Y.1341 (2004), *Caractéristiques des blocs fonctionnels des équipements de réseau de transport Ethernet*.
- Recommandation UIT-T M.495 (1988), *Rétablissement de transmission et diversité de routage de transmission: terminologie et principes généraux*.
- Recommandation UIT-T Y.1731 (2006), *Fonctions et mécanismes d'exploitation et de maintenance pour les réseaux fondés sur Ethernet*.

- IEEE Standard 802-2001, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*.
- IEEE Standard 802.1D-2004, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*.
- IEEE Standard 802.1Q-2005, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*.

3 Définitions

La présente Recommandation utilise des termes définis dans la Rec. UIT-T G.780/Y.1351:

3.1 commutation de protection bidirectionnelle

3.2 commutation de protection unidirectionnelle

La présente Recommandation utilise des termes définis dans la Rec. UIT-T G.805:

3.3 informations adaptées

3.4 informations caractéristiques

3.5 liaison

3.6 connexion de liaison

3.7 dégradation du signal (SD)

3.8 défaillance du signal (SF)

3.9 connexion en cascade

3.10 chemin

3.11 terminaison de chemin

La présente Recommandation utilise les termes définis dans la Rec. UIT-T G.806:

3.12 fonction atomique

3.13 défaut

3.14 défaillance

3.15 défaillance du signal de serveur (SSF)

3.16 défaillance du signal de chemin (TSF)

La présente Recommandation utilise des termes définis dans la Rec. UIT-T G.870/Y.1352:

3.17 protocole APS

3.17.1 protocole à une phase

3.18 classe de protection

3.18.1 protection individuelle

3.18.2 protection de groupe

3.18.3 protection de connexion de réseau

3.18.4 protection de connexion de sous-réseau

3.18.4.1 surveillance de sous-couche (/S)

- 3.18.4.2 surveillance sans intrusion**
- 3.18.4.3 surveillance intrinsèque**
- 3.18.4.4 surveillance par test (/T)**
- 3.18.5 protection de chemin**
- 3.19 commutation**
- 3.20 composant**
 - 3.20.1 domaine protégé**
 - 3.20.2 pont**
 - 3.20.2.1 pont permanent**
 - 3.20.2.2 pont sélecteur**
 - 3.20.3 sélecteur**
 - 3.20.3.1 sélecteur sélectif**
 - 3.20.3.2 sélecteur fusionneur**
 - 3.20.4 extrémité de tête**
 - 3.20.5 extrémité de queue**
 - 3.20.6 nœud puits**
 - 3.20.7 nœud source**
 - 3.20.8 nœud intermédiaire**
- 3.21 architecture**
 - 3.21.1 architecture de protection 1+1**
 - 3.21.2 architecture de protection 1:n**
 - 3.21.3 architecture de protection (1:1)ⁿ**
- 3.22 signal**
 - 3.22.1 signal de trafic**
 - 3.22.2 signal de trafic normal**
 - 3.22.3 signal de trafic supplémentaire**
 - 3.22.4 signal vidéo**
- 3.23 temps**
 - 3.23.1 temps de détection**
 - 3.23.2 temps d'attente de protection**
 - 3.23.3 période d'attente avant rétablissement**
 - 3.23.4 temps de commutation**
- 3.24 entité de transport**
 - 3.24.1 entité de transport de protection**
 - 3.24.2 entité de transport de service**

- 3.24.3 entité de transport active**
- 3.24.4 entité de transport en réserve**
- 3.25 protection**
- 3.26 dégradation**
- 3.27 rapport de protection**

La présente Recommandation utilise des termes définis dans la Rec. UIT-T G.809:

- 3.28 adaptation**
- 3.29 flux**
- 3.30 domaine de flux**
- 3.31 point de flux**
- 3.32 terminaison de flux**
- 3.33 réseau de couche**
- 3.34 flux de liaison**
- 3.35 réseau**
- 3.36 port**
- 3.37 transport**
- 3.38 entité de transport**
- 3.39 point de flux de terminaison**

La présente Recommandation utilise des termes définis dans la Rec. UIT-T G.8010/Y.1306:

- 3.40 informations caractéristiques Ethernet (ETH_CI)**
- 3.41 point de flux Ethernet (ETH_FP)**
- 3.42 entité de maintenance**
- 3.43 groupe d'entités de maintenance**
- 3.44 niveau de groupe d'entités de maintenance**

La présente Recommandation utilise des termes définis dans la Rec. UIT-T G.8021/Y.1341:

- 3.45 fonction de transmission de flux Ethernet (ETH_FF)**

La présente Recommandation utilise des termes définis dans la Rec. UIT-T M.495:

- 3.46 temps de transfert (Tt)**

La présente Recommandation utilise des termes définis et décrits dans les Recommandations UIT-T G.8010/Y.1306 et Y.1731:

- 3.47 point d'extrémité de groupe d'entités de maintenance (MEP)**

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AI	information adaptée (<i>adapted information</i>)
APS	commutation de protection automatique (<i>automatic protection switching</i>)
CCM	message de vérification de continuité (<i>continuity check message</i>)
CI	information caractéristique (<i>characteristic information</i>)
DNR	ne pas inverser à l'état initial (<i>do not revert</i>)
EC	connexion Ethernet (<i>Ethernet connection</i>)
ETH	réseau de couche Ethernet (<i>Ethernet layer network</i>)
ETH-AIS	fonction de signal d'indication d'alarme Ethernet (<i>Ethernet alarm indication signal function</i>)
ETH-APS	fonction de commutation de protection automatique Ethernet (<i>Ethernet automatic protection switching function</i>)
ETH-CC	fonction de vérification de continuité Ethernet (<i>Ethernet continuity check function</i>)
EXER	test (<i>exercise</i>)
FS	commutation forcée (<i>forced switch</i>)
FT	terminaison de flux (<i>flow termination</i>)
LCK	verrouillé (<i>locked</i>)
LO	verrouillage de la protection (<i>lockout for protection</i>)
LOC	perte de continuité (<i>loss of continuity</i>)
LSB	bit de plus faible poids (<i>least significant bit</i>)
MEP	point d'extrémité de groupe d'entités de maintenance (<i>maintenance entity group end point</i>)
MIP	point intermédiaire de groupe d'entités de maintenance (<i>maintenance entity group intermediate point</i>)
MS	commutation manuelle (<i>manual switch</i>)
MSB	bit de plus fort poids (<i>most significant bit</i>)
NR	pas de demande (<i>no request</i>)
OAM	gestion, exploitation et maintenance (<i>operation, administration and maintenance</i>)
PDU	unité de données protocolaire (<i>protocol data unit</i>)
PS	commutation de protection (<i>protection switching</i>)
RR	demande d'inversion (<i>reverse request</i>)
RSTP	protocole d'arbre de recouvrement rapide (<i>rapid spanning tree protocol</i>)
SD	dégradation du signal (<i>signal degrade</i>)
SF	défaillance du signal (<i>signal fail</i>)
SF-P	dégradation du signal dans l'entité de protection (<i>signal fail on protection</i>)
SNC	connexion de sous-réseau (<i>subnetwork connection</i>)

SNC/I	connexion de sous-réseau à surveillance intrinsèque (<i>inherently monitored subnetwork connection</i>)
SNC/N	connexion de sous-réseau à surveillance sans intrusion (<i>non-intrusively monitored subnetwork connection</i>)
SNC/S	connexion de sous-réseau à surveillance de sous-couche (<i>sub-layer monitored subnetwork connection</i>)
SNC/T	connexion de sous-réseau à surveillance de chemin de test (<i>test-trail monitored subnetwork connection</i>)
VID	identificateur VLAN (<i>VLAN identifier</i>)
VLAN	réseau local virtuel (<i>virtual LAN</i>)
WTR	attente avant rétablissement (<i>wait-to-restore</i>)

5 Conventions

5.1 Représentation des champs

Les champs sont représentés conformément aux définitions de la norme IEEE 802.1D.

Lorsque des octets consécutifs servent à représenter un nombre binaire, l'octet de plus faible rang correspond à la valeur la plus significative.

Les bits d'un octet sont numérotés de 1 à 8, le bit 1 étant le bit de plus faible poids (LSB, *least significant bit*) et le bit 8 le bit de plus fort poids (MSB, *most significant bit*).

6 Introduction

La présente Recommandation spécifie les mécanismes de commutation de protection linéaires à appliquer aux réseaux Ethernet VLAN tels qu'ils sont décrits dans la Rec. UIT-T G.8010/Y.1306. La commutation de protection est un mécanisme de capacité de survie pleinement attribué, dans le sens où la voie et la largeur de bande de l'entité de protection est réservée pour une entité de service sélectionnée. Le mécanisme de capacité de survie est rapide et simple. L'opérateur de réseau peut plus facilement obtenir l'état du réseau (topologie de réseau actif par exemple) à l'aide d'une commutation de protection qu'avec d'autres mécanismes de capacité de survie tels que le protocole RSTP.

La présente Recommandation spécifie une architecture de commutation de protection 1+1 linéaire ainsi qu'une architecture de commutation de protection 1:1 linéaire. La première utilise une commutation unidirectionnelle ou bidirectionnelle et la seconde une commutation bidirectionnelle.

Dans une architecture de commutation de protection 1+1 linéaire, une entité de transport de protection est attribuée à chaque entité de transport de service. Le trafic normal est copié et alimente l'entité de transport de service et l'entité de transport de protection par le biais d'un pont permanent situé à la source du domaine protégé. Le trafic transitant sur ces deux entités est transmis simultanément au puits du domaine protégé, où une sélection est faite sur la base de certains critères prédéterminés, tels qu'une indication de défaut de serveur.

Bien que la sélection se fasse uniquement au puits du domaine protégé dans l'architecture de commutation de protection 1+1 linéaire, la commutation de protection 1+1 bidirectionnelle requiert le protocole de coordination APS de telle sorte que les sélecteurs sélectionnent la même entité dans les deux sens. Par contre, la commutation de protection 1+1 unidirectionnelle ne requiert pas ce protocole.

Dans l'architecture de commutation de protection 1:1 linéaire, l'entité de transport de protection est associée à l'entité de transport de service. Toutefois, le trafic normal est acheminé dans l'entité de transport de service ou dans l'entité de transport de protection à l'aide d'un pont sélecteur situé à la source du domaine protégé. Le sélecteur situé au puits du domaine protégé sélectionne l'entité qui achemine le trafic normal. Le protocole de coordination APS est nécessaire car la source et le puits doivent être coordonnés pour que le point sélecteur à la source et le sélecteur au puits sélectionnent la même entité.

7 Prescriptions

- 1) La commutation de protection Ethernet devrait être applicable à la connexion de sous-réseau ETH VLAN point à point qui fournit une connectivité entre deux points de flux ETH dans un domaine de flux ETH. Un ou plusieurs identificateurs VID peuvent être utilisés pour identifier une ou plusieurs connexions de sous-réseau ETH VLAN point à point au sein de liaisons ETH. On pourra obtenir d'autres détails sur l'Ethernet et les fonctions atomiques associées dans la Rec. UIT-T G.8010/Y.1306. La protection d'autres entités appelle un complément d'étude.
- 2) Le domaine protégé devrait être configuré de telle sorte que 100% du trafic de service dégradé soit protégé en cas de défaillance d'une seule entité de service.
- 3) Le temps de transfert (Tt) devrait être inférieur à 50 ms.
- 4) La connectivité de couche ETH de l'entité de transport de service et de l'entité de transport de protection devrait être surveillée périodiquement.
- 5) Après un événement de commutation de protection, les trames devraient être fournies dans l'ordre.
NOTE – Après un événement de commutation de protection, les trames peuvent être temporairement perdues ou dupliquées en raison de la différence des temps de propagation entre conduits.
- 6) La commutation de protection individuelle et la commutation de protection de groupe devraient être prises en charge.
- 7) La commutation réversible et la commutation non réversible devraient être proposées comme options d'opérateur de réseau.
- 8) Une discordance entre les positions pont/sélecteur aux extrémités proche et distante devrait être détectée.
 - La discordance pont/sélecteur pour l'élément de réseau local devrait être détectée et signalée.
 - La discordance pont/sélecteur devrait être supprimée par l'opérateur de réseau.
- 9) Des demandes d'opérateur telles des commandes de verrouillage de la protection, de commutation forcée ou de commutation manuelle devraient être prises en charge.
- 10) La protection avec ordre de priorité entre une défaillance du signal (SF, *signal fail*) et des demandes d'opérateur devrait être prise en charge.
- 11) Une "fonction d'attente générique" réglable devrait être fournie de manière à différer le début de l'action de commutation de protection.

8 Caractéristiques de protection

8.1 Méthodes et conditions de surveillance

La commutation de protection sera fondée sur la détection de certains défauts dans les entités de transport (de service et de protection) du domaine protégé. La façon dont on détecte ces défauts fait l'objet de Recommandations sur les équipements (par exemple, la Rec. UIT-T G.8021/Y.1341). Dans le cadre du processus de commutation de protection, une entité de transport du domaine protégé présente suivant le cas l'état OK, défaillant (défaillance du signal = SF) ou dégradé (dégradation du signal = SD).

Les méthodes de surveillance habituelles sont les suivantes:

Surveillance intrinsèque – La surveillance intrinsèque est fondée sur la détection de défauts par une fonction de terminaison de chemin ou une fonction d'adaptation au niveau de l'extrémité de queue. La protection de sous-réseau Ethernet à surveillance intrinsèque (SNC/I) est fondée sur le mécanisme de surveillance intrinsèque.

Surveillance non intrusive – La commutation de protection est déclenchée par une surveillance non intrusive au niveau de l'extrémité de queue du groupe de protection, ce qui permet de protéger un segment d'un chemin ne faisant pas l'objet de contrainte en raison du début ou de la fin du chemin. La protection de sous-réseau Ethernet à surveillance non intrusive (SNC/N) est une protection linéaire fondée sur le mécanisme de surveillance non intrusive. La surveillance non intrusive peut être fondée sur la surveillance d'une couche ou d'une sous-couche (surveillance non intrusive TCM par exemple).

Surveillance de sous-couche – La protection de sous-couche Ethernet à surveillance de sous-couche (SNC/S) est une architecture de protection linéaire fondée sur la surveillance de sous-couche. Chaque connexion de liaison composite en série est étendue par la surveillance de connexion en cascade (TCM, *tandem connection monitoring*) ou par des fonctions d'adaptation/de terminaison de segment pour obtenir l'état de défaut indépendamment du signal de trafic présent. Dans le cas de couches de réseau prenant en charge la surveillance TCM, il est intéressant d'instancier un segment à surveillance TCM d'un chemin précisément dans un segment protégé de telle sorte que la commutation de protection ne soit fondée que sur les défauts apparaissant dans le segment protégé. Cela présente en outre, par rapport à la protection SNC/N, l'avantage suivant: les défauts présents en aval du segment protégé ne seront pas visibles à des fins de commutation de protection.

Chemin de test – Les défauts sont détectés au moyen d'un chemin de test supplémentaire. Un chemin de test supplémentaire est établi entre la source et le puits du domaine protégé, qui comprend un groupe de protection de connexions de sous-réseau. La protection de sous-réseau Ethernet à surveillance de chemin de test (SNC/T) est fondée sur un mécanisme de surveillance de test applicable uniquement à la protection de groupe.

Le contrôleur de commutation de protection ne tient pas compte de la méthode de surveillance utilisée tant qu'il peut obtenir des informations (OK, SF, SD le cas échéant) sur les entités de transport du domaine protégé. Certains mécanismes de surveillance ou couches de réseau peuvent ne pas avoir de méthode de détection de défaillance du signal. Si c'est le cas, il est inutile d'utiliser un autre protocole APS – il n'y aurait simplement pas d'émission d'une défaillance du signal de la part d'un équipement incapable de le détecter. En cas d'utilisation d'un protocole APS, l'implémentation ne devrait pas empêcher l'extrémité distante de déclarer une défaillance du signal vers le protocole APS, même si le mécanisme de surveillance à l'extrémité proche ne peut pas la détecter.

Dans la présente version de la présente Recommandation, l'architecture de surveillance SNC/S est prise en charge pour la connexion de sous-réseau ETH VLAN point à point. D'autres méthodes de surveillance (telles que SNC/I, SNC/N et SNC/T) appellent un complément d'étude.

9 Commandes de groupe de protection

9.1 Commandes et états de bout en bout

Le présent paragraphe décrit des commandes qui s'appliquent au groupe de protection dans son ensemble. Lorsqu'un protocole APS est présent, ces commandes sont signalées à l'extrémité distante de la connexion. En commutation bidirectionnelle, ces commandes affectent le pont et le sélecteur aux deux extrémités.

