Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

G.808.1

(03/2006)

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

Réseaux numériques – Généralités

Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux

Recommandation UIT-T G.808.1

RECOMMANDATIONS UIT-T DE LA SÉRIE G

SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

CONNEXIONS ET CIRCUITS TÉLÉPHONIQUES INTERNATIONAUX	G.100–G.199
CARACTÉRISTIQUES GÉNÉRALES COMMUNES À TOUS LES SYSTÈMES ANALOGIQUES À COURANTS PORTEURS	G.200–G.299
CARACTÉRISTIQUES INDIVIDUELLES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX À COURANTS PORTEURS SUR LIGNES MÉTALLIQUES	G.300–G.399
CARACTÉRISTIQUES GÉNÉRALES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX HERTZIENS OU À SATELLITES ET INTERCONNEXION AVEC LES SYSTÈMES SUR LIGNES MÉTALLIQUES	G.400–G.449
COORDINATION DE LA RADIOTÉLÉPHONIE ET DE LA TÉLÉPHONIE SUR LIGNES	G.450–G.499
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.600–G.699
EQUIPEMENTS TERMINAUX NUMÉRIQUES	G.700–G.799
RÉSEAUX NUMÉRIQUES	G.800–G.899
Généralités	**G.800–G.809**
Objectifs de conception pour les réseaux numériques	G.810–G.819
Objectifs de qualité et de disponibilité	G.820–G.829
Fonctions et capacités du réseau	G.830–G.839
Caractéristiques des réseaux à hiérarchie numérique synchrone	G.840–G.849
Gestion du réseau de transport	G.850–G.859
Intégration des systèmes satellitaires et hertziens à hiérarchie numérique synchrone	G.860–G.869
Réseaux de transport optiques	G.870–G.879
SECTIONS NUMÉRIQUES ET SYSTÈMES DE LIGNES NUMÉRIQUES	G.900–G.999
QUALITÉ DE SERVICE ET DE TRANSMISSION – ASPECTS GÉNÉRIQUES ET ASPECTS LIÉS À L'UTILISATEUR	G.1000–G.1999
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.6000–G.6999
DONNÉES SUR COUCHE TRANSPORT – ASPECTS GÉNÉRIQUES	G.7000–G.7999
ASPECTS RELATIFS AU PROTOCOLE ETHERNET SUR COUCHE TRANSPORT	G.8000–G.8999
RÉSEAUX D'ACCÈS	G.9000–G.9999

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

Recommandation UIT-T G.808.1

Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux

Résumé

La présente Recommandation définit les modèles fonctionnels, les caractéristiques et les processus génériques associés à divers procédés de protection linéaire pour couches de réseau en mode connexion; par exemple, les réseaux de transport optique (OTN, *optical transport network*), les réseaux en hiérarchie numérique synchrone (SDH, *synchronous digital hierarchy*) et les réseaux en mode de transfert asynchrone (ATM, *asynchronous transfer mode*).

Elle définit également les objectifs et les applications de ces procédés. Les procédés de sécurisation décrits dans la présente Recommandation sont la protection des chemins et la protection des connexions SNC avec diverses options de surveillance pour des signaux individuels ou pour des groupes de signaux. Elle décrit par ailleurs la capacité d'autorétablissement offerte par le procédé d'ajustement de la capacité d'une liaison (procédé LCAS, *link capacity adjustment scheme*).

Les modèles fonctionnels, les caractéristiques et les processus génériques concernant les procédés de sécurisation d'anneau et de sous-réseau interconnecté (par exemple, en anneau) sont définis dans d'autres Recommandations.

Source

La Recommandation UIT-T G.808.1 a été approuvée le 29 mars 2006 par la Commission d'études 15 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

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

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

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

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T G.808.1

Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux

1 Domaine d'application

La présente Recommandation donne un aperçu général des aspects génériques de la commutation de protection linéaire. Elle couvre les procédés de sécurisation dans les réseaux de types OTN, SDH et ATM. Des aperçus généraux des procédés de protection annulaire et d'interconnexion de sous-réseaux binodaux (par exemple, en anneau) seront fournies dans d'autres Recommandations.

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.783 (2006), *Caractéristiques des blocs fonctionnels des équipements de la hiérarchie numérique synchrone*.

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

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

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

– Recommandation UIT-T G.842 (1997), *Interfonctionnement des architectures de protection des réseaux à hiérarchie numérique synchrone*.

– Recommandation UIT-T G.873.1 (2006), *Réseau de transport optique: protection linéaire*.

– Recommandation UIT-T I.630 (1999), *Commutation de protection ATM*.

– Recommandation UIT-T I.732 (2000), *Caractéristiques fonctionnelles des équipements ATM*.

– Recommandation UIT-T M.495 (1988), *Rétablissement de transmission et diversité de routage de transmission: terminologie et principes généraux*.

3 Termes et définitions

3.1 La présente Recommandation utilise les termes suivants:

– **A**: désignation d'extrémité utilisée lors de la description d'un domaine protégé; A est l'extrémité source des signaux protégés pour lesquels la signalisation de requête de commutation est lancée à partir de l'autre extrémité, Z.

– **Z**: désignation d'extrémité utilisée lors de la description d'un domaine protégé; Z est l'extrémité à partir de laquelle la signalisation de requête de commutation est lancée.

3.2 La présente Recommandation utilise les termes suivants, qui sont définis dans la Rec. UIT-T G.805:

a) information adaptée (AI, *adapted information*);

b) information caractéristique (CI, *characteristic information*);

c) connexion de liaison;

d) réseau;

e) connexion de liaison composite en série;

f) sous-réseau;

g) chemin.

3.3 Dans la présente Recommandation, les termes ci-après figurant dans la Rec. UIT-T G.870/Y.1352 sont utilisés:

3.3.1 Action

3.3.1.1 commutation: voir la Rec. UIT-T G.870/Y.1352.

3.3.2 Protocole de commutation APS

3.3.2.1 à 1 phase: voir la Rec. UIT-T G.870/Y.1352.

3.3.2.2 à 2 phases: voir la Rec. UIT-T G.870/Y.1352.

3.3.2.3 à 3 phases: voir la Rec. UIT-T G.870/Y.1352.