Verrouillage de la protection – Cette commande empêche la sélection d'un signal de service dans l'entité de transport de protection, ce qui en pratique désactive le groupe de protection.

Commutation forcée du signal de trafic normal vers l'entité de protection – Cette commande force la sélection du signal de trafic normal dans l'entité de transport de protection.

Commutation manuelle du signal de trafic normal vers l'entité de protection – En l'absence de défaillance d'une entité de transport de service ou de protection, cette commande force la sélection du signal de trafic normal dans l'entité de transport de protection.

Attente avant rétablissement du signal de trafic normal – En fonctionnement réversible, après suppression d'un état SF (ou SD le cas échéant) dans l'entité de transport de service, cette commande maintient le signal de trafic normal tel que sélectionné dans l'entité de transport de protection jusqu'à l'expiration d'un temporisateur d'attente avant rétablissement. Si cette expiration se produit avant tout autre événement ou commande, l'état passera à NR. Ce mécanisme sert à éviter l'utilisation fréquente du sélecteur en cas de défaillances intermittentes.

Signal de test – Cette commande permet de tester le protocole APS. Le signal est choisi de façon à ne pas modifier le sélecteur.

Ne pas inverser le signal de trafic normal – En fonctionnement non réversible, cette commande est utilisée pour maintenir un signal de trafic normal sélectionné dans l'entité de transport de protection.

Pas de demande – Cette commande désigne l'état auquel passe la logique de priorité locale dans toutes les situations où aucune demande de commutation de protection locale notamment "attente avant rétablissement" et "Ne pas inverser" n'est active. Le signal de trafic normal est sélectionné dans l'entité de transport correspondante.

Suppression – Cette commande supprime la commande de verrouillage de la protection, de commutation de protection, de commutation manuelle, d'état WTR ou de test dans l'extrémité proche active.

9.2 Commandes locales

Ces commandes ne s'appliquent qu'à l'extrémité proche du groupe de protection. Même en cas de prise en charge d'un protocole APS, elles ne sont pas signalées à l'extrémité distante.

Gel – Cette commande gèle l'état du groupe de protection. Tant que le gel n'est pas supprimé, les nouvelles commandes d'extrémité proches sont rejetées. Les changements de situation et les informations APS reçues sont ignorés. Lorsque la commande de gel est supprimée, l'état du groupe de protection est recalculé à partir de la situation et des informations APS reçues.

Suppression du gel

Verrouillage hors protection du signal de trafic normal – Cette commande empêche la sélection du signal de trafic normal dans l'entité de protection. Les commandes applicables au signal de trafic normal seront rejetées. Pour le trafic normal, toute indication d'état SF (ou SD le cas échéant) sera ignorée. En commutation bidirectionnelle, les demandes de pont distant relatives au signal de trafic normal continueront à être honorées pour empêcher des défaillances de protocole. Par conséquent, un signal de trafic normal doit être verrouillé hors de l'entité de transport de protection aux deux extrémités afin d'empêcher sa sélection dans l'entité de transport de protection en raison d'une commande ou d'une défaillance à l'une de ses deux extrémités.

Suppression du verrouillage hors protection du signal de trafic normal

10 Architectures de protection

Dans le cadre de l'architecture de protection linéaire définie dans la présente version de la Recommandation, la commutation de protection intervient aux deux points d'extrémité distinctes d'une connexion de sous-réseau ETH VLAN point à point. Entre ces deux points d'extrémité se trouvent une entité de transport "de service" et une entité de transport "de protection".

Dans un sens de transmission donné, "l'extrémité de tête" de l'entité protégée est capable d'assurer une fonction de pont qui place en cas de besoin une copie d'un signal de trafic normal dans une entité de transport de protection. "L'extrémité de queue" assure alors une fonction de sélecteur en sélectionnant un signal de trafic normal dans son entité de transport de service habituel ou dans une entité de transport de protection. Dans le cas d'une transmission bidirectionnelle, où les deux sens de transmission sont protégés, les deux extrémités de l'entité protégée assurent généralement des fonctions de pont et de sélecteur.

Les architectures suivantes sont possibles:

1+1 – Dans une architecture 1+1, une entité de transport de protection est utilisée pour protéger le signal de trafic normal. Au niveau de l'extrémité de tête, le pont est permanent. La commutation a lieu exclusivement au niveau de l'extrémité de queue.

1:1 – Dans une architecture 1:1, une entité de transport de protection est utilisée pour protéger le signal de trafic normal. Au niveau de l'extrémité de tête, le pont n'est établi que lorsqu'une commutation de protection est requise.

L'architecture à chaque extrémité du domaine protégé doit être adaptée.

10.1 Commutation unidirectionnelle ou bidirectionnelle

Dans le cas d'une transmission bidirectionnelle, on peut choisir d'appliquer une commutation unidirectionnelle ou bidirectionnelle. En commutation unidirectionnelle, les sélecteurs à chaque extrémité sont complètement indépendants. En commutation bidirectionnelle, on essaie de coordonner les deux extrémités de telle sorte qu'elles présentent des réglages de pont et de sélecteur identiques, même en cas de défaillance unidirectionnelle. La commutation bidirectionnelle requiert toujours des informations APS pour coordonner les deux points d'extrémité. La commutation unidirectionnelle permet d'assurer une protection lorsque deux défaillances unidirectionnelles apparaissent suivant des sens opposés dans des entités différentes.

10.2 Nécessité d'une communication APS

La commutation unidirectionnelle 1+1 correspond au seul type de commutation pour lequel l'utilisation d'une communication APS n'est pas obligatoire. Un pont permanent se trouve à l'extrémité de tête et il est inutile de coordonner les positions du sélecteur entre les deux extrémités: le sélecteur à l'extrémité de queue peut être exploité uniquement en fonction des défauts et des commandes reçus à cette extrémité.

La commutation bidirectionnelle requiert toujours une communication APS.

10.3 Commutation réversible ou non réversible

En fonctionnement réversible, le signal de trafic normal est rétabli dans l'entité de transport de service une fois que la ou les conditions ayant entraîné une commutation ont été supprimées. En cas de suppression d'une commande (par exemple la commutation forcée), ce rétablissement est immédiat. En cas de suppression d'un défaut, le rétablissement se produit généralement après l'expiration d'un temporisateur "d'attente avant rétablissement", utilisé pour éviter le basculement répété du sélecteur dans le cas de défauts intermittents.

En fonctionnement non réversible, le signal de trafic normal est autorisé à rester dans l'entité de transport de protection même après la suppression du motif de commutation. Cela se fait généralement en remplaçant la demande de commutation précédente par une demande DNR "Ne pas inverser", qui est de faible priorité.

Une protection 1+1 est souvent configurée comme non réversible, la protection étant pleinement attribuée dans tous les cas; on évite ainsi l'apparition d'un second "signal transitoire" dans le signal de trafic normal. Il peut toutefois y avoir des motifs en faveur d'une configuration à commutation réversible (par exemple pour que le signal de trafic normal utilise le conduit "court" sauf en situation de défaillance. Certaines politiques d'opérateur imposent également le mode réversible même en protection 1+1).

La protection 1:1 est généralement réversible. Bien que l'on puisse définir le protocole de manière à autoriser le fonctionnement non réversible en protection 1:1, il est préférable, en raison du degré d'optimisation généralement supérieur de l'entité de transport (en termes de temps de propagation et de ressources), d'inverser la commutation du signal de trafic normal (moyennant l'apparition d'un signal transitoire) lorsque l'entité de transport de service est réparée.

En général, le choix du mode de fonctionnement (réversible ou non réversible) sera le même aux deux extrémités du groupe de protection. Une discordance entre les valeurs de ce paramètre n'empêcherait cependant pas l'interfonctionnement – il serait seulement bizarre qu'un côté passe à l'état WTR pour supprimer une commutation lancée à cette extrémité tandis que l'autre côté passe à l'état DNR pour sa commutation.

10.4 Discordances de configuration

Compte tenu de toutes les options de configuration des groupes de protection, il existe des risques de discordance entre les configurations des deux extrémités. Ces discordances peuvent prendre plusieurs formes:

- Discordance empêchant tout fonctionnement correct.
- Discordance pour laquelle un des côtés ou les deux peuvent adapter leur fonctionnement afin d'assurer un certain degré d'interfonctionnement en dépit de la discordance.
- Discordance n'empêchant pas l'interfonctionnement. Voir à titre d'exemple la discordance entre les fonctionnements réversible/non réversible aux § 10.3 et 11.4.

Certaines discordances de configuration ne peuvent pas être communiquées et détectées par les informations transmises par la communication APS. Il y a en fait un trop grand nombre de combinaisons valables d'entités pour avoir une visibilité complète de toutes les options de configuration. Il est souhaitable, toutefois, d'avoir une visibilité concernant la catégorie intermédiaire, dans laquelle les côtés peuvent adapter leur fonctionnement pour assurer un interfonctionnement en dépit de la discordance. Par exemple, un équipement configuré pour une commutation bidirectionnelle pourrait revenir à une commutation unidirectionnelle pour permettre l'interfonctionnement. Un équipement configuré pour une commutation 1+1 avec communication APS pourrait revenir à un fonctionnement en commutation unidirectionnelle 1+1 sans communication APS. L'utilisateur pourrait continuer à être informé de la discordance de configuration, un certain niveau de protection pouvant toutefois être encore assuré par l'équipement.

10.5 Déclenchement de la commutation de protection

La commutation de protection devrait par exemple être effectuée:

- lorsqu'elle est lancée au moyen d'une commande d'opérateur (par exemple commutation forcée, commutation manuelle) de priorité supérieure à toute autre demande locale ou à la demande d'extrémité distante;
- lorsque l'état SF est déclaré dans l'entité de transport active et ne l'est pas dans l'entité de transport de réserve, et que la situation SF détectée est de priorité supérieure à toute autre demande locale à la demande d'extrémité distante;
- lorsque l'on reçoit, dans une architecture 1+1 ou 1:1 bidirectionnelle, une demande de protocole APS de commutation de priorité supérieure à toute autre demande locale.

D'autres cas sont décrits, sous forme de transition d'états, dans l'Annexe A.

10.5.1 Conditions de déclaration de défaillance du signal

L'état SF est déclaré lorsque la condition de défaillance du signal de chemin ETH est détectée. La défaillance du signal de chemin ETH est spécifiée dans la Rec. UIT-T G.8021/Y.1341.

10.6 Modèles de commutation de protection

La Figure 10-1 donne un exemple des modèles de commutation de protection SNC/S ETH VLAN définis dans la présente Recommandation. D'autres scénarios de réseau sont admissibles.

Dans la fonction de transmission de flux ETH (ETH_FF), un processus de commutation de protection de connexion de sous-réseau ETH est instancié pour protéger la connexion ETH (EC). Une commutation de protection configurée pour une connexion Ethernet (c'est-à-dire pour la connexion de sous-réseau ETH protégée) est définie entre deux points de flux ETH (ETH_FP) conformément à la Figure 10-1. Chaque processus de commutation de protection de connexion de sous-réseau instancié détermine la sortie ETH_FP spécifique sur laquelle les informations ETH_CI protégées sont transférées.

Par exemple, dans le cas d'une configuration de commutation de protection 1:1, les informations ETH_CI de la connexion ETH protégée peuvent être transférées vers l'entité de transport de service ou vers l'entité de transport de protection par le processus de commutation de protection de sous-réseau ETH instancié dans la fonction ETH_FF.

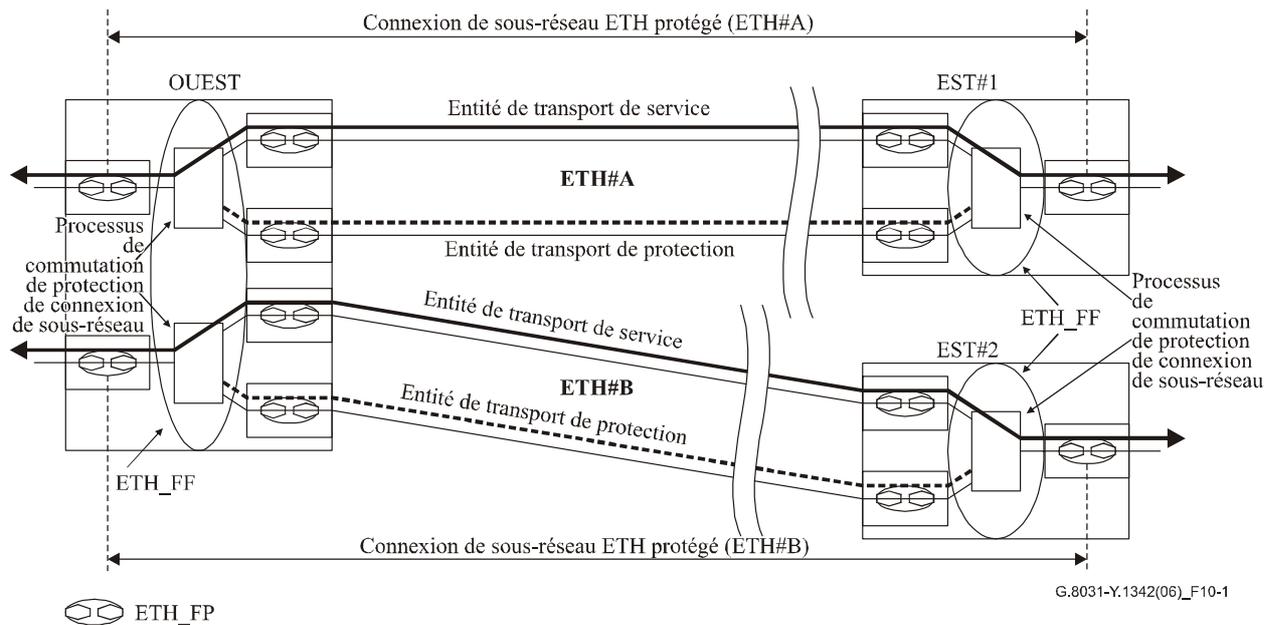


Figure 10-1/G.8031/Y.1342 – Architecture de commutation de protection SNC/S ETH

Le mécanisme de commutation de protection nécessitant la surveillance de l'entité de transport de service et de l'entité de transport de protection, il faut activer des points MEP pour surveiller ces entités. A cette fin, on échange sur chacune d'elles des messages CCM définis dans la Rec. UIT-T Y.1731 (voir la Figure 10-2 ci-après).

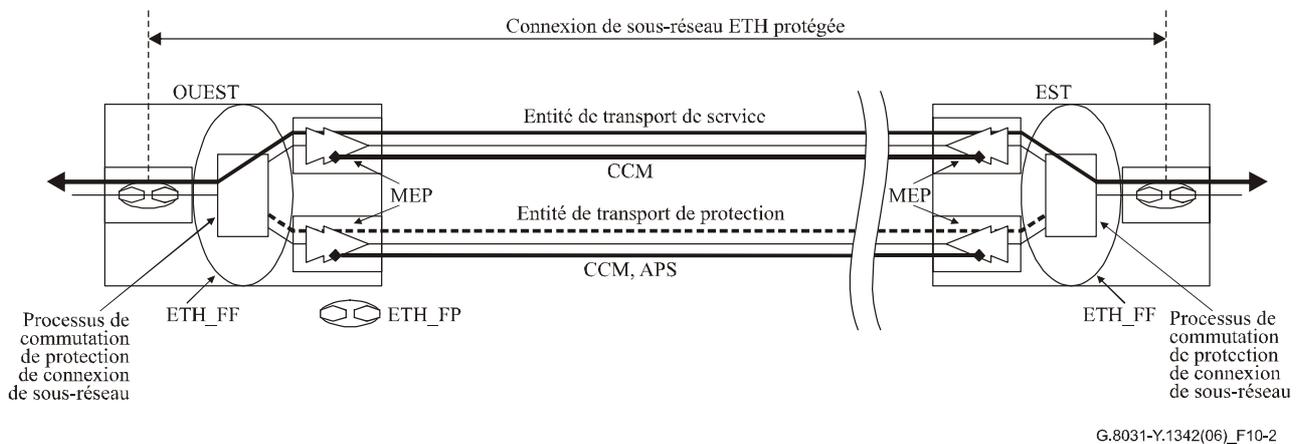


Figure 10-2/G.8031/Y.1342 – Points MEP dans l'architecture de commutation de protection SNC/S ETH

Le processus de commutation de protection requiert également une communication APS pour coordonner son comportement de commutation avec l'autre extrémité du domaine protégé si l'architecture de commutation de protection n'est pas de type unidirectionnel 1+1. Des unités PDU APS sont transmises et reçues entre la paire considérée de points MEP dans l'entité de transport de protection dans laquelle des messages CCM sont transmis à des fins de surveillance.