3.3.3 Classe de protection

3.3.3.1 protection de chemin: voir la Rec. UIT-T G.870/Y.1352.

3.3.3.2 protection de connexion de sous réseau: voir la Rec. UIT-T G.870/Y.1352.

La détermination d'un état de défaut d'une connexion de liaison composite en série dans le domaine protégé peut être effectuée comme suit:

3.3.3.2.1 surveillance de sous-couche (/S): voir la Rec. UIT-T G.870/Y.1352.

3.3.3.2.2 surveillance sans intrusion (/N): voir la Rec. UIT-T G.870/Y.1352.

3.3.3.2.3 surveillance intrinsèque (/I): voir la Rec. UIT-T G.870/Y.1352.

3.3.3.2.4 surveillance par essai (/T): voir la Rec. UIT-T G.870/Y.1352.

3.3.3.3 protection de connexion de réseau: voir la Rec. UIT-T G.870/Y.1352.

3.3.3.4 protection individuelle: voir la Rec. UIT-T G.870/Y.1352.

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

3.3.4 Sous-classe de protection

3.3.4.1 surdébit/flux OAM (e) de bout en bout: voir la Rec. UIT-T G.870/Y.1352.

3.3.4.2 surdébit/flux OAM (s) de sous-couche: voir la Rec. UIT-T G.870/Y.1352.

3.3.5 Composants

3.3.5.1 domaine protégé: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.2 dérivation: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.2.1 dérivation permanente: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.2.2 dérivation divergente: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.2.3 dérivation sélective: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.3 **extracteur**: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.3.1 **extracteur divergent**: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.3.2 **extracteur convergent**: voir la Rec. UIT-T G.870/Y.1352.

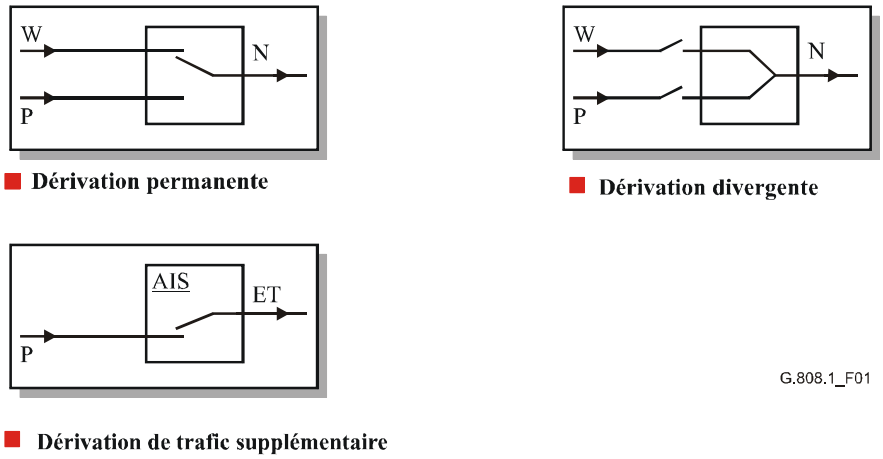


Figure 1/G.808.1 – Dérivations de protection

3.3.5.4 **tête**: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.5 **queue**: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.6 **nœud collecteur**: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.7 **nœud source**: voir la Rec. UIT-T G.870/Y.1352.

3.3.5.8 **nœud intermédiaire**: voir la Rec. UIT-T G.870/Y.1352.

3.3.6 Etat de défaut

3.3.6.1 **signal de dégradation (SD, *signal degrade*)**: voir la Rec. UIT-T G.805.

3.3.6.2 **signal de panne (SF, *signal fail*)**: voir la Rec. UIT-T G.805.

3.3.6.3 **signal de dégradation de groupe (SDG, *signal degrade group*)**: voir la Rec. UIT-T G.870/Y.1352.

3.3.6.4 **signal de panne de groupe (SFG, *signal fail group*)**: voir la Rec. UIT-T G.870/Y.1352.

3.3.6.5 **signal de dégradation du serveur (SSD, *server signal degrade*)**: voir la Rec. UIT-T G.806.

3.3.6.6 **signal de panne du serveur (SSF, *server signal fail*)**: voir la Rec. UIT-T G.806.

3.3.6.7 **signal de dégradation d'un chemin (TSD, *trail signal degrade*)**: voir la Rec. UIT-T G.806.

3.3.6.8 **panne de signal d'un chemin (TSF, *trail signal fail*)**: voir la Rec. UIT-T G.806.

3.3.7 Architecture

3.3.7.1 **architecture (de protection par redondance) 1+1**: voir la Rec. UIT-T G.870/Y.1352.

3.3.7.2 **architecture (de protection par redondance) 1:n (n ≥ 1)**: voir la Rec. UIT-T G.870/Y.1352.

3.3.7.3 architecture (de protection par redondance) m:n: voir la Rec. UIT-T G.870/Y.1352.

3.3.7.4 architecture de protection $(1:1)^n$ (multidoublée): voir la Rec. UIT-T G.870/Y.1352.

3.3.8 Commandes externes

3.3.8.1 verrouillage de l'entité de transport de protection #i (LO #i): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.2 verrouillage du signal de trafic normal #i: voir la Rec. UIT-T G.870/Y.1352.

3.3.8.3 relève de verrouillage du signal de trafic normal #i: voir la Rec. UIT-T G.870/Y.1352.

3.3.8.4 gel: voir la Rec. UIT-T G.870/Y.1352.

3.3.8.5 commutation forcée du signal de trafic normal #i (FS #i): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.6 commutation forcée du signal vide (FS #0): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.7 commutation forcée du signal de trafic supplémentaire (FS #ExtraTrafficSignalNumber): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.8 commutation manuelle du signal de trafic normal #i (MS #i): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.9 commutation manuelle du signal vide (MS #0): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.10 commutation manuelle du signal de trafic supplémentaire (MS #ExtraTrafficSignalNumber): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.11 signal d'essai préalable #i (EX, *exercise signal* #i): voir la Rec. UIT-T G.870/Y.1352.

3.3.8.12 acquittement (CLR, *clear*): voir la Rec. UIT-T G.870/Y.1352.

3.3.9 Etats

3.3.9.1 maintien du signal de trafic normal #i (DNR, *do not revert* #i): voir la Rec. UIT-T G.870/Y.1352.

3.3.9.2 absence de requête (NR, *no request*): voir la Rec. UIT-T G.870/Y.1352.

3.3.9.3 période d'attente de rétablissement du signal de trafic normal #i (WTR, *wait-to-restore*): voir la Rec. UIT-T G.870/Y.1352.

3.3.10 Fonctionnement

3.3.10.1 fonctionnement (de protection) réversible: voir la Rec. UIT-T G.870/Y.1352.

3.3.10.2 fonctionnement (de protection) irréversible: voir la Rec. UIT-T G.870/Y.1352.

3.3.11 Signal

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

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

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

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

3.3.12 Commutation

3.3.12.1 commutation (de protection) bidirectionnelle: voir la Rec. UIT-T G.780/Y.1351.

3.3.12.2 commutation (de protection) unidirectionnelle: voir la Rec. UIT-T G.780/Y.1351.

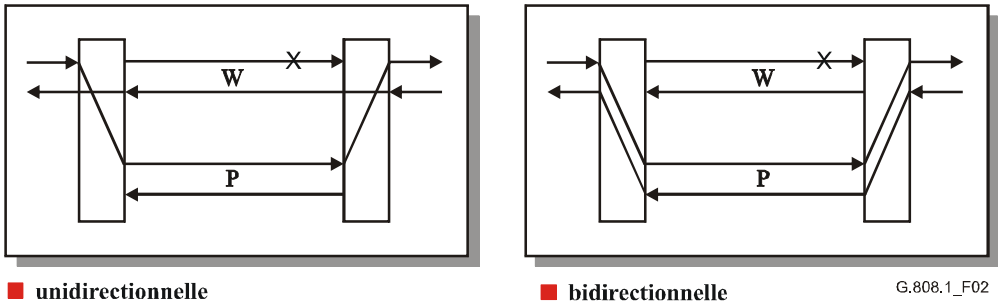


Figure 2/G.808.1 – Types de commutation

3.3.13 Temps

3.3.13.1 temps de détection: voir la Rec. UIT-T G.870/Y.1352.

3.3.13.2 temps d'attente de protection: voir la Rec. UIT-T G.870/Y.1352.

3.3.13.3 période d'attente de rétablissement: voir la Rec. UIT-T G.870/Y.1352.

3.3.13.4 temps de commutation: voir la Rec. UIT-T G.870/Y.1352.

3.3.14 Entité de transport

3.3.14.1 entité de transport: voir la Rec. UIT-T G.870/Y.1352.

3.3.14.2 protection d'entité de transport: voir la Rec. UIT-T G.870/Y.1352.

3.3.14.3 entité de transport en protection: voir la Rec. UIT-T G.870/Y.1352.

3.3.14.4 entité de transport de service: voir la Rec. UIT-T G.870/Y.1352.

3.3.14.5 entité de transport active: voir la Rec. UIT-T G.870/Y.1352.

3.3.14.6 entité de transport en réserve: voir la Rec. UIT-T G.870/Y.1352.

3.3.14.7 groupe: voir la Rec. UIT-T G.870/Y.1352.

3.3.15 protection: voir la Rec. UIT-T G.870/Y.1352.

3.3.16 rétablissement: voir la Rec. UIT-T G.870/Y.1352.

3.3.17 escalade: voir la Rec. UIT-T G.870/Y.1352.

3.3.18 commutation de protection transparente: voir la Rec. UIT-T G.870/Y.1352.

3.3.19 dégradation: voir la Rec. UIT-T G.870/Y.1352.

3.3.20 capacité d'autorétablissement d'un réseau: voir la Rec. UIT-T G.870/Y.1352.

3.3.21 rapport de protection: voir la Rec. UIT-T G.870/Y.1352.

3.3.22 interfonctionnement de sous-réseaux: voir la Rec. UIT-T G.870/Y.1352.

3.3.23 réseau autorétablissable: voir la Rec. UIT-T G.780/Y.1351.

3.3.24 événement de commutation: voir la Rec. UIT-T G.870/Y.1352.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ABR débit binaire disponible (*available bit rate*)

AI information adaptée (*adapted information*)

AIS signal d'indication d'alarme (*alarm indication signal*)

AP point d'accès (*access point*)
APS commutation automatique de protection (*automatic protection switching*)
ATM mode de transfert asynchrone (*asynchronous transfer mode*)
AU unité administrative (*administrative unit*)
B largeur de bande (*bandwidth*)
BER taux d'erreurs sur les bits (*bit error rate*)
BR dérivation (*bridge*)
CC contrôle de continuité (*continuity check*)
CI information caractéristique (*characteristic information*)
CP point de connexion (*connection point*)
DEG dégradation
ET trafic supplémentaire (signal) (*extra traffic*)
F4 flux n° 4 (mode ATM)
FDI indication de défaut vers l'avant (*forward defect indication*)
HO temps d'attente (*hold off*)
IMG groupe à multiplexage inverse (*inverse multiplexed group*)
LCAS procédé d'ajustement de capacité de liaison (*link capacity adjustment scheme*)
MPLS commutation multiprotocolaire avec étiquette (*multi-protocol label switching*)
MS section multiplex (*multiplex section*)
N normal (signal)
NE élément de réseau (*network element*)
NIM surveillance non intrusive (*non-intrusive monitoring*)
NR absence de requête (*no request*)
NUT trafic non protégé et non réservable (*non-pre-emptible unprotected traffic*)
OAM gestion, exploitation et maintenance (*operations, administration and maintenance*)
OCh canal optique (*optical channel*)
OH en-tête (*overhead*)
OTN réseau de transport optique (*optical transport network*)
P protection
PDH hiérarchie numérique plésiochrone (*plesiochronous digital hierarchy*)
POH préfixe de conduit (*path overhead*)
PP traitement de pointeur (*pointer processing*)
PU unité d'interface (*port unit*)
RDI indication de défaut distant (*remote defect indication*)
REI indication d'erreur distante (*remote error indication*)
RI informations distantes (*remote information*)
RS section de régénération (*regenerator section*)

SD dégradation du signal (*signal degrade*)

SDG groupe de dégradations de signal (*signal degrade group*)