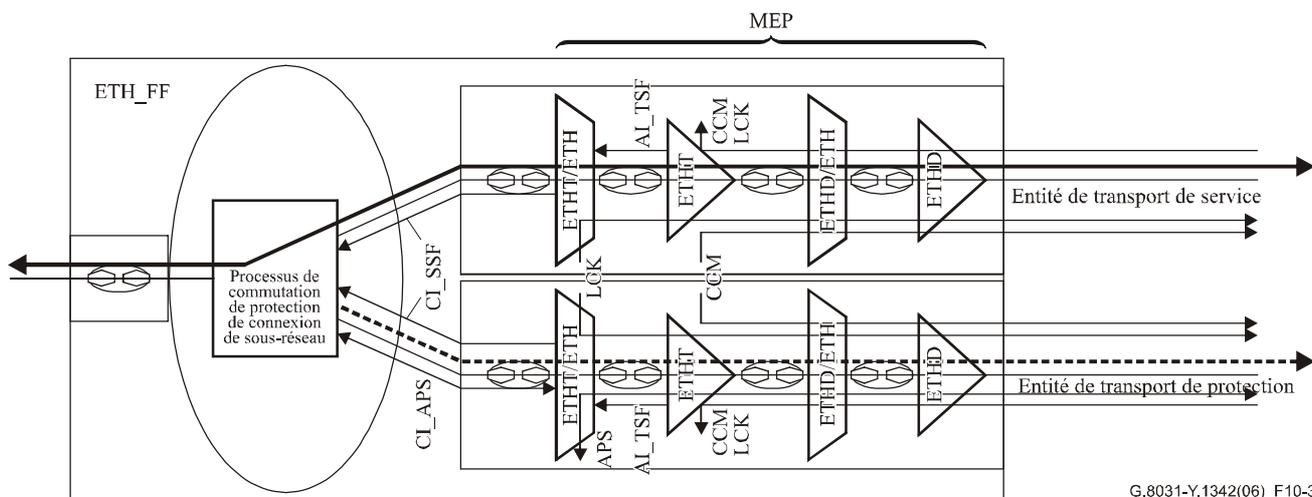
Les informations APS et la situation de défaut, dont la terminaison/détection est assurée par la fonction puits MEP, peuvent servir d'entrée au processus de commutation de protection comme le montre la Figure 10-3 ci-après.

Un point MEP détectant une anomalie qui contribue à une situation de défaut SF signalera au processus de commutation de protection qu'une situation de défaillance a été détectée. La terminaison des messages CCM et des signaux LCK (définis dans la Rec. UIT-T Y.1731) est assurée par la fonction atomique ETH_FT. Si cette fonction détecte une situation de défaillance, un signal AI_TSF est envoyé à la fonction puits d'adaptation ETH(x) à ETH (ETH(x)/ETH_A_Sk) qui génère ensuite un signal CI_SSF. La fonction d'adaptation ETH(x)/ETH utilise ce signal CI_SSF pour notifier au processus de protection de connexion de sous-réseau ETH la situation de défaillance du signal.

La fonction ETH(x)/ETH_A_Sk assure la terminaison des unités PDU APS au niveau du point MEP. Elle extrait ensuite les informations spécifiques APS des unités PDU APS reçus puis les transfère au processus de protection de connexion de sous-réseau ETH en tant qu'informations caractéristiques APS (CI_APS).

Le processus de commutation de protection détermine le nouvel état de commutation après avoir reçu un signal CI_SSF ou CI_APS puis détermine le point ETH_FP de sortie spécifique au travers duquel les informations ETH_CI protégées sont transférées si nécessaire.

Il convient de noter que, pour les deux entités de transport (de service et de protection), l'état administratif de la fonction d'adaptation ETH(x)/ETH ne doit pas être verrouillé.



G.8031-Y.1342(06)_F10-3

Figure 10-3/G.8031/Y.1342 – Comportements des deux points MEP et du processus de commutation de protection de sous-réseau dans l'architecture de commutation de protection SNC/S ETH

La protection SNC/S n'est pas limitée aux connexions de sous-réseau; il est également possible d'étendre ce mécanisme de protection pour prendre en charge une seule connexion de liaison ou plusieurs connexions de réseau.

10.6.1 Commutation de protection bidirectionnelle 1+1

La Figure 10-4 décrit l'architecture de commutation de protection linéaire bidirectionnelle 1+1. Le trafic ETH_CI protégé est ponté en permanence à la fois vers l'entité de transport de service et vers l'entité de transport de protection. Sur cette figure, le trafic est représenté comme étant reçu via la fonction ETH_FF en provenance de l'entité de service uniquement. La Figure 10-5 décrit le cas d'une commutation de protection due à une situation de défaillance du signal dans l'entité de transport de service. Il convient de noter qu'il y a commutation pour les deux sens même s'il s'agit d'un défaut unidirectionnel, d'où la nécessité d'utiliser le protocole de coordination APS.

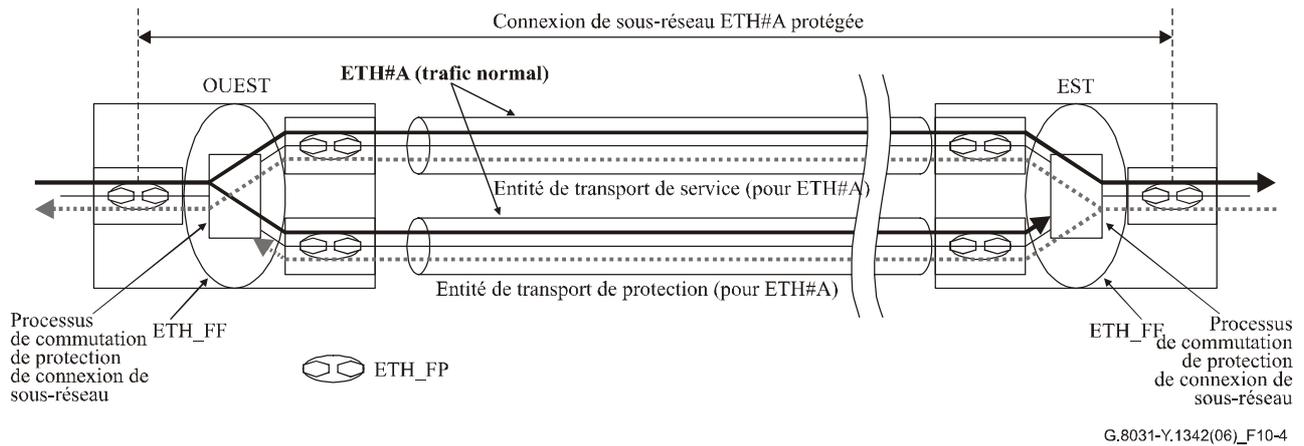


Figure 10-4/G.8031/Y.1342 – Architecture de commutation de protection bidirectionnelle 1+1

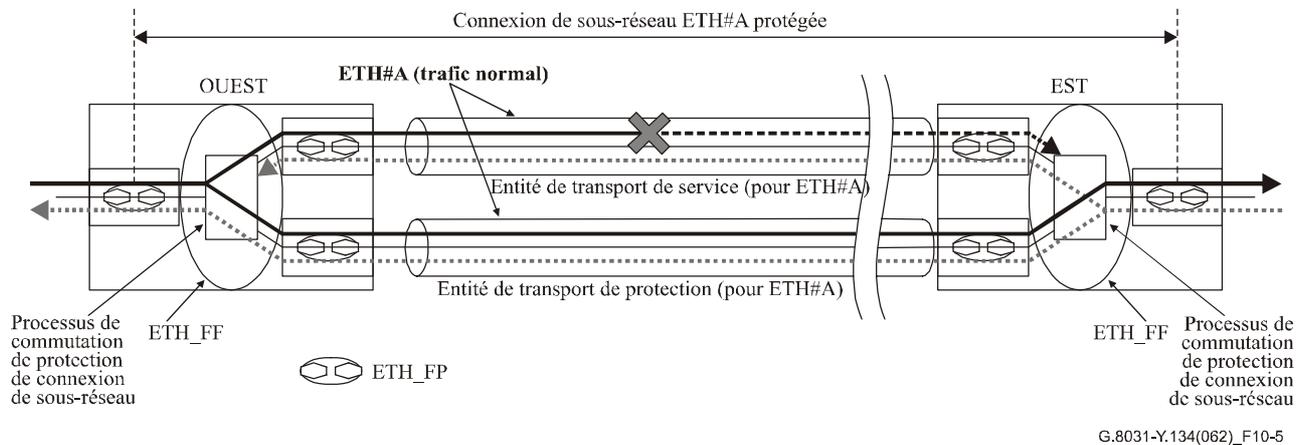


Figure 10-5/G.8031/Y.1342 – Architecture de commutation de protection bidirectionnelle 1+1 – Situation de défaillance du signal pour l'entité de transport

10.6.2 Commutation de protection unidirectionnelle 1+1

La Figure 10-6 décrit l'architecture de commutation de protection linéaire unidirectionnelle 1+1. Le trafic ETH_CI protégé est ponté en permanence à la fois vers l'entité de transport de service et vers l'entité de transport de protection. Sur cette figure, le trafic est représenté comme étant reçu via la fonction ETH_FF en provenance de l'entité de service uniquement, et ce dans les deux sens. La Figure 10-7 décrit le cas d'une commutation de protection due à une situation de défaillance du signal dans l'entité de transport de service dans le sens ouest-est. Le trafic normal dans le sens est-ouest continue d'être reçu via l'entité de transport de service. En commutation de protection unidirectionnelle, chaque sens est commuté de façon indépendante. Le fonctionnement d'un sélecteur au niveau puits du domaine protégé n'est fondé que sur des informations locales. L'utilisation du protocole de coordination APS n'est donc pas nécessaire.

La Figure 10-8 décrit le cas où des situations de défaillance du signal apparaissent dans l'entité de transport de service dans le sens ouest-est et dans l'entité de transport de protection dans le sens est-ouest. La commutation de protection unidirectionnelle permet de faire face à ce type de scénario à deux défauts, contrairement à la commutation de protection bidirectionnelle.

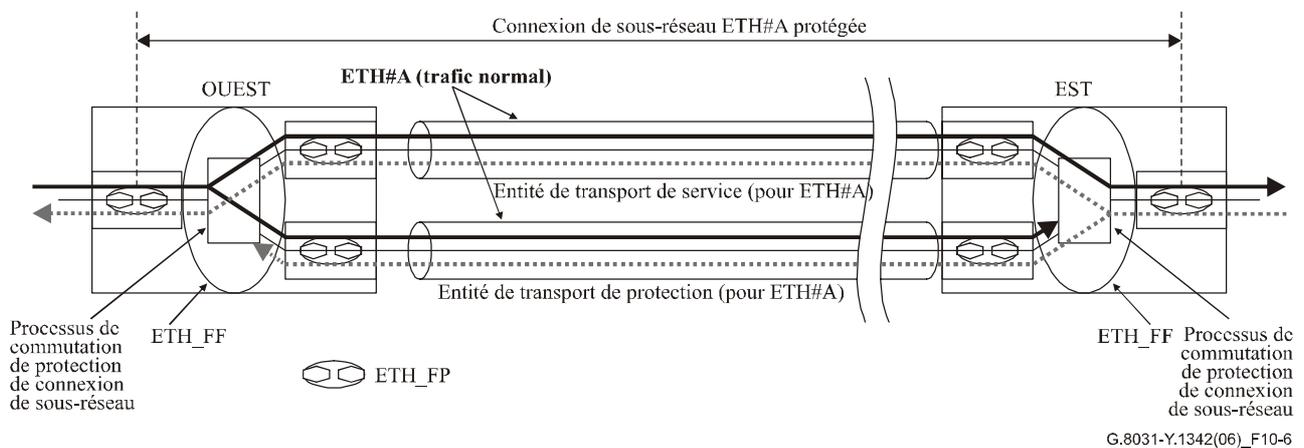


Figure 10-6/G.8031/Y.1342 – Architecture de commutation de protection unidirectionnelle 1+1

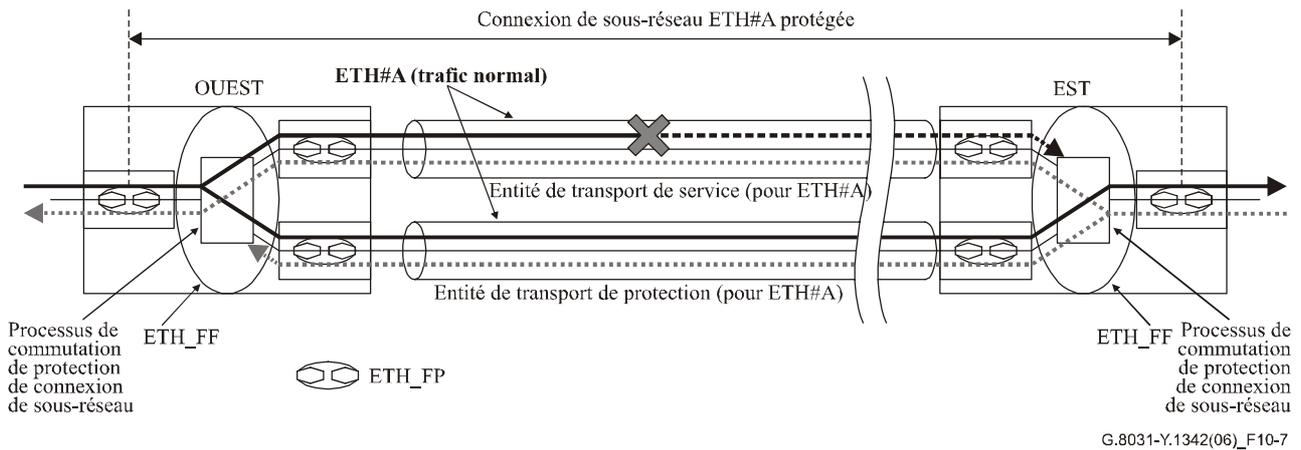


Figure 10-7/G.8031/Y.1342 – Architecture de commutation de protection unidirectionnelle 1+1 – Situation de défaillance du signal dans l'entité de transport de service dans le sens ouest-est

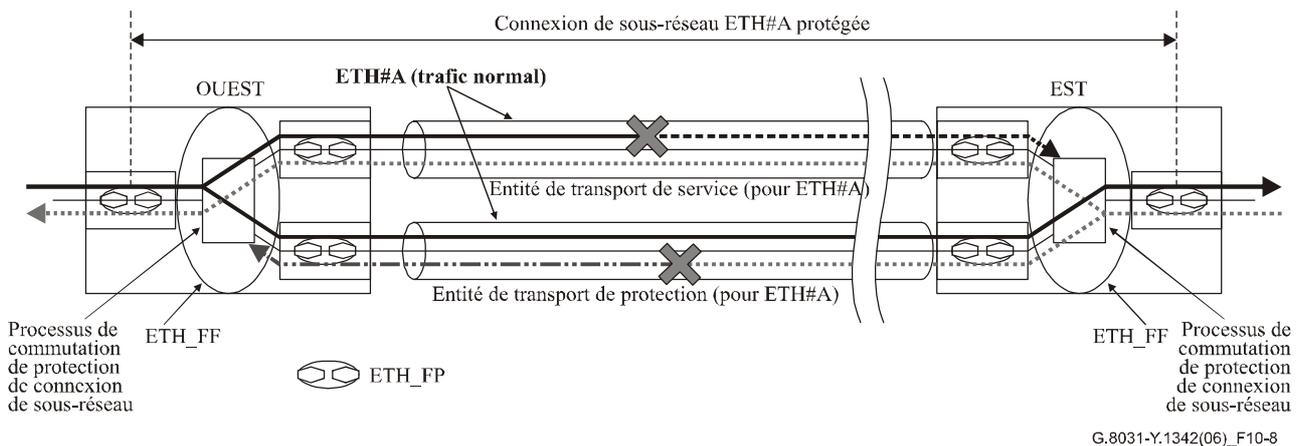


Figure 10-8/G.8031/Y.1342 – Architecture de commutation de protection unidirectionnelle 1+1 – Situations de défaillance du signal dans les deux sens

10.6.3 Commutation de protection 1:1

La Figure 10-9 décrit l'architecture de commutation de protection linéaire 1:1, où le trafic normal (ETH#A) est transmis via l'entité de transport de service. Même si les entités de transport de protection de service et de protection associées au trafic ETH#A peuvent être utilisées par tout autre trafic ETH, le processus de commutation de protection de connexion de sous-réseau ETH ne détermine le point ETH_FP de sortie spécifique vers lequel les informations ETH_CI protégées du trafic ETH#A sont transférées que si la commutation de protection n'est établie que pour le trafic ETH#A.

La Figure 10-10 décrit le cas d'une commutation de protection due à une situation de défaillance du signal dans l'entité de transport de service. Au niveau du nœud source, le trafic normal (ETH#A) est transmis à l'entité de transport de protection. Au niveau du nœud puits, le trafic normal (ETH#A) est reçu en provenance de l'entité de transport de protection. Durant l'opération de commutation de protection, il est possible qu'apparaisse une discordance transitoire entre les positions pont/sélecteur aux deux extrémités du domaine protégé est possible. Toutefois, il est impossible d'avoir une erreur

de connexion entre les informations ETH_CI du trafic ETH#A et d'autres informations ETH_CI, car le trafic est toujours transmis correctement à travers la fonction ETH_FF, sur la base de la valeur de l'identificateur VID. On notera que pour réaliser ce comportement de transmission, il faut configurer des identificateurs VID différents dans l'entité de transport de protection pour le trafic ETH#A protégé et pour le trafic ETH non protégé.

Du fait de la transmission du trafic en fonction de l'identificateur VID dans la fonction ETH_FF, il n'y a jamais d'erreur de connexion de trafic en architecture 1:1. La fonctionnalité de protocole de commutation de protection s'en trouve grandement facilitée: on peut utiliser un protocole à 1 phase, un seul échange d'informations étant requis entre les deux extrémités pour réaliser une commutation bidirectionnelle.

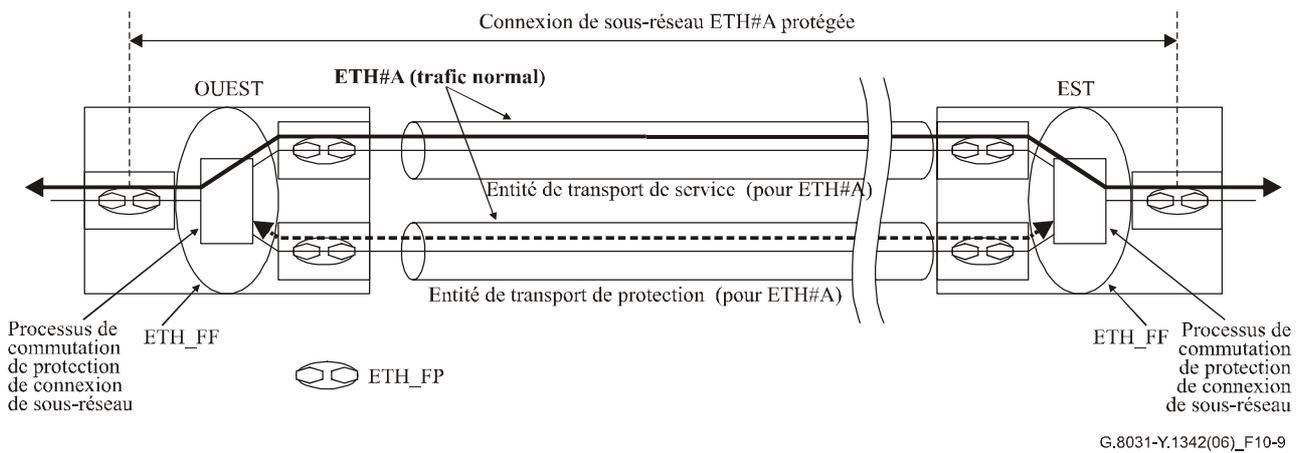


Figure 10-9/G.8031/Y.1342 – Architecture de commutation de protection 1:1

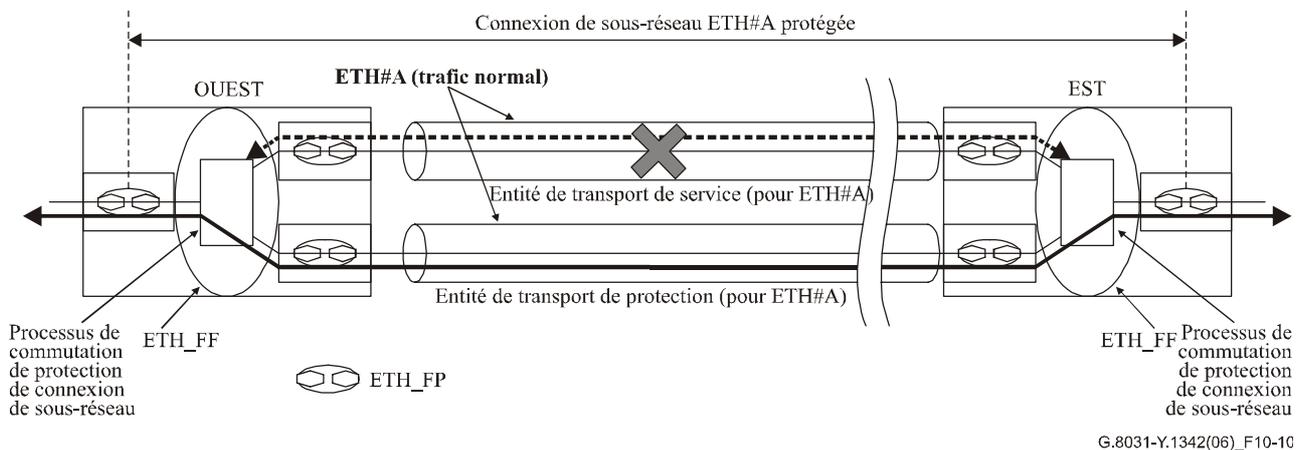


Figure 10-10/G.8031/Y.1342 – Architecture de commutation de protection 1:1 – Situation de défaillance du signal dans l'entité de transport de service

11 Protocole APS

11.1 Format du protocole APS

Les informations APS sont acheminées dans l'unité PDU APS appartenant à une séquence d'unités PDU OAM Ethernet. Les formats des unités PDU OAM pour les différents types d'exploitation

OAM Ethernet sont définis dans la Rec. UIT-T Y.1731. Les informations spécifiques APS sont transmises dans des champs spécifiques de l'unité PDU APS. L'unité PDU APS est identifiée par une valeur OpCode OAM Ethernet spécifique. Dans la présente version de la Recommandation, 4 octets de l'unité PDU APS sont utilisés pour acheminer des informations spécifiques APS (voir la Figure 11-1 ci-dessous). En outre, il convient de noter que dans la présente version de la présente Recommandation, le champ décalage TLV doit être mis à 0x04.

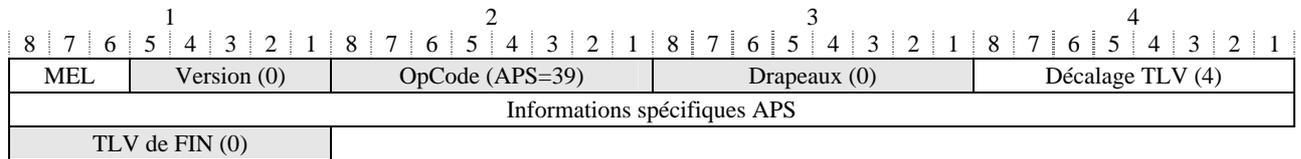


Figure 11-1/G.8031/Y.1342 – Format d'unité PDU APS

Pour les autres champs (version, OpCode, drapeaux et TLV de FIN), les valeurs suivantes doivent être utilisées conformément à la Rec. UIT-T Y.1731:

- **Version:** 0x00
- **OpCode:** 0x39
- **Drapeaux:** 0x00
- **TLV DE FIN:** 0x00

Le niveau MEG de l'unité PDU APS est inséré dans le champ MEL.

Le format des informations spécifiques APS dans chaque unité PDU APS est défini sur la Figure 11-2:

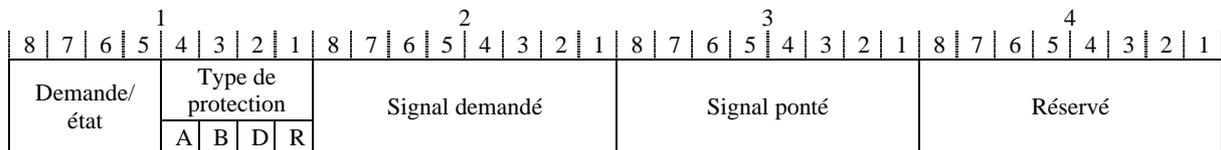


Figure 11-2/G.8031/Y.1342 – Format des informations spécifiques APS

Le Tableau 11-1 décrit le code et les valeurs associés aux informations spécifiques APS.

Tableau 11-1/G.8031/Y.1342 – Code et valeurs de champ associés aux informations spécifiques APS

Demande/Etat	1111	Verrouillage de la protection (LO)	Priorité
	1110	Défaillance du signal pour l'entité de protection (SF-P)	La plus élevée
	1101	Commutation forcée (FS)	
	1011	Défaillance du signal pour l'entité de service (SF)	
	1001	Dégradation du signal (SD) (Note 1)	
	0111	Commutation manuelle (MS)	
	0101	Attente avant rétablissement (WTR)	
	0100	Test (EXER)	
	0010	Demande d'inversion (RR) (Note 2)	
	0001	Ne pas inverser (DNR)	
	0000	Pas de demande (NR)	La moins élevée
	Autres valeurs	Réservées pour une future normalisation internationale	
Type de protection	A	0	Pas de canal APS
		1	Canal APS
	B	0	1+1 (pont permanent)
		1	1:1 (pas de pont permanent)
	D	0	Commutation unidirectionnelle
		1	Commutation bidirectionnelle
	R	0	Fonctionnement non réversible
		1	Fonctionnement réversible
Signal demandé	0	Signal néant	
	1	Signal de trafic normal	
	2-255	(Réservé pour une utilisation future)	
Signal ponté	0	Signal néant	
	1	Signal de trafic normal	
	2-255	(Réservé pour une utilisation future)	
NOTE 1 – La dégradation SD appelle un complément d'étude.			
NOTE 2 – La demande RR est réservée pour une normalisation future par l'UIT-T.			

Il faut utiliser un protocole APS à une phase pour les architectures de protection décrites au § 10.

11.2 Protocole APS à une phase

11.2.1 Principe d'exploitation

La Figure 11-3 illustre le principe de l'algorithme de commutation de protection linéaire 1+1/1:1. L'algorithme est appliqué dans des éléments de réseau aux deux extrémités du domaine protégé (OUEST et EST). La commutation bidirectionnelle est obtenue en transmettant des demandes de commutation locale à l'extrémité distante via le champ "Demande/Etat" dans le premier octet des informations spécifiques APS (voir la Figure 11-2). Les champs "Signal demandé" et "Signal ponté" dans les deuxième et troisième octets des informations spécifiques APS contiennent des informations d'état sur le pont/sélecteur local; une discordance persistante entre les deux extrémités peut ainsi être détectée et conduit à une alarme.

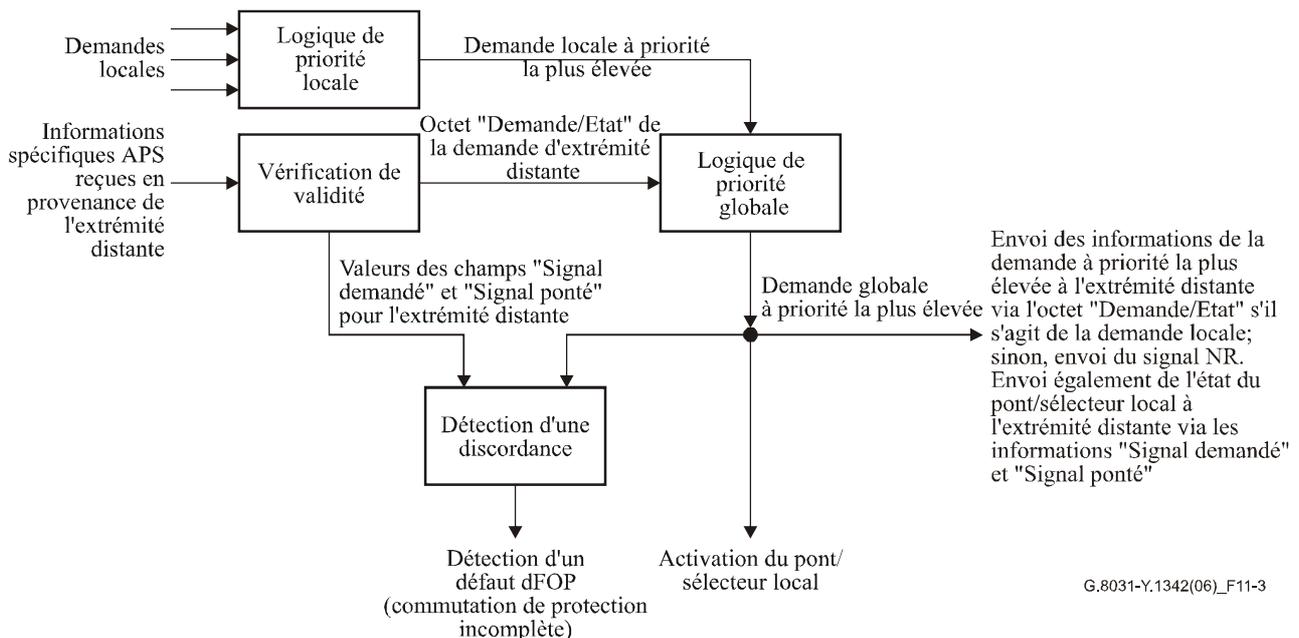


Figure 11-3/G.8031/Y.1342 – Principe de l'algorithme de commutation de protection linéaire 1+1/1:1

On décrit ci-après le détail de l'algorithme (voir la Figure 11-3).

Au niveau de l'élément de réseau local, une ou plusieurs demandes de commutation de protection locales (telles qu'énumérées aux § 9.1 et 9.2) peuvent être actives. La "logique de priorité locale" détermine la demande qui a la priorité la plus élevée, suivant l'ordre des priorités donné dans le Tableau 11-1. Cette demande locale à priorité la plus élevée est transmise à la "logique de priorité globale".

L'élément de réseau local reçoit les informations provenant de l'élément de réseau extrémité distante via les informations spécifiques APS. Les informations spécifiques APS reçues font l'objet d'une vérification de validité (voir le § 11.2.4). Les informations contenues dans le champ "Demande/Etat" reçu (qui indique la demande locale à priorité la plus élevée de l'extrémité distante) sont ensuite transmises à la "logique de priorité globale". Celle-ci compare la demande locale à priorité la plus élevée à la demande figurant dans le champ "Demande/Etat" reçu (conformément à l'ordre des priorités du Tableau 11-1) pour déterminer la demande globale à priorité la plus élevée. Si la demande globale à priorité la plus élevée est la demande

champ "Demande/Etat"; sinon, la valeur "NR" sera indiquée. Cette demande détermine ensuite comme suit la position (ou l'état) du pont/sélecteur de l'élément de réseau local:

- en architecture 1+1, seule la position du sélecteur est commandée. En architecture 1:1, on commande les positions du pont et du sélecteur, qui doivent être les mêmes;
- si la demande globale à priorité la plus élevée est une demande relative à une entité de service, le trafic de service associé est ponté/commuté vers l'entité de protection (le pont/sélecteur associé de l'élément de réseau local sélectionne l'entité de protection). Une demande de commutation relative à une entité de service est une demande de commutation de l'entité de service vers l'entité de protection.

L'état du pont/sélecteur est transmis à l'extrémité distante via les champs "signal demandé" et "Signal ponté" (conformément au code décrit dans le Tableau 11-1). Il est également comparé à l'état du pont/sélecteur de l'extrémité distante tel qu'indiqué par les champs "Signal demandé" et "Signal ponté" reçus. Il convient de noter que l'algorithme de commutation de protection linéaire est immédiatement lancé chaque fois qu'un des signaux d'entrée (voir la Figure 11-3) est modifié, c'est-à-dire lorsque la position du pont/sélecteur local change ou lorsque des informations spécifiques APS différentes sont reçues en provenance de l'extrémité distante. Les actions résultantes de l'algorithme sont également immédiatement lancées (changement de la position du pont/sélecteur (le cas échéant), transmission de nouvelles informations spécifiques APS (le cas échéant) ou détection d'un défaut dFOP si la commutation de protection n'est pas réalisée dans un délai spécifié au § 11.15.

11.2.2 Mode réversible

En fonctionnement réversible, lorsque le trafic de service est reçu via l'entité de protection et que les demandes de commutation de protection locales (voir la Figure 11-3) précédemment actives sont devenues inactives, on passe à l'état local "Attente avant rétablissement". Puisqu'il correspond à présent à la demande à priorité locale la plus élevée, cet état est indiqué dans le champ "Demande/Etat" transmis et maintient la commutation.

Généralement cet état s'achève et se termine et est remplacé par l'état "Pas de demande" à l'expiration du temporisateur d'attente avant rétablissement. Celui-ci est désactivé plus tôt en cas de préemption de l'état "Attente avant rétablissement" par une demande locale à priorité plus élevée.