SDH hiérarchie numérique synchrone (*synchronous digital hierarchy*)

SEL sélecteur

SES seconde gravement erronée (*severely errored second*)

SF défaillance du signal (*signal fail*)

SFG groupe de défaillances du signal (*signal fail group*)

SIM autorétablissement de connexions de liaison à multiplexage inverse (*survivability of inverse multiplexed link connections*)

Sm couche de conteneurs VC-m (m = 11, 12, 2) d'ordre inférieur

Sn couche de conteneurs VC-n (n = 3, 4, 4-Xc) d'ordre supérieur ou couche de conteneurs VC-3 d'ordre inférieur

SNC connexion de sous-réseau (*subnetwork connection*)

SNC/I protection SNCP à surveillance intrinsèque (*inherently monitored subnetwork connection protection*)

SNC/N protection SNCP à surveillance non intrusive (*non-intrusively monitored subnetwork connection protection*)

SNC/Ne protection SNC/N à surveillance du surdébit de bout en bout (*SNC/N, monitoring of end-to-end OH*)

SNC/Ns protection SNC/N à surveillance du surdébit de sous-couche (*SNC/N, monitoring of sub-layer OH*)

SNC/S protection SNCP à surveillance de sous-couche (*SNCP with sublayer monitoring*)

SNC/Ss protection SNC/S à surveillance du surdébit de sous-couche (*SNC/S, monitoring of sublayer OH*)

SNC/T protection SNCP à surveillance de chemin d'essai (*SNCP with test trail monitoring*)

SNC/Te protection SNC/T à surveillance du surdébit de bout en bout (*SNC/T, monitoring of end-to-end OH*)

SNC/Ts protection SNC/T à surveillance du surdébit de sous-couche (*SNC/T, monitoring of sublayer OH*)

SNCP protection de connexion de sous-réseau (*subnetwork connection protection*)

Sn-Xv couche de conteneurs VC-n-Xv (*VC-n-Xv layer*)

SOH surdébit de section (*section overhead*)

SSD dégradation de signal de serveur (*server signal degrade*)

SSF défaillance de signal de serveur (*server signal fail*)

STM-N module de transport synchrone de niveau N (*synchronous transport module, level N*)

TCP point de connexion de terminaison (*termination connection point*)

TSD dégradation de signal de chemin (*trail signal degrade*)

TSF défaillance de signal de chemin (*trail signal fail*)

TSI échange d'intervalle de temps (*timeslot interchange*)

TT terminaison de cheminement (*trail termination*)

TU unité d'affluents (*tributary unit*)

UBR débit cellulaire non spécifié (*unspecified bit rate*)

UPSR anneau de commutation de trajet unidirectionnelle (*unidirectional path switch ring*)

VC voie virtuelle (ATM) (*virtual channel*)

VCG groupe de concaténations virtuelles (*virtual concatenation group*)

VC-n conteneur virtuel d'ordre n (*virtual container-n*)

VC-n-Xv conteneurs virtuels d'ordre n concaténés avec des conteneurs virtuels d'ordre X (*virtual concatenation of X virtual containers (of level n)*)

VP conduit virtuel (ATM) (*virtual path*)

VPI identificateur de conduit virtuel (*virtual path identifier*)

W trafic (*working*)

WTR (période d')attente de rétablissement (*wait-to-restore*)

X, Y, Z désignations de couche (non spécifiée) ou d'effectif de groupe (*layer (for non-specified layers) or group size designations*)

5 Conventions

Aucune.

6 Concepts de protection individuelle et de protection de groupe

Le concept de protection individuelle s'applique aux situations où il est utile de protéger seulement une partie des signaux de trafic, qui nécessitent un niveau élevé de fiabilité. Le reste des signaux de trafic dans la couche de réseau demeure non protégé. Cela contribue à réduire la largeur de bande nécessaire à la protection.

Le concept de protection de groupe s'applique aux situations:

i) où il est utile de protéger un grand nombre (mais pas la totalité) des signaux de trafic transportés au moyen des mêmes chemins de couche serveur, avec des temps de protection dans le même ordre que la protection individuelle (d'un petit ensemble de signaux de trafic). Une commutation de protection rapide est obtenue par le traitement d'un faisceau logique d'entités de transport comme une seule entité après le commencement des actions de protection;

ii) où il est utile de protéger un groupe de signaux de trafic qui réalise un seul signal de trafic, par exemple au moyen d'une concaténation virtuelle ou d'un multiplexage inverse.

La complexité du processus de protection est réduite par le traitement du groupe de signaux comme une seule entité, au cours d'un seul processus de protection. L'état des groupes de trafic et de protection est décrit par les indications de groupe SF et SD.

La complexité peut encore être réduite par l'introduction d'un signal d'essai supplémentaire (transporté sur les mêmes chemins de couche serveur), dont les indications SF et SD servent à décrire l'état du groupe. L'*inconvénient* de cette dernière technique de réduction de la complexité est l'impossibilité de surveiller les signaux individuels dans chaque groupe, quant à leur connexité, quant à leur continuité et quant à leur qualité. Un de ces défauts, apparaissant dans un des signaux du groupe, ne sera pas détecté et ne sera donc pas protégé.

7 Types d'architecture

L'architecture de protection peut être de type 1+1, 1:n, m:n ou $(1:1)^n$.

Les avantages possibles de l'architecture en 1+1 sont les suivants:

1) faible complexité;

2) dans le cas d'une commutation dans un seul sens, possibilité de prendre en charge l'interconnexion de paires de nœuds de sous-réseaux protégés.

Les inconvénients possibles de l'architecture 1+1 sont les suivants:

3) 100% de la capacité nécessaire.

Les avantages possibles des architectures en 1:n, m:n et $(1:1)^n$ sont les suivants:

1) possibilité de fournir un accès de protection; l'entité de transport/la largeur de bande de protection peut transporter un signal de trafic supplémentaire lorsque l'entité de transport/la largeur de bande de protection n'est pas appelée à transporter un signal de trafic normal;

2) la capacité supplémentaire est limitée à 100/n % ou m × 100/n %;

3) dans le cas de l'architecture en m:n, jusqu'à m défauts peuvent être protégés.