Il convient de noter que seules les demandes locales sont prises en compte pour décider du passage à l'état "Attente avant rétablissement". Une commutation vers l'entité de protection peut être maintenue par un état local d'attente avant rétablissement ou une demande distante (attente avant rétablissement ou autre) reçue via les informations "Demande/Etat". Par conséquent, lorsqu'une défaillance bidirectionnelle s'est produite dans une entité de service et qu'une réparation a ensuite lieu, la réversion bidirectionnelle vers l'entité de service ne se produit pas avant l'expiration des deux temporisateurs d'attente avant rétablissement présents aux deux extrémités.

11.2.3 Mode non réversible

En fonctionnement non réversible, lorsque le trafic de service est transmis via l'entité de protection et que les demandes de commutation de protection locales (voir la Figure 11-3) précédemment actives sont devenues inactives, on passe à l'état local "Ne pas inverser". Puisqu'il correspond à présent à la demande à priorité locale la plus élevée, cet état est indiqué dans le champ "Demande/Etat" transmis et maintient la commutation, ce qui empêche ainsi en mode non réversible une réversion vers la position du pont/sélecteur libérée en l'absence de demande.

11.2.4 Transmission et acceptation du protocole APS

Les unités de trafic qui acheminent des unités PDU APS sont appelées trames APS. Les trames APS sont acheminées uniquement via l'entité de transport de protection; elles sont insérées par l'extrémité de tête du domaine protégé et sont extraites par l'extrémité de queue.

Une nouvelle trame APS doit être immédiatement transmise en cas de modification de l'état transmis (voir la Figure 11-3).

Les trois premières trames APS devraient être transmises aussi rapidement que possible après modification de l'état du point d'extrémité de protection de telle sorte que la commutation de protection rapide soit possible même si une ou deux trames APS sont perdues ou détériorées. En cas de commutation de protection rapide d'une durée de 50 ms, il est souhaitable d'avoir entre les trois premières trames APS un intervalle de 3,3 ms, c'est-à-dire le même intervalle que celui utilisé pour les trames CCM en détection de défaut rapide. Les trames APS qui suivent les trois premières devraient être transmises avec un intervalle de 5 secondes.

Si aucune information spécifique APS valable n'est reçue, les dernières informations reçues valables restent applicables. Si une situation de défaillance du signal est détectée dans l'entité de transport de protection, les informations spécifiques APS reçues devraient être évaluées.

S'il reçoit des informations spécifiques APS en provenance de l'entité de service, un point d'extrémité de protection devrait les ignorer et devrait détecter le défaut de défaillance de protocole concernant l'élément de réseau local (voir le § 11.15).

11.3 Type de demande

Les types de demande susceptibles d'apparaître dans les informations spécifiques APS sont les types "normalisés" généralement pris en charge par la commutation de protection dans les réseaux SONET et SDH. Ces demandes reflètent la situation, la commande ou l'état à priorité la plus élevée. En commutation unidirectionnelle, il s'agit de la valeur de priorité la plus élevée déterminée uniquement par l'extrémité proche. En commutation bidirectionnelle, la demande locale ne sera indiquée que si elle est de priorité égale ou supérieure à toute demande reçue en provenance de l'extrémité distante via la communication APS; sinon, la valeur NR sera indiquée. En protocole APS à une phase, l'extrémité distante ne signalera jamais de demande d'inversion même si la demande de l'extrémité distante a la priorité la plus élevée.

11.4 Type de protection

Les types de protection valables sont les suivants:

000x	1+1 unidirectionnel sans communication APS
100x	1+1 unidirectionnel avec communication APS
101x	1+1 bidirectionnel avec communication APS
111x	1:1 bidirectionnel avec communication APS

Les valeurs sont choisies de telle sorte que la valeur par défaut (tous les bits à zéro) corresponde au seul type de protection qui puisse être appliqué sans communication APS (1+1 unidirectionnel).

On notera que les valeurs 010x, 001x et 011x ne sont pas valables puisque les modes 1:1 et bidirectionnel nécessitent une communication APS.

En cas de discordance concernant le bit "B", le sélecteur est libéré car les modes 1:1 et 1+1 sont incompatibles. Il en résultera l'apparition d'un défaut.

S'il y a concordance entre les valeurs du bit "B", les considérations ci-après s'appliquent:

En cas de discordance concernant le bit "A", le côté qui attend une communication APS reviendra à une communication unidirectionnelle 1+1 sans communication APS.

En cas de discordance concernant le bit "D", le côté bidirectionnel reviendra à une communication unidirectionnelle.

En cas de discordance concernant le bit "R", un côté supprimera la commutation pour passer à l'état "WTR" tandis que l'autre côté passera à l'état "DNR". Les deux côtés interfonctionneront et le trafic sera protégé.

11.5 Signal demandé

Ce champ désigne le signal que l'extrémité proche demande d'acheminer dans le conduit de protection. Pour une demande NR, il s'agit du signal néant lorsque l'extrémité distante ne pont pas le signal de trafic normal vers l'extrémité de protection. Lorsque l'extrémité distante pont le signal de trafic normal vers l'entité de protection, le signal demandé est le signal de trafic normal pour une demande NR; pour une demande LO, il ne peut s'agir que du signal néant. Pour une demande Test, il peut s'agir du signal néant lorsqu'une demande Test remplace une demande NR ou du signal de trafic normal lorsqu'une demande Test remplace une demande DNR. En cas de demande SF (ou SD le cas échéant), il s'agira du signal de trafic normal, ou du signal néant pour indiquer que la protection est défaillante ou dégradée. Pour toutes les autres demandes, il s'agira du signal de trafic normal dont on a demandé l'acheminement dans l'entité de transport de protection.

11.6 Signal ponté

Ce champ désigne le signal qui est ponté vers le conduit de protection. En protection 1+1, il devrait toujours s'agir du signal de trafic normal, ce qui reflète précisément l'utilisation d'un pont permanent. En protection 1:1, ce champ désigne le signal qui est effectivement ponté vers l'entité de protection (le signal néant ou le signal de trafic normal). Il s'agira généralement du pont demandé par l'extrémité distante.

11.7 Commande du pont

En architecture 1+1, le signal de trafic normal est en permanence ponté vers l'entité de protection. La valeur "Signal de trafic normal" sera toujours indiquée dans le champ "Signal ponté" des informations APS.

En architecture 1:1, le pont sera réglé à la valeur indiquée par le champ "Signal demandé" des informations APS entrantes. Une fois le pont établi, le réglage du pont sera indiqué dans le champ "Signal ponté" des informations APS sortantes.

11.8 Commande du sélecteur

En architecture unidirectionnelle 1+1 (avec ou sans communication APS), le réglage du sélecteur se fait entièrement conformément à la demande locale à priorité la plus élevée. Il s'agit d'une commutation à une seule phase.

En architecture bidirectionnelle 1+1, le signal de trafic normal est sélectionné dans l'entité de protection lorsque le champ "Signal demandé" sortant a pour valeur "Signal de trafic normal".

En architecture bidirectionnelle 1:1, le signal de trafic normal est sélectionné dans l'entité de protection lorsque le nombre correspondant apparaît dans le champ "Signal demandé".

11.9 Défaillance du signal dans l'entité de transport de protection

La défaillance du signal dans l'entité de transport de protection a une priorité plus élevée que tout défaut qui entraînerait la sélection d'un signal de trafic normal dans l'entité de protection. En cas d'utilisation d'un signal APS, un défaut SF-P dans l'entité de transport de protection (dans laquelle le signal APS est acheminé) a une priorité plus élevée qu'une demande de commutation forcée: en situations de défaillance, l'état de verrouillage doit rester actif.

11.10 Demandes d'égale priorité

En général, lorsqu'une commutation a été effectuée suite à une demande, elle n'est pas supplantée par une autre demande de même priorité (fonctionnement du type "premier arrivé, premier servi"). Deux demandes d'égale priorité provenant des deux côtés d'un groupe de protection bidirectionnelle sont chacune considérées comme valables.

11.11 Acceptation et rétention de commande

Les commandes CLEAR, LO, FS, MS et EXER sont acceptées ou rejetées en fonction des commandes précédentes, de l'état des entités de service et de protection dans le groupe de protection et (en communication bidirectionnelle uniquement) des informations APS reçues.

La commande CLEAR n'est valable que si une commande LO, FS, MS ou EXER d'extrémité proche est appliquée ou si un état WTR est présent à l'extrémité proche; sinon, elle est rejetée. Elle supprimera la commande d'extrémité proche ou l'état WTR, permettant l'activation de la demande (en commutation bidirectionnelle) ou de la demande APS à priorité immédiatement inférieure.

Les autres commandes sont rejetées sauf si elles sont de priorité supérieure à la commande, à la situation ou (en commutation bidirectionnelle) à la demande APS existante précédemment. Si une nouvelle commande est acceptée, toute commande précédente à priorité inférieure ayant été supplantée est "oubliée". Si une commande à priorité supérieure supprime une situation ou (en commutation bidirectionnelle) une demande APS à priorité inférieure, cette ancienne demande sera réactivée si elle existe toujours au moment où la commande est supprimée.

Si une commande est supplantée par une situation ou (en commutation bidirectionnelle) par une demande APS, cette commande est "oubliée".

11.12 Temporisateur d'attente de protection

Un temporisateur d'attente de protection peut être nécessaire pour coordonner le rythme des commutations de protection au niveau de différentes couches ou à travers des domaines protégés en cascade. L'objectif est soit de permettre à une commutation de protection de couche serveur de pouvoir régler le problème posé avant la commutation au niveau d'une couche serveur, soit de permettre à un domaine protégé amont de commuter avant un domaine aval (par exemple pour permettre à un anneau amont de commuter avant l'anneau aval dans une configuration d'interconnexion à double nœud de telle sorte que la commutation et la défaillance se produisent dans le même anneau).

Chaque groupe de protection devrait disposer d'un temporisateur d'attente de protection configurable. Les valeurs de temporisation suggérées varient entre 0 et 10 secondes par pas de 100 ms (précision de ± 5 ms).

Le temporisateur fonctionne selon la méthode à "double lecture en mémoire" spécifiée dans les normes SDH. Plus précisément, lorsqu'un défaut nouveau ou plus grave apparaît (nouvel état SF (ou SD, le cas échéant), cet événement ne sera pas immédiatement signalé à la commutation de protection si la valeur du temporisateur d'attente de protection configurée n'est pas égale à zéro. Le temporisateur sera en revanche activé. A l'expiration de la temporisation, on vérifiera s'il existe encore un défaut sur le chemin ayant activé le temporisateur. Dans l'affirmative, ce défaut sera signalé à la commutation de protection. Il peut être différent de celui qui a entraîné l'activation du temporisateur.

11.13 Temporisateur d'attente avant rétablissement

En fonctionnement réversible, il faut, pour éviter le recours fréquent à la commutation de protection en raison d'un défaut intermittent, qu'une entité de transport de service défaillante devienne exempte de dérangement. Une fois que l'entité de transport de service défaillante répond à ce critère, une durée fixe doit s'écouler avant qu'elle soit à nouveau utilisée par un signal de trafic normal. Cette durée, appelée temps d'attente avant rétablissement (WTR, *wait-to-restore*), doit être configurée par l'opérateur à une valeur comprise (par pas de 1 minute) entre 5 et 12 minutes, 5 minutes étant la valeur par défaut. Une situation SF (ou SD, le cas échéant) supplantera l'état WTR.

Lorsque, en fonctionnement réversible, la protection n'est plus demandée, c'est-à-dire lorsque l'entité de transport de service défaillante n'est plus dans la situation SF (ou SD, le cas échéant) (en supposant qu'il n'y a pas d'autres entités de transport demandeuses), un état local d'attente avant rétablissement est activé. Devenant l'état à priorité la plus élevée, il est indiqué dans le signal APS (le cas échéant) et maintient, dans l'entité de transport de protection, le signal de trafic normal issu de l'entité de transport de service précédemment défectueuse. Cet état doit normalement arriver à expiration et devenir un signal néant "Pas de demande". Le temporisateur d'attente avant rétablissement est désactivé plus tôt si une demande à priorité plus élevée préempte cet état.

11.14 Commande test

La commande test permet de vérifier si la communication APS fonctionne correctement. Elle est de priorité inférieure à toute demande de commutation "réelle". Elle n'est valable qu'en commutation bidirectionnelle, car il faut attendre une réponse pour réaliser un test significatif.

La commande de test doit être émise avec les mêmes numéros de signal demandé et de signal ponté que ceux qui figurent dans la demande NR ou DNR qu'elle remplace. En protocole APS à 1 phase, la réponse valable doit être un message NR accompagné des numéros de signal demandé et de signal ponté correspondant. La réponse normalisée à une demande DNR devrait être de type DNR plutôt que NR. Lorsque la commande de test est supprimée, elle doit être remplacée par un message NR si le numéro de signal demandé vaut 0 ou par un message DNR si ce numéro vaut 1 (signal de trafic normal).

11.15 Défauts de défaillance de protocole

Les critères d'entrée et de sortie associés aux défauts de défaillance de protocole (dFOP, *failure of protocol defect*) du protocole APS défini dans la présente Recommandation sont décrits ci-après dans le Tableau 11-2.

Tableau 11-2/G.8031/Y.1342 – Critères d'entrée/sortie associés aux défauts dFOP

Configuration totalement incompatible (discordance concernant le bit "B")	
Critère d'entrée	Réception de trois trames APS avec des valeurs de bit "B" incompatibles durant la période de 22,5 secondes.
Critère de sortie	Réception de la première trame APS avec une valeur de bit "B" compatible.
Commutation de protection incomplète	
Critère d'entrée	S'il n'y a pas concordance entre le "Signal demandé" émis et le "Signal ponté" reçu pendant une période d'au moins 50 ms.
Critère de sortie	Réception de la première trame APS indiquant une valeur de "Signal ponté" identique à la valeur de "Signal demandé" émise.
Discordance entre les configurations de service/de protection	
Critère d'entrée	Réception de trois trames APS provenant de l'entité de transport de service pendant une période de 22,5 secondes.
Critère de sortie	Si aucune trame APS n'est reçue en provenance de l'entité de transport de service pendant une période de 22,5 secondes.
NOTE – 22,5 secondes est une période qui permet de recevoir trois trames APS même si deux trames APS sont perdues.	

Si une demande inconnue ou une demande portant sur un numéro de signal non valable est reçue, elle est ignorée.

Annexe A

Tableaux de transitions d'états pour la commutation de protection

Dans la présente annexe les tableaux de transitions d'états associés aux configurations de commutation de protection suivantes sont décrits:

- 1:1 bidirectionnelle (mode réversible, mode non réversible)
- 1+1 bidirectionnelle (mode réversible, mode non réversible)
- 1+1 unidirectionnelle (mode réversible, mode non réversible)

A.1 Transitions d'états associées à la commutation bidirectionnelle 1:1 en mode réversible

A.1.1 Demandes locales

Le Tableau A.1 décrit les transitions d'états provoquées par une demande locale pour la commutation de protection 1:1 en mode réversible.

Tableau A.1/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1:1, bidirectionnelle, mode réversible)

Etat		APS signalé	Demande locale									
			a	b	c	d	e	f	g	h	i	j
			Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	N/R [r/b=néant]	→C	→D	→E ^{a)}	Sans objet	→F	Sans objet	→G	O	→I	Sans objet
B	Pas de demande Entité de service/ en réserve Entité de protection/active	N/R [r/b=normal]	→C	→D	(→B) ^{b)} ou →E	O	→F	Sans objet	→G	O	O	Sans objet
C	Verrouillage Entité de service/ active Entité de protection/ en réserve	LO [r/b=néant]	O	O	O	O	O	O	O	→A ou →E ^{c)} →F ^{d)}	O	Sans objet
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→C	O	O	O	→F	Sans objet	O	→A ou →E ^{c)}	O	Sans objet
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→C	→D	Sans objet	→H	→F	Sans objet	O	O	O	Sans objet
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant]	→C	O	O	O	Sans objet	→A	O	O	O	Sans objet

Tableau A.1/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1:1, bidirectionnelle, mode réversible)

Etat	APS signalé	Demande locale										
		a	b	c	d	e	f	g	h	i	j	
		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR	
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	O	→A	O	Sans objet
H	Attente avant rétablissement Entité de service/ en réserve Entité de protection/ active	WTR [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→A	O	→A
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→A	O	Sans objet

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.

NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.

NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.

a) Il transite vers l'état E s'il y a encore défaillance du signal après expiration du temporisateur d'attente de protection.

b) Si l'état FS est indiqué dans le message APS reçu en provenance de l'extrémité distante.

c) Si l'état SF est réactivé.

d) Si l'état SF-P est réactivé.

A.1.2 Demandes d'extrémité distante

Le Tableau A.2 décrit les transitions d'états provoquées par une demande d'extrémité distante reçue via le protocole APS pour la commutation de protection bidirectionnelle 1:1 en mode réversible.

Tableau A.2/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante (1:1, bidirectionnelle, mode réversible)

Etat	APS signalé	Demande d'extrémité distante reçue									
		k	l	m	n	o	p	q	r	s	
		LO [r/b=néant]	SF-P [r/b=néant]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=néant]	NR [r/b=néant]	NR [r/b=normal]	
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	NR [r/b=néant]	(→A)	(→A)	→B	→B	→B	Sans objet	(→A)	(→A) ou →E ^{a)} ou →F ^{b)}	(→A)
B	Pas de demande Entité de service/ en réserve Entité de protection/ active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	(→B)	Sans objet	→A ou →E ^{a)}	Sans objet
C	Verrouillage Entité de service/ active Entité de protection/ en réserve	LO [r/b=néant]	(→C)	O	O	O	O	O	O	O	O
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O

**Tableau A.2/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante
(1:1, bidirectionnelle, mode réversible)**

Etat	APS signalé	Demande d'extrémité distante reçue									
		k	l	m	n	o	p	q	r	s	
		LO [r/b=néant]	SF-P [r/b=néant]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=néant]	NR [r/b=néant]	NR [r/b=normal]	
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant]	→A	(→F)	O	O	O	O	O	O	O
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O
H	Attente avant rétablissement Entité de service/ en réserve Entité de protection/ active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	Sans objet	O
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant]	→A	→A	→B	→B	→B	Sans objet	(→I)	O	Sans objet

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.
 NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.
 NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.
 a) Si l'état SF est réactivé.
 b) Si l'état SF-P est réactivé.

A.2 Transitions d'états associées à la commutation bidirectionnelle 1:1 en mode non réversible

A.2.1 Demandes locales

Le Tableau A.3 décrit les transitions d'états provoquées par une demande locale pour une commutation de protection bidirectionnelle 1:1 en mode non réversible.

Tableau A.3/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1:1, bidirectionnelle, mode non réversible)

Etat		APS signalé	Demande locale								
			a	b	c	d	e	f	g	h	i
			Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	NR [r/b=néant]	→C	→D	→E ^{a)}	Sans objet	→F	Sans objet	→G	O	→I
B	Pas de demande Entité de service/ en réserve Entité de protection/ active	NR [r/b=normal]	→C	→D	(→B) ^{b)} ou →E	Sans objet	→F	Sans objet	→G	O	O
C	Verrouillage Entité de service/ active Entité de protection/ en réserve	LO [r/b=néant]	O	O	O	O	O	O	O	→A ou →E ^{c)} →F ^{d)}	O
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→C	O	O	O	→F	Sans objet	O	→H ou →E ^{c)}	O
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→C	→D	Sans objet	→H	→F	Sans objet	O	O	O

Tableau A.3/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1:1, bidirectionnelle, mode non réversible)

Etat		APS signalé	Demande locale								
			a	b	c	d	e	f	g	h	i
			Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant]	→C	O	O	O	Sans objet	→A	O	O	O
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	O	→H	O
H	Ne pas inverser Entité de service/ en réserve Entité de protection/ active	DNR [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	O	→J
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→A	O
J	Test Entité de service/ en réserve Entité de protection/ active	EXER [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→H	O

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.

NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.

NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.

a) Il transite vers l'état E s'il y a encore défaillance du signal après expiration du temporisateur d'attente de protection.

b) Si la demande FS est indiquée dans le message APS reçu depuis l'extrémité distante.

c) Si l'état SF est réactivé.

d) Si l'état SF-P est réactivé.

A.2.2 Demandes d'extrémité distante

Le Tableau A.4 décrit les transitions d'états pour une demande d'extrémité distante reçue via le protocole APS pour la commutation de protection bidirectionnelle 1:1 en mode non réversible.

Tableau A.4/G.8031/Y.1342 – Transitions d'états provoquées par des demandes d'extrémité distante (1:1, bidirectionnelle, mode non réversible)

Etat	APS signalé	Demande d'extrémité distante reçue										
		k	l	m	n	o	q	r	s	t	u	
		LO [r/b=néant]	SF-P [r/b=néant]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=néant]	EXER [r/b=normal]	NR [r/b=néant]	NR [r/b=normal]	DNR [r/b=normal]	
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	NR [r/b=néant]	(→A)	(→A)	→B	→B	→B	(→A)	Sans objet	(→A) ou →E ^{a)} ou →F ^{b)}	(→A)	Sans objet
B	Pas de demande Entité de service/ en réserve Entité de protection/active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	Sans objet	(→B)	→A ou →E ^{a)}	Sans objet	(→B)
C	Verrouillage Entité de service/ active Entité de protection/en réserve	LO [r/b=néant]	(→C)	O	O	O	O	O	O	O	O	O
D	Commutation forcée Entité de service/ en réserve Entité de protection/active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O

**Tableau A.4/G.8031/Y.1342 – Transitions d'états provoquées par des demandes d'extrémité distante
(1:1, bidirectionnelle, mode non réversible)**

Etat	APS signalé	Demande d'extrémité distante reçue										
		k	l	m	n	o	q	r	s	t	u	
		LO [r/b=néant]	SF-P [r/b=néant]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=néant]	EXER [r/b=normal]	NR [r/b=néant]	NR [r/b=normal]	DNR [r/b=normal]	
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant]	→A	(→F)	O	O	O	O	O	O	O	O
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	Ne pas inverser Entité de service/ en réserve Entité de protection/ active	DNR [r/b=normal]	→A	→A	→B	→B	→B	Sans objet	(→H)	O	O	(→H)
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant]	→A	→A	→B	→B	→B	(→I)	Sans objet	O	O	Sans objet
J	Test Entité de service/ en réserve Entité de protection/ active	EXER [r/b=normal]	→A	→A	→B	→B	→B	Sans objet	(→J)	O	O	O

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.
NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.
NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.
^{a)} Si l'état SF est réactivé.
^{b)} Si l'état SF-P est réactivé.

A.3 Transitions d'états associées à la commutation bidirectionnelle 1+1 en mode réversible

A.3.1 Demandes locales

Le Tableau A.5 décrit les transitions d'états provoquées par une demande locale pour la commutation de protection bidirectionnelle 1+1 en mode réversible.

Tableau A.5/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, bidirectionnelle, mode réversible)

			Demande locale									
			a	b	c	d	e	f	g	h	i	j
Etat	APS signalé		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR
A	Pas de demande Entité de service/ active	NR [r/b=néant/ normal]	→C	→D	→E ^{a)}	Sans objet	→F	Sans objet	→G	O	→I	Sans objet
B	Pas de demande Entité de service/ en réserve	NR [r/b=normal]	→C	→D	(→B) ^{b)} ou →E	O	→F	Sans objet	→G	O	O	Sans objet
C	Verrouillage Entité de service/ active	LO [r/b=néant/ normal]	O	O	O	O	O	O	O	→A ou →E ^{c)} →F ^{d)}	O	Sans objet

Tableau A.5/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, bidirectionnelle, mode réversible)

Etat	APS signalé	Demande locale										
		a	b	c	d	e	f	g	h	i	j	
		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR	
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→C	O	O	O	→F	Sans objet	O	→A ou →E ^{c)}	O	Sans objet
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→C	→D	Sans objet	→H	→F	Sans objet	O	O	O	Sans objet
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b= néant/ normal]	→C	O	O	O	Sans objet	→A	O	O	O	Sans objet
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	O	→A	O	Sans objet

Tableau A.5/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, bidirectionnelle, mode réversible)

Etat		APS signalé	Demande locale									
			a	b	c	d	e	f	g	h	i	j
			Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR
H	Attente avant rétablissement Entité de service/ en réserve Entité de protection/ active	WTR [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→A	O	→A
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant/ normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→A	O	Sans objet

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.

NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.

NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.

a) Il transite vers l'état E s'il y a encore défaillance du signal après expiration du temporisateur d'attente de protection.

b) Si la demande FS est indiquée dans le message APS reçu en provenance de l'extrémité distante.

c) Si l'état SF est réactivé.

d) Si l'état SF-P est réactivé.

A.3.2 Demandes d'extrémité distante

Le Tableau A.6 décrit les transitions d'états provoquées par une demande d'extrémité distante reçue via le protocole APS pour la commutation de protection bidirectionnelle 1+1 en mode réversible.

Tableau A.6/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante (1+1, bidirectionnelle, mode réversible)

Etat	APS signalé	Demande d'extrémité distante reçue									
		k	l	m	n	o	p	q	r	s	
		LO [r/b=néant/ normal]	SF-P [r/b=néant/ normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=néant/ normal]	NR [r/b=néant/ normal]	NR [r/b=normal]	
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	NR [r/b=néant/ normal]	(→A)	(→A)	→B	→B	→B	Sans objet	(→A)	(→A) ou →E ^{a)} ou →F ^{b)}	(→A)
B	Pas de demande Entité de service/ en réserve Entité de protection/ active	NR [r/b=normal]	→A	(→A)	(→B)	(→B)	(→B)	(→B)	Sans objet	→A ou →E ^{a)}	Sans objet
C	Verrouillage Entité de service/ active Entité de protection/ en réserve	LO [r/b=néant/ normal]	(→C)	O	O	O	O	O	O	O	O
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O

**Tableau A.6/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante
(1+1, bidirectionnelle, mode réversible)**

Etat	APS signalé	Demande d'extrémité distante reçue									
		k	l	m	n	o	p	q	r	s	
		LO [r/b=néant/ normal]	SF-P [r/b=néant/ normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=néant/ normal]	NR [r/b=néant/ normal]	NR [r/b=normal]	
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant/ normal]	→A	(→F)	O	O	O	O	O	O	O
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O
H	Attente avant rétablissement Entité de service/ en réserve Entité de protection/ active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	Sans objet	O
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant/ normal]	→A	→A	→B	→B	→B	Sans objet	(→I)	O	Sans objet
<p>NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré. NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure. NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.</p> <p>a) Si l'état SF est réactivé. b) Si l'état SF-P est réactivé.</p>											

A.4 Transitions d'états associées à la commutation bidirectionnelle 1+1 en mode non réversible

A.4.1 Demandes locales

Le Tableau A.7 décrit les transitions d'états provoquées par une demande locale pour la commutation de protection bidirectionnelle 1 +1 en mode non réversible.

Tableau A.7/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, bidirectionnelle, mode non réversible)

Etat		APS signalé	Demande locale								
			a	b	c	d	e	f	g	h	i
			Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	NR [r/b=néant/ normal]	→C	→D	→E ^{a)}	Sans objet	→F	Sans objet	→G	O	→I
B	Pas de demande Entité de service/ en réserve Entité de protection/ active	NR [r/b=normal]	→C	→D	(→B) ^{b)} ou →E	Sans objet	→F	Sans objet	→G	O	O
C	Verrouillage Entité de service/ active Entité de protection/ en réserve	LO [r/b=néant/ normal]	O	O	O	O	O	O	O	→A ou →E ^{c)} →F ^{d)}	O
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→C	O	O	O	→F	Sans objet	O	→H ou →E ^{c)}	O
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→C	→D	Sans objet	→H	→F	Sans objet	O	O	O

Tableau A.7/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, bidirectionnelle, mode non réversible)

Etat	APS signalé	Demande locale									
		a	b	c	d	e	f	g	h	i	
		Verrouil- lage	Commu- tation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commu- tation manuelle	Suppression	Test	
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant/ normal]	→C	O	O	O	Sans objet	→A	O	O	O
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	O	→H	O
H	Ne pas inverser Entité de service/ en réserve Entité de protection/ active	DNR [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	Sans objet	→J
I	Test Entité de service/ active Entité de protection/ en réserve	EXER [r/b=néant/ normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→A	O
J	Test Entité de service/ en réserve Entité de protection/ active	EXER [r/b=normal]	→C	→D	→E	Sans objet	→F	Sans objet	→G	→H	O

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.

NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.

NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.

a) Il transite vers l'état E s'il y a encore défaillance du signal après expiration du temporisateur d'attente de protection.

b) Si la demande FS est indiquée dans le message APS reçu en provenance de l'extrémité distante.

c) Si l'état SF est réactivé.

d) Si l'état SF-P est réactivé.

A.4.2 Demandes d'extrémité distante

Le Tableau A.8 décrit les transitions d'états provoquées par une demande d'extrémité distante reçue via le protocole APS pour la commutation de protection bidirectionnelle 1 +1 en mode non réversible.

Tableau A.8/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante (1+1, bidirectionnelle, mode non réversible)

Etat	APS signalé	Demande d'extrémité distante reçue										
		k	l	m	n	o	q	r	s	t	u	
		LO [r/b=néant/ normal]	SF-P [r/b=néant/ normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=néant/ normal]	EXER [r/b=normal]	NR [r/b=néant/ normal]	NR [r/b=normal]	DNR [r/b=normal]	
A	Pas de demande Entité de service/active Entité de protection/en réserve	NR [r/b=néant/ normal]	(→A)	(→A)	→B	→B	→B	(→A)	Sans objet	(→A) ou →E ^{a)} ou →F ^{b)}	(→A)	Sans objet
B	Pas de demande Entité de service/ en réserve Entité de protection/ active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	Sans objet	(→B)	→A ou →E ^{a)}	Sans objet	(→B)
C	Verrouillage Entité de service/ active Entité de protection/ en réserve	LO [r/b=néant/ normal]	(→C)	O	O	O	O	O	O	O	O	O
D	Commutation forcée Entité de service/ en réserve Entité de protection/ active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O

**Tableau A.8/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante
(1+1, bidirectionnelle, mode non réversible)**

Etat	APS signalé	Demande d'extrémité distante reçue										
		k	l	m	n	o	q	r	s	t	u	
		LO [r/b=néant/ normal]	SF-P [r/b=néant/ normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=néant/ normal]	EXER [r/b=normal]	NR [r/b=néant/ normal]	NR [r/b=normal]	DNR [r/b=normal]	
E	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	SF-P [r/b=néant/ normal]	→A	(→F)	O	O	O	O	O	O	O	O
G	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	Ne pas inverser Entité de service/ en réserve Entité de protection/ active	DNR [r/b=normal]	→A	→A	→B	→B	→B	Sans objet	(→H)	O	O	(→H)

**Tableau A.8/G.8031/Y.1342 – Transitions d'états provoquées par une demande d'extrémité distante
(1+1, bidirectionnelle, mode non réversible)**

Etat		APS signalé	Demande d'extrémité distante reçue									
			k	l	m	n	o	q	r	s	t	u
			LO [r/b=néant/ normal]	SF-P [r/b=néant/ normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=néant/ normal]	EXER [r/b=normal]	NR [r/b=néant/ normal]	NR [r/b=normal]	DNR [r/b=normal]
I	Test Entité de service/ en réserve Entité de protection/ active	EXER [r/b=néant/ normal]	→A	→A	→B	→B	→B	(→I)	Sans objet	O	O	Sans objet
J	Test Entité de service/ en réserve Entité de protection/ active	EXER [r/b=normal]	→A	→A	→B	→B	→B	Sans objet	(→J)	O	O	O

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.
 NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.
 NOTE 3 – "(→X)" indique que l'état n'est pas modifié et reste identique.

a) Si l'état SF est réactivé.
 b) Si l'état SF-P est réactivé.

A.5 Transitions d'états associées à la commutation unidirectionnelle 1+1 en mode réversible

A.5.1 Demandes locales

Le Tableau A.9 décrit les transitions d'états provoquées par une demande locale pour la commutation de protection unidirectionnelle 1+1 en mode réversible.

Tableau A.9/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, unidirectionnelle, mode réversible)

Etat		Demande locale									
		a	b	c	d	e	f	g	h	i	j
		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	→B	→C	→D ^{b)}	Sans objet	→E	Sans objet	→F	O	Sans objet	Sans objet
B	Verrouillage Entité de service/ active Entité de protection/ en réserve	O	O	O	O	O	O	O	→A ou →D ^{b)} →E ^{c)}	Sans objet	Sans objet
C	Commutation forcée Entité de service/ en réserve Entité de protection/ active	→B	O	O	O	→E	Sans objet	O	→A ou →D ^{c)}	Sans objet	Sans objet
D	Défaillance du signal(W) Entité de service/ en réserve Entité de protection/ active	→B	→C	Sans objet	→G	→E	Sans objet	O	O	Sans objet	Sans objet

Tableau A.9/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1+1, unidirectionnelle, mode réversible)

Etat		Demande locale									
		a	b	c	d	e	f	g	h	i	j
		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test	Expiration du temporisateur WTR
E	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	→B	O	O	O	Sans objet	→A	O	O	Sans objet	Sans objet
F	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	→B	→C	→D	Sans objet	→E	Sans objet	O	→A	Sans objet	Sans objet
G	Attente avant rétablissement Entité de service/ en réserve Entité de protection/ active	→B	→C	→D	Sans objet	→E	Sans objet	→F	→A	Sans objet	→A

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.
 NOTE 2 – "O" signifie que la demande doit être supplantée "overruled" par la condition existante car elle est de priorité inférieure.

a) Il transite vers l'état D s'il y a encore défaillance du signal après expiration du temporisateur d'attente de protection.
 b) Si l'état SF est réactivé.
 c) Si l'état SF-P est réactivé.