Les inconvénients possibles des architectures en 1:n, m:n et $(1:1)^n$ sont les suivants:

4) complexité;

5) dans le cas de la classe de protection de connexion SNC, il est nécessaire d'ajouter des fonctions de terminaison de sous-couche aux points d'entrée et de sortie du domaine protégé de chaque entité de transport de trafic normal et de trafic protégé;

6) cette architecture ne prend pas en charge l'interconnexion de paires de nœuds de sous-réseaux protégés;

7) $n \geq 2$: chacune des n entités de transport en service doit toujours être routée au moyen de différentes ressources et de différents équipements afin d'éviter l'apparition de points de panne communs ne pouvant pas être protégés par l'unique entité de transport en protection dans une architecture en 1:n ou $(1:1)^n$.

NOTE 1 – Normalement, n+1 trajets de secours entre deux nœuds du réseau ne seront pas disponibles. Par elles-mêmes, les architectures en 1:n et $(1:1)^n$, avec $n \geq 2$, *n'offriront pas une protection adéquate* aux n signaux de trafic normal transportés normalement au moyen des n entités de transport en service. n = 1 semble donc être le seul choix logique.

NOTE 2 – En mode ATM, l'accès de protection n'est pas explicitement tenu de permettre l'usage de la largeur de bande de protection normalement inutilisée; le trafic à débit ABR et UBR pourra utiliser cette largeur de bande de protection au moyen d'une surréservation de la largeur de bande du signal serveur contenant l'entité de transport en protection. Le mécanisme de commande de couche supérieure à débit ABR/UBR est censé réduire le trafic lorsque la protection est réellement utilisée. Les nœuds d'entrée/de sortie du domaine de protection ne sont pas tenus de s'aligner sur les nœuds d'entrée/de sortie du trafic à débit ABR/UBR. Cette caractéristique ajoute de la flexibilité au réseau et en réduit la complexité.

7.1 Architecture de protection 1+1 (doublée)

Dans le type d'architecture 1+1, une entité de transport en protection est spécialisée comme ressource de secours offerte à l'entité de transport en service, le signal de trafic normal étant dérivé vers l'entité de transport en protection à l'extrémité source du domaine protégé. Le trafic normal des entités de transport en service et en protection est transmis simultanément à l'extrémité collectrice du domaine protégé, où une sélection entre entités de transport en service et en protection est effectuée sur la base de certains critères prédéterminés, tels que des indications de panne du signal et de dégradation du signal. Voir la Figure 3.

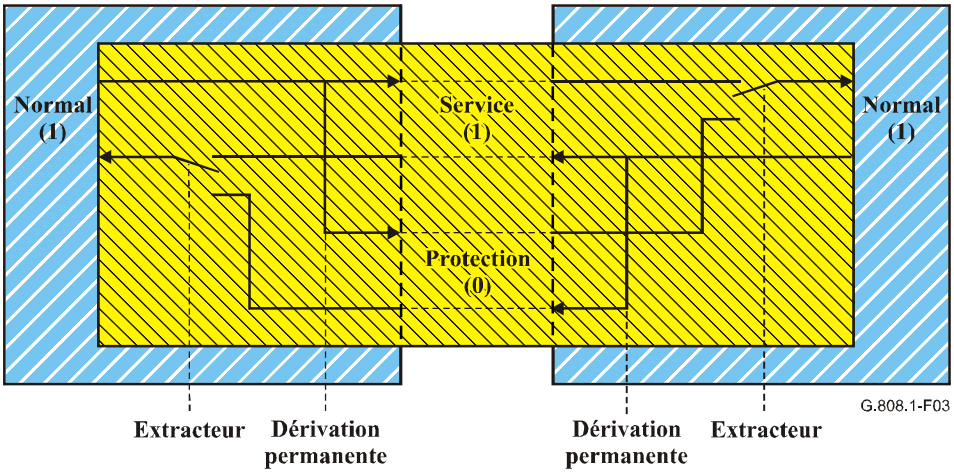


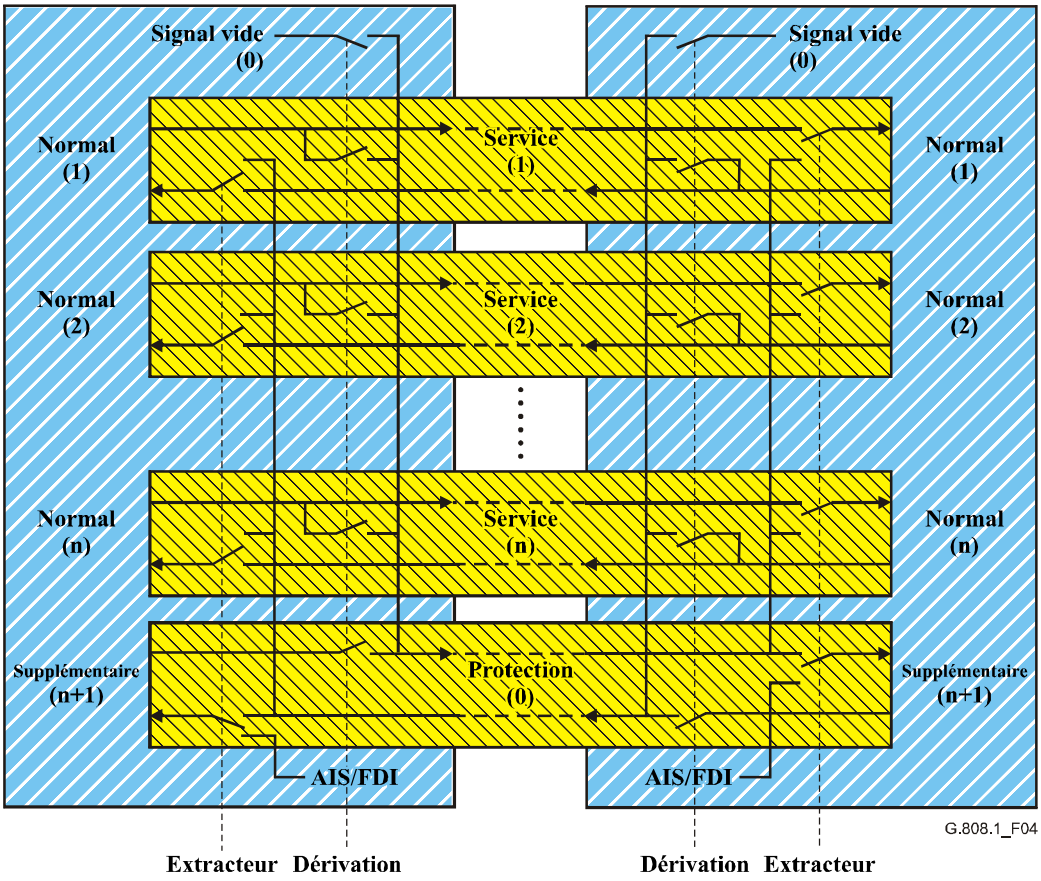
Figure 3/G.808.1 – Architecture de protection 1+1 (doublée)