A.6 Transitions d'états associées à la commutation unidirectionnelle 1+1 à mode non réversible

A.6.1 Demandes locales

Le Tableau A.10 décrit les transitions d'états provoquées une demande locale pour la commutation de protection unidirectionnelle 1:1 en mode non réversible.

Tableau A.10/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1:1, unidirectionnelle, mode non réversible)

Etat		Demande locale								
		a	b	c	d	e	f	g	i	j
		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test
A	Pas de demande Entité de service/ active Entité de protection/ en réserve	→B	→C	→D ^{a)}	Sans objet	→E	Sans objet	→F	O	Sans objet
B	Verrouillage Entité de service/ active Entité de protection/ en réserve	O	O	O	O	O	O	O	→A ou →D ^{b)} →E ^{c)}	Sans objet
C	Commutation forcée Entité de service/ en réserve Entité de protection/ active	→B	O	O	O	→E	Sans objet	O	→G ou →D ^{b)}	Sans objet
D	Défaillance du signal (W) Entité de service/ en réserve Entité de protection/ active	→B	→C	Sans objet	→G	→E	Sans objet	O	O	Sans objet

Tableau A.10/G.8031/Y.1342 – Transitions d'états provoquées par une demande locale (1:1, unidirectionnelle, mode non réversible)

Etat		Demande locale								
		a	b	c	d	e	f	g	i	j
		Verrouillage	Commutation forcée	Défaillance du signal dans l'entité de service	Rétablissement de l'entité de service après un état SF	Défaillance du signal dans l'entité de protection	Rétablissement de l'entité de protection après un état SF	Commutation manuelle	Suppression	Test
E	Défaillance du signal (P) Entité de service/ active Entité de protection/ en réserve	→B	O	O	O	Sans objet	→A	O	O	Sans objet
F	Commutation manuelle Entité de service/ en réserve Entité de protection/ active	→B	→C	→D	Sans objet	→E	Sans objet	O	→G	Sans objet
G	Ne pas inverser Entité de service/en réserve Entité de protection/ active	→B	→C	→D	Sans objet	→E	Sans objet	→F	O	Sans objet

NOTE 1 – "Sans objet" signifie que l'événement considéré ne peut pas se produire pour l'état considéré.
 NOTE 2 – "O" signifie que la demande doit être supplantée ("overruled") par la condition existante car elle est de priorité inférieure.

a) Il transite vers l'état D s'il y a encore défaillance du signal après expiration du temporisateur d'attente de protection.
 b) Si l'état SF est réactivé.
 c) Si l'état SF-P est réactivé.

Appendice I

Exemple de fonctionnement du protocole APS à une phase

I.1 Introduction

On trouvera ci-après des exemples de fonctionnement du protocole APS à une phase (1:1, mode réversible ou non réversible).

I.2 Exemples de scénario

I.2.1 Mode réversible

On considère l'exemple de scénario suivant:

- 1) le domaine protégé fonctionne sans aucun défaut (l'entité de service est sélectionnée);
- 2) une défaillance du signal (SF, *signal fail*) se produit dans le sens ouest-est (commutation vers l'entité de protection);
- 3) ce défaut est corrigé (passage à l'état WTR et maintien de la sélection de l'entité de protection);
- 4) expiration du temporisateur WTR (commutation vers l'entité de service).

I.2.2 Mode non réversible

On considère l'exemple de scénario suivant:

- 1) le domaine protégé fonctionne sans aucun défaut (l'entité de service est sélectionnée);
- 2) une défaillance du signal (SF) se produit dans le sens ouest-est (commutation vers l'entité de protection);
- 3) ce défaut est corrigé (passage à l'état DNR et maintien de la sélection de l'entité de protection).

I.2.3 Défaillance du signal et commutation forcée

On considère l'exemple de scénario suivant:

- 1) une défaillance du signal (SF) se produit dans le sens ouest-est (commutation vers l'entité de protection);
- 2) la commande FS (commutation forcée) est acceptée du côté est (passage à l'état FS);
- 3) la commande FS est supprimée du côté est et l'état SF est réactivé à l'est.

I.3 Exemples de protocole APS

Des exemples de protocole APS sont illustrés sur la Figure I.1 (mode réversible), la Figure I.2 (mode non réversible) et la Figure I.3 (SF et FS).

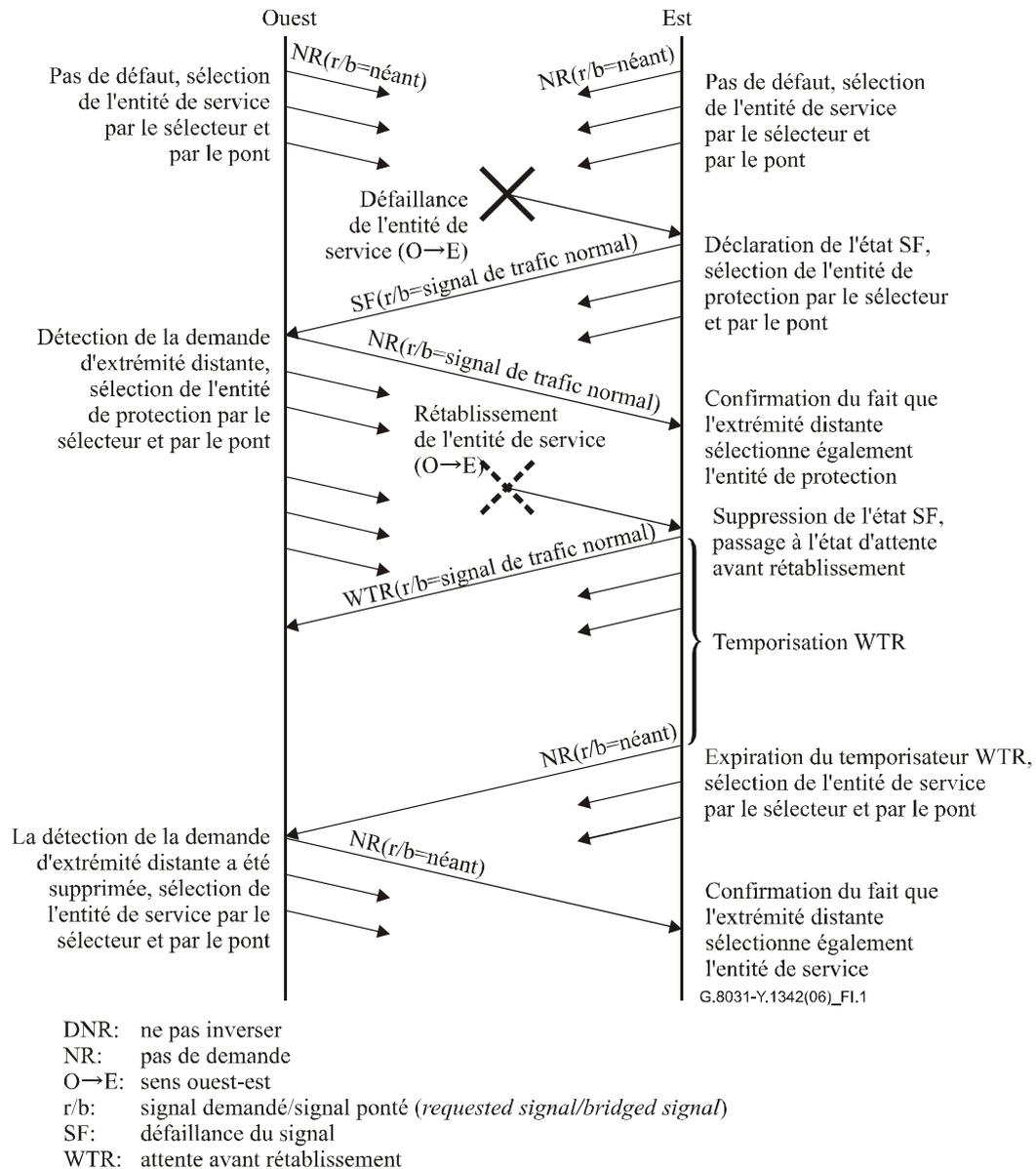
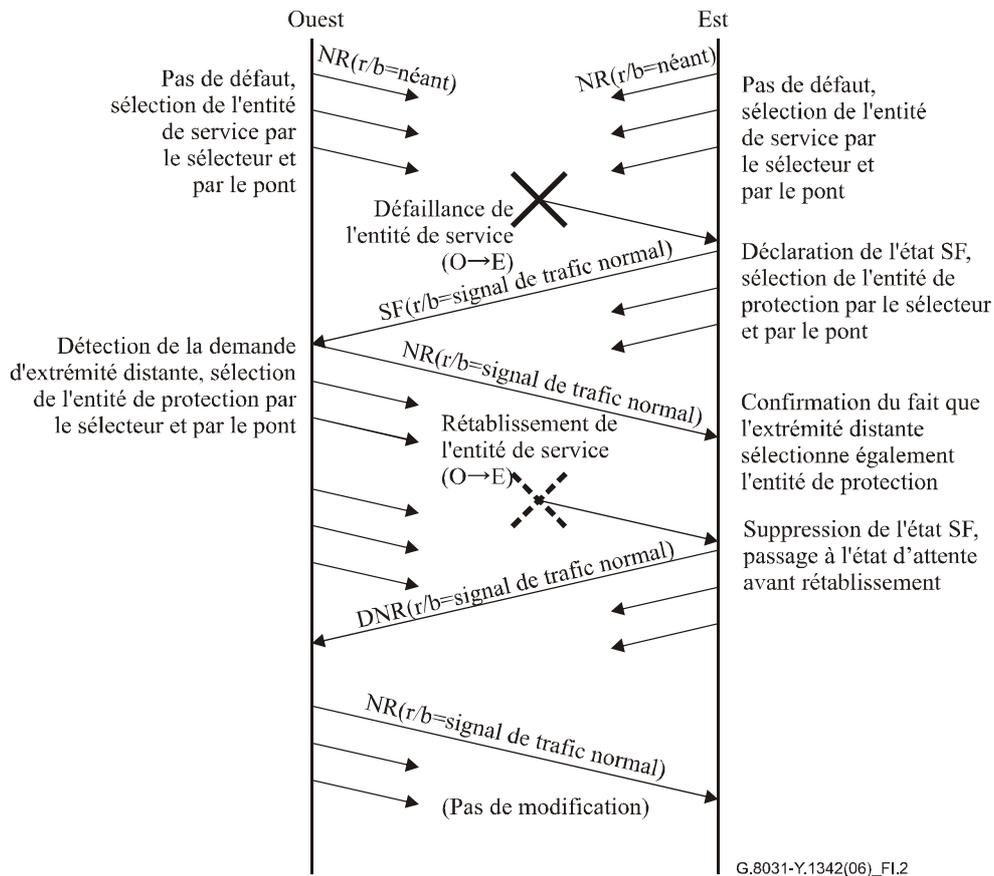


Figure I.1/G.8031/Y.1342 – Exemple de protocole (mode réversible)



G.8031-Y.1342(06)_F1.2

DNR: ne pas inverser
 NR: pas de demande
 O→E: sens ouest-est
 r/b: signal demandé/signal ponté (*requested signal/bridged signal*)
 SF: défaillance du signal
 WTR: attente avant rétablissement

Figure I.2/G.8031/Y.1342 – Exemple de protocole (mode non réversible)

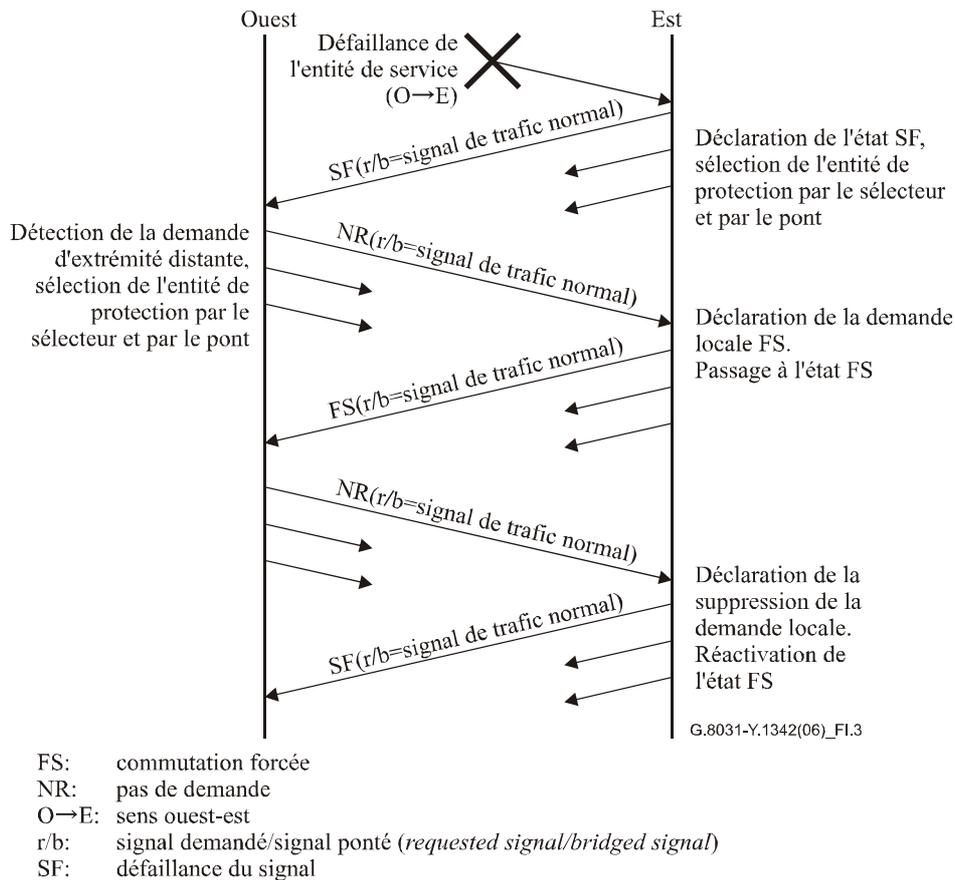


Figure I.3/G.8031/Y.1342 – Exemple de protocole (commandes SF et FS)

Appendice II

Interaction entre la commutation de protection Ethernet et le protocole STP

Le présent appendice montre qu'un port de pont dans le domaine protégé ne doit pas intervenir dans un domaine du protocole d'interconnexion arborescente (STP, *spanning tree protocol*) s'il s'agit d'éviter des interactions indésirables entre le protocole STP et la commutation de protection Ethernet. Une des solutions consiste à désactiver le protocole STP dans le domaine protégé, l'activation du protocole STP restant toutefois possible hors de ce domaine. Une autre solution consiste à faire en sorte que les entités de transport de service et de protection appartiennent à deux domaines STP différents. Ces deux scénarios sont étudiés dans le présent paragraphe.

La Figure II.1 illustre la première solution susmentionnée: le domaine protégé et les domaines STP (#1 et #2) sont segmentés verticalement et ne se chevauchent pas. Les ponts #A et #B situés aux bords du domaine protégé et des domaines STP assurent l'interconnexion des domaines STP sans problème de boucle.

La seconde solution susmentionnée est illustrée sur la Figure II.2. Les domaines STP (#1 et #2) sont segmentés horizontalement et fournissent deux entités de transport aux fins de commutation de protection Ethernet. La Figure II.3 montre que les entités de transport de service et de protection utilisées aux fins de commutation de protection Ethernet sont fournies séparément dans des domaines STP différents. Dans cet exemple, on utilise efficacement chaque réseau VLAN et chaque ressource de réseau.

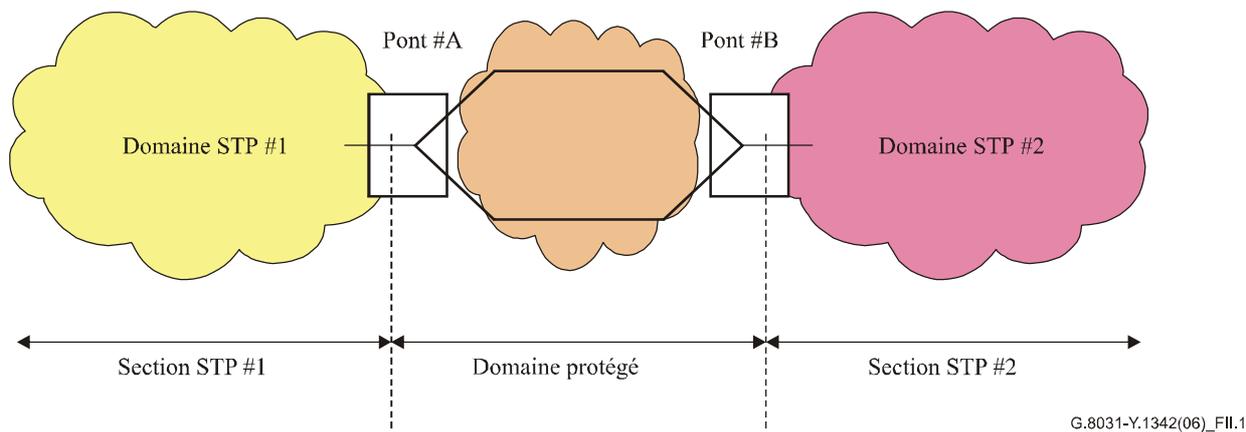


Figure II.1/G.8031/Y.1342 – Pas de chevauchement entre le domaine protégé et les domaines STP

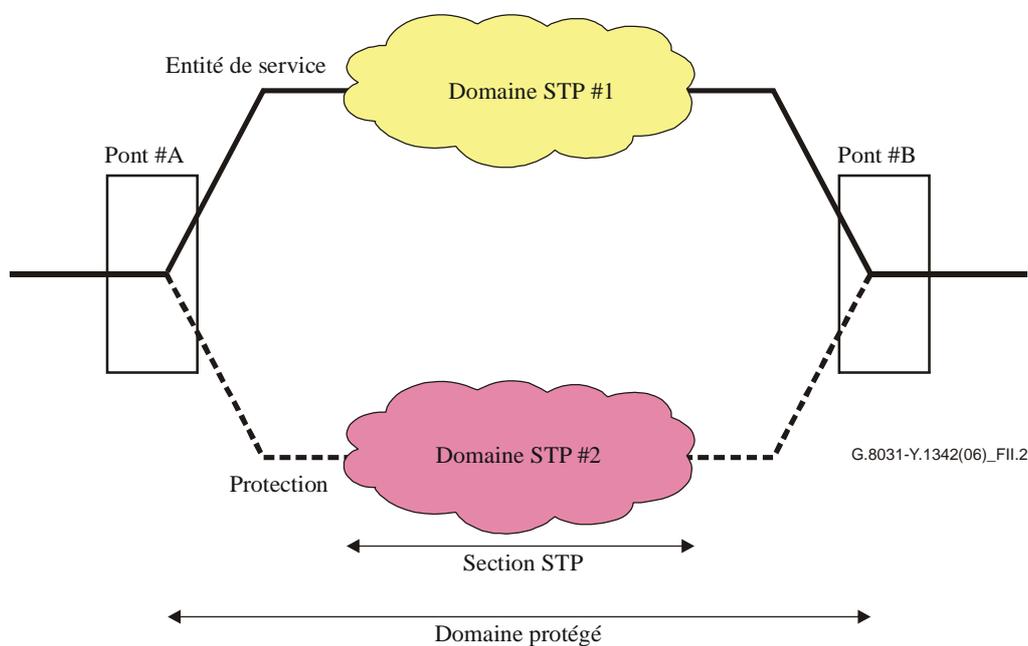


Figure II.2/G.8031/Y.1342 – Chevauchement entre le domaine protégé et les domaines STP

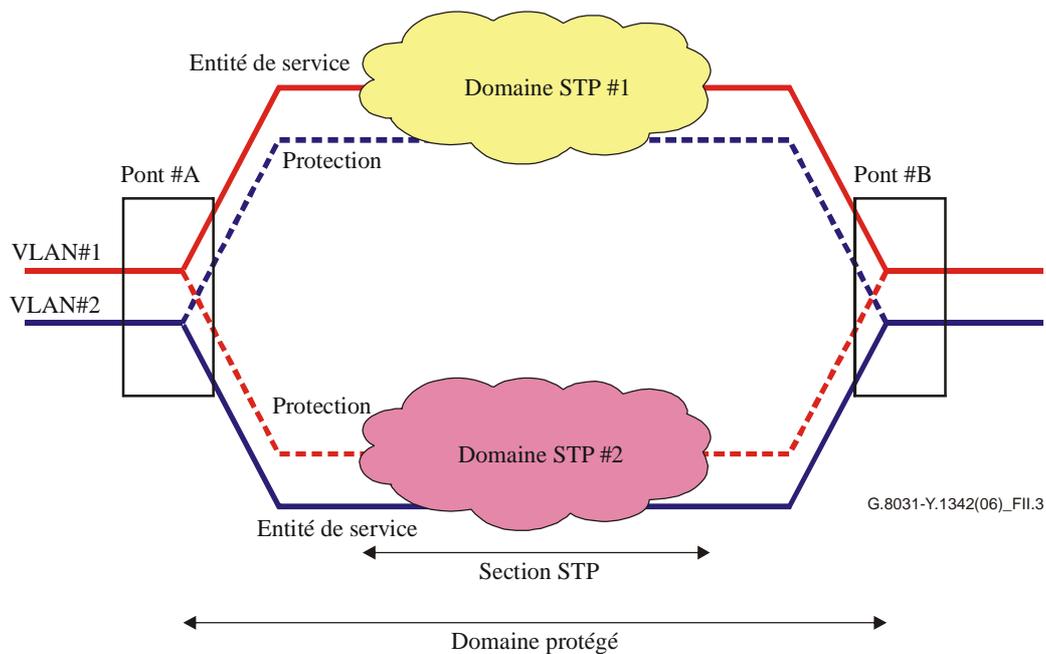


Figure II.3/G.8031/Y.1342 – Chevauchement entre le domaine protégé et les domaines STP par réseau VLAN

Appendice III

Utilisation de points MIP dans un environnement de commutation de protection

III.1 Introduction

Le présent appendice traite de l'utilisation de points MIP dans un environnement de commutation de protection et donne certains exemples de configuration.

III.2 Généralités

La Figure III.1 donne un exemple de configuration de points MEP et MIP permettant la commutation de protection. Deux paires de points MEP sont configurés pour surveiller l'entité de transport de service et l'entité de transport de protection au niveau MEG N. Au niveau MEG N+1 également, des points MEP et MIP sont configurés au niveau de chaque port (voir la figure).

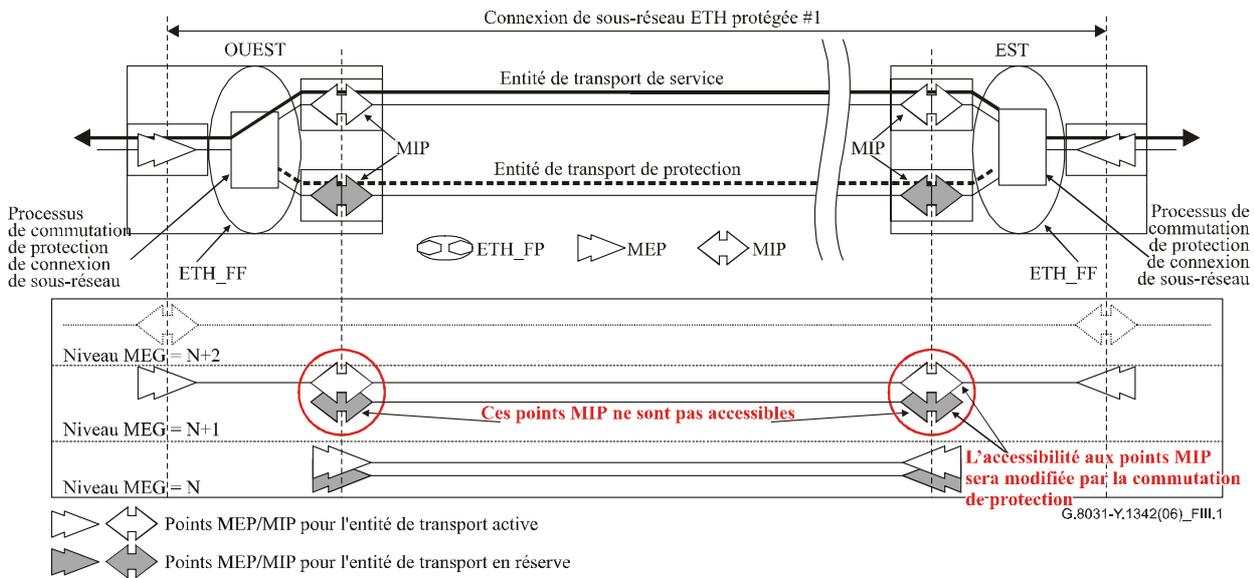


Figure III.1/G.8031/Y.1342 – Points MEP et MIP utilisés pour la commutation de protection bidirectionnelle 1:1

En commutation de protection 1:1, les points MIP de niveau MEG N+1 dans l'entité de transport en réserve ne sont pas accessibles aux points MEP du même groupe MEG. L'accessibilité aux points MIP sera modifiée par la commutation de protection. Les points MIP de niveau MEG N+1 représentés sur la Figure III.1 semblent donc inutiles.

La Figure III.2 décrit une configuration de points MEP et MIP dans un environnement de commutation de protection unidirectionnelle 1+1. Dans le cas décrit, une communication de demande/réponse entre un point MEP et un point MIP ne peut pas être effectuée correctement. Les points MIP de niveau MEG N+1 représentés sur la Figure III.2 semblent donc également inutiles.

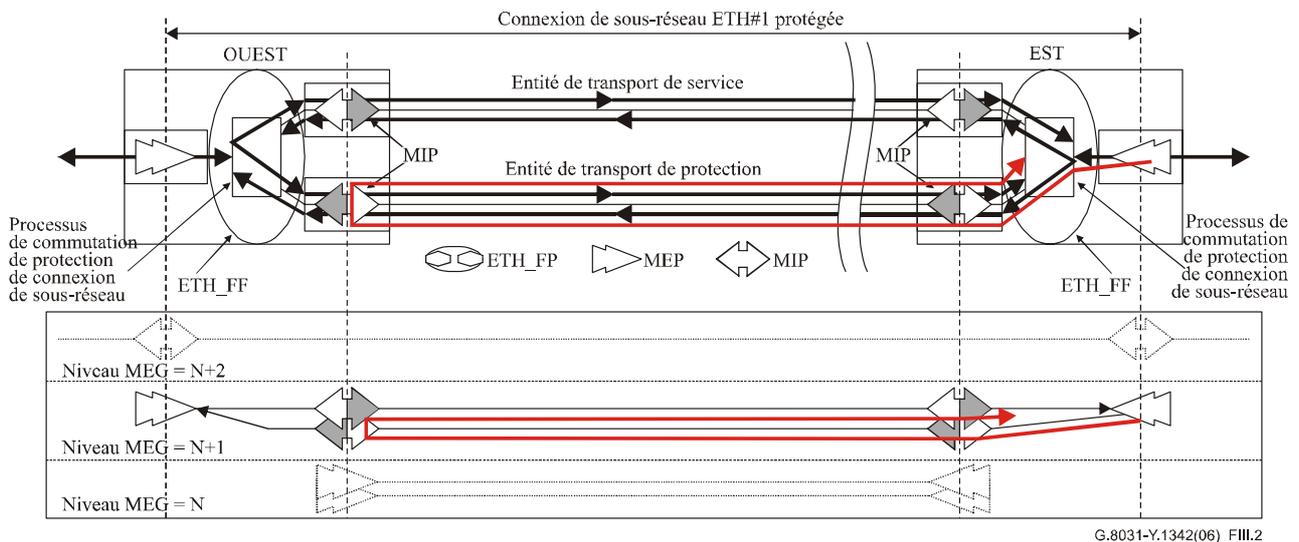


Figure III.2/G.8031/Y.1342 – Points MEP et MIP utilisés pour la commutation de protection unidirectionnelle 1+1

Comme on l'a vu plus haut, il semble inutile de configurer des points MIP quelque part dans le domaine protégé, à un niveau MEG supérieur à celui des points MEP qui surveillent l'entité de transport de service et l'entité de transport de protection.

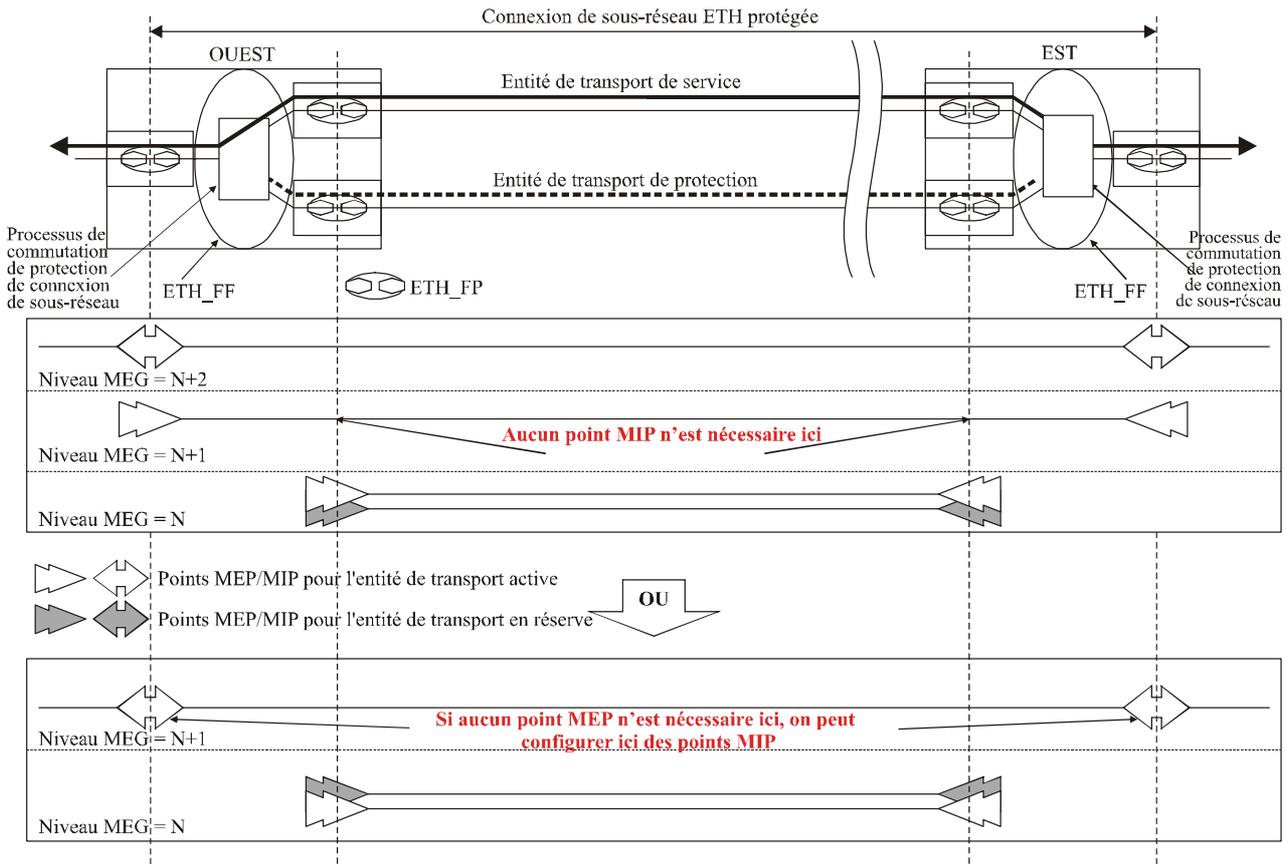
III.3 Exemples de configuration

La Figure III.3 illustre deux exemples de configurations possibles de points MEP et MIP.

Dans le premier exemple (milieu de la Figure III.3), aucun point MIP n'est configuré au niveau MEG N+1 mais on y trouve des points MEP. Dans ce cas, le groupe MEG de niveau MEG N+1 représente le domaine protégé.

Dans le second exemple (bas de la Figure III.3), les points MIP sont configurés au niveau MEG N+1 aux bords du domaine protégé.

Les points MEP et MIP représentés dans les deux exemples sont pleinement accessibles car ils ne sont pas configurés à l'intérieur du domaine protégé.



G.8031-Y.1342(06)_FIII.3

Figure III.3/G.8031/Y.1342 – Exemples de configuration de points MEP et MIP dans un environnement de commutation de protection

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

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

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