7.2 Architecture de protection 1:n (partagée)

Dans le type d'architecture en 1:n, une entité de transport en protection spécialisée est une ressource de secours partagée entre n entités de transport en service. La largeur de bande de l'entité de transport en protection devrait être attribuée de telle manière qu'il soit possible de protéger l'une quelconque des n entités de transport en service si l'entité de transport en protection est disponible.

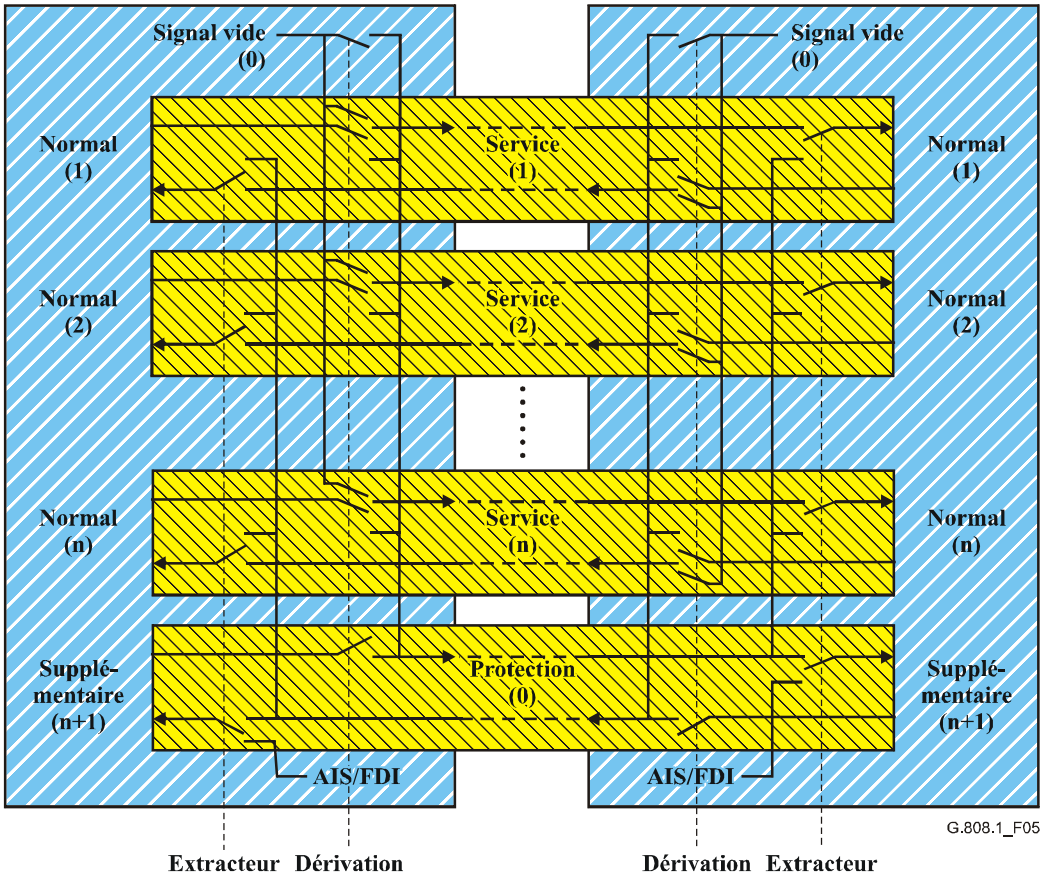
Lorsqu'une entité de transport en service est détectée comme étant dégradée, son signal de trafic normal doit toujours être transféré de l'entité de transport en service à l'entité de transport en protection aux deux extrémités – source et collectrice – du domaine protégé. Il est noté que si plus d'une seule entité de transport en service est dégradée, un seul signal de trafic normal peut être protégé.

La dérivation peut être réalisée de deux façons: par dérivation sélective ou par dérivation divergente. En connexité par dérivation sélective (Figure 5), le signal de trafic normal est connecté soit à l'entité de transport en service ou à l'entité de transport en protection. En connexité par dérivation divergente (Figure 4), le signal de trafic normal est connecté en permanence à l'entité de transport en service et occasionnellement à l'entité de transport en protection. L'interfonctionnement entre les deux options est garanti.



Option de dérivation divergente: signal de trafic normal permanent connecté sur trafic et occasionnellement sur protection

Figure 4/G.808.1 – Architecture de protection 1:n

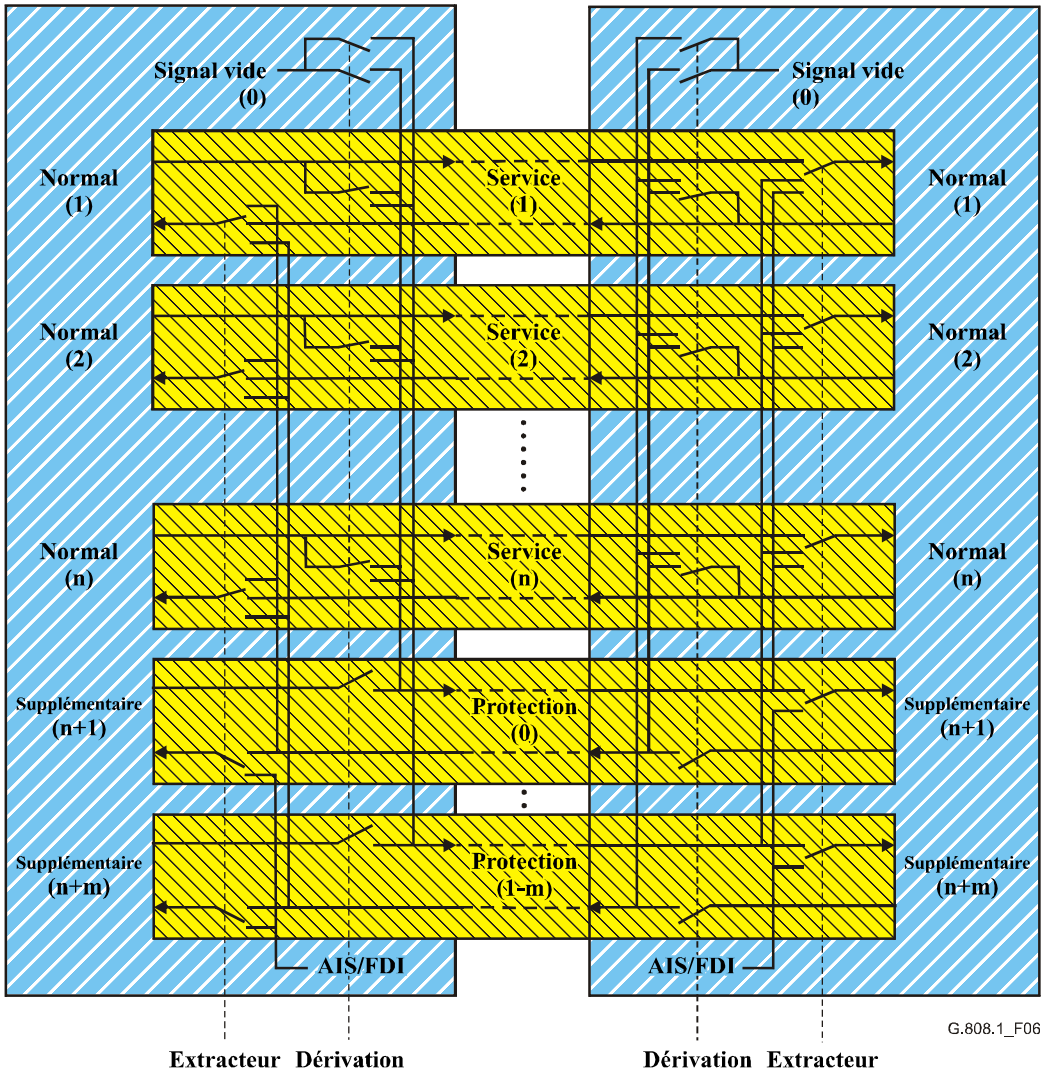


Option de dérivation sélective: signal de trafic normal connecté à entité de service ou de protection

Figure 5/G.808.1 – Architecture de protection 1:n

7.3 Architecture de protection m:n (multipartagée)

Dans le type d'architecture en m:n, m entités de transport en protection spécialisées se partagent des ressources de sécurisation pour n entités de transport en service, avec normalement m ≤ n. La largeur de bande de chaque entité de transport en protection devrait être attribuée de telle manière qu'il soit possible de protéger la totalité des n entités de transport en service dans le cas où au moins une des m entités de transport en protection est disponible. Lorsqu'une entité de transport en service est détectée comme étant dégradée, son signal de trafic normal doit d'abord être assigné à une entité de transport en protection disponible, puis faire l'objet d'une transition de l'entité de transport en service à l'entité de transport en protection assignée aux deux extrémités – source et collectrice – du domaine protégé. Il est noté que si plus de m entités de transport en service sont dégradées, seules m entités de transport en service peuvent être protégées. Voir la Figure 6.

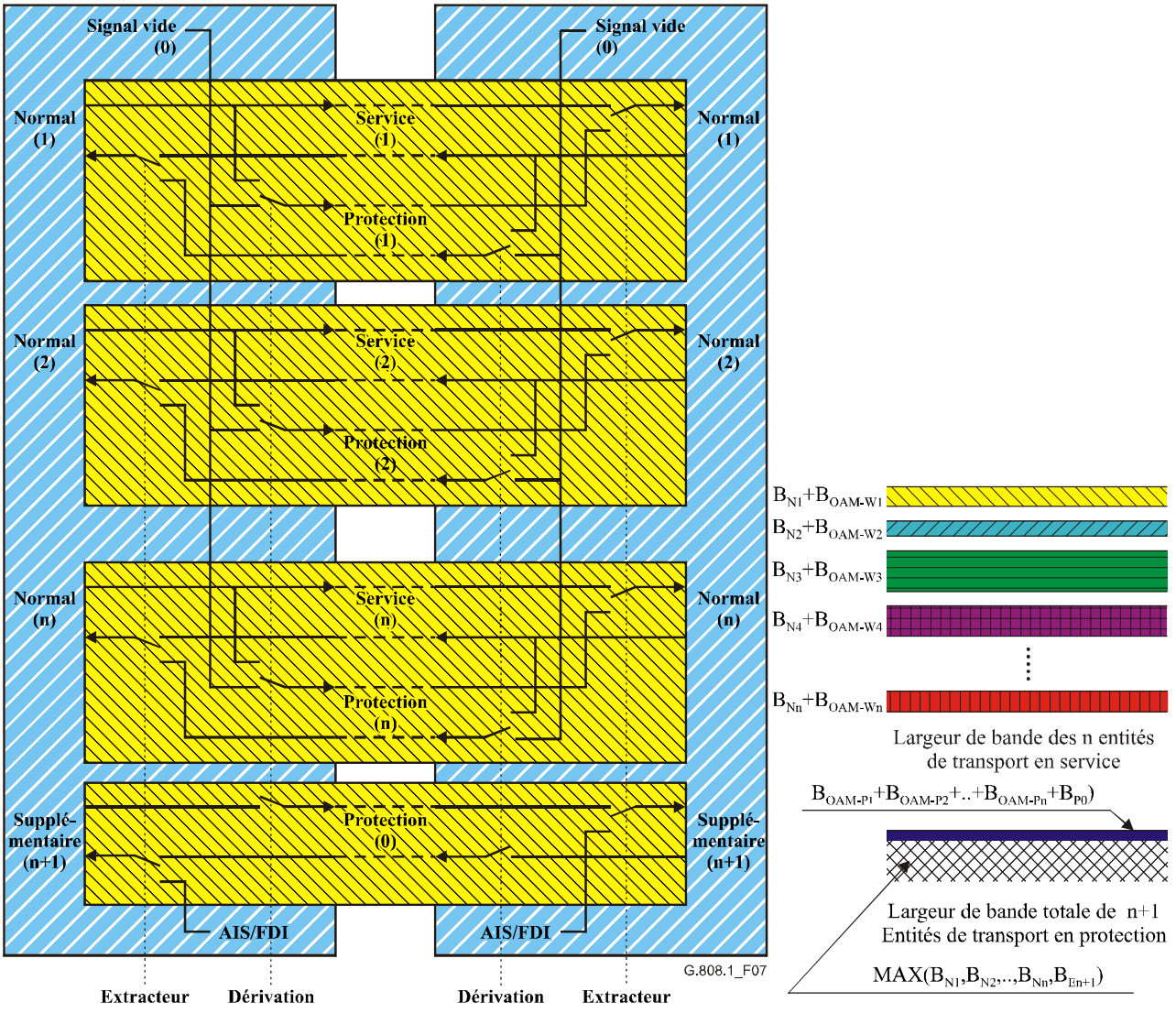


Option de dérivation divergente: signal de trafic normal connecté en permanence sur trafic et occasionnellement sur protection

Figure 6/G.808.1 – Architecture de protection m:n

7.4 Architecture de protection en $(1:1)^n$ (multidoublée)

Dans l'architecture de protection $(1:1)^n$ (multidoublée), n entités de transport en protection spécialisées, qui se partagent la même largeur de bande, sont des ressources de sécurisation pour n entités de transport en service. La largeur de bande de protection devrait être attribuée de telle manière qu'il soit possible de protéger la totalité des n entités de transport en service en cas de disponibilité de la largeur de bande de transport en protection et de l'entité de transport en protection spécifiquement associée à l'entité de transport en service à commuter. Lorsqu'une entité de transport en service est détectée comme étant dégradée, son signal de trafic normal doit d'abord être assigné à l'entité de transport en protection associée et disponible, puis faire l'objet d'une transition de l'entité de transport en service à l'entité de transport en protection assignée aux deux extrémités – source et collectrice – du domaine protégé. Il est noté que si plusieurs entités de transport en service sont dégradées, une seule entité de transport en service peut être protégée. Voir la Figure 7.



Option de dérivation divergente: signal de trafic normal connecté en permanence sur trafic et occasionnellement sur protection

Figure 7/G.808.1 – Architecture de protection à partage de largeur de bande $(1:1)^n$

Les "n" entités de transport en service sont toutes routées au moyen de différentes ressources et de différents équipements (afin d'éviter qu'un point de panne commun puisse ne pas être protégé). Les "n+1" entités de transport en protection sont toutes routées au moyen des mêmes ressources et des mêmes équipements, en plus des ressources et équipements de service. Voir un exemple à l'Appendice IV.

La largeur de bande occupée par chaque entité de transport en service est $B_{Wi} = B_{Ni}+B_{OAM-Wi}$; c'est-à-dire la largeur de bande du signal de trafic normal #i plus la largeur de bande de la connexion en cascade/du segment OAM utilisé afin de surveiller l'entité de transport en service #i. La largeur de bande occupée par les entités de transport en protection est $Bp = MAX(B_{N1},B_{N2},..,B_{Nn},B_{En+1}) + (B_{OAM-P1}+B_{OAM-P2}+..+B_{OAM-Pn}+B_{OAM-P0})$. Du point de vue de la largeur de bande, cette architecture de protection $(1:1)^n$ se comporte comme une architecture 1:n.

Une erreur de connexion d'un signal de trafic normal #i à l'entrée du domaine protégé, sur la sortie d'un signal de trafic normal #j ($j \neq i$) au départ du domaine protégé, ne peut pas se produire. Un protocole de commutation APS à 3 phases n'est pas requis en tant que tel.

Noter que cette architecture est destinée au trafic en mode paquet/cellule et non au trafic de type à débit constant.

8 Types de commutation

La commutation de protection peut être d'un des deux types suivants: unidirectionnelle ou bidirectionnelle.

En commutation **unidirectionnelle**, la commutation est complète lorsque le signal de trafic (service) est extrait de l'entité de transport en réserve à l'extrémité qui détecte le défaut. Dans le cas de l'architecture 1+1, seul l'extracteur situé à l'extrémité collectrice est actionné (sans communication avec l'extrémité source). Dans le cas des architectures 1:n, m:n et $(1:1)^n$, l'extracteur situé à l'extrémité collectrice et la dérivation située à l'extrémité source sont actionnés.

En commutation **bidirectionnelle**, le signal de trafic (service) est commuté à partir de l'entité de transport active vers l'entité de transport en réserve aux deux extrémités de l'arc de protection. Dans le cas de l'architecture 1+1, les extracteurs situés aux extrémités collectrice et source sont actionnés. Dans le cas des architectures 1:n, m:n et $(1:1)^n$, les extracteurs et les dérivations situés aux extrémités collectrice et source sont actionnés.

NOTE 1 – Tous les types de commutation sauf la commutation 1+1 unidirectionnelle, nécessitent un canal de communication entre les deux extrémités du domaine protégé; ce canal est appelé *canal de commutation automatique de protection* (APS, *automatic protection switching*). Le canal de commutation APS aboutit aux fonctions de connexion situées à chaque extrémité du domaine protégé.

Dans les protocoles de commutation bidirectionnelle, la commutation (actionnement d'extracteur et de dérivation) à une seule extrémité n'est pas autorisée. Les deux extrémités communiquent afin de lancer le transfert du signal de trafic normal. Si la priorité de la requête de l'extrémité source est inférieure à celle de l'extrémité collectrice ou n'existe pas, l'extrémité collectrice lance le transfert du signal de trafic normal et l'extrémité source se conforme à ce transfert.

Dans le type de commutation unidirectionnelle, les avantages possibles sont les suivants:

1) la commutation unidirectionnelle est un procédé simple à implémenter, qui n'exige pas de protocole dans une architecture 1+1.

   NOTE 2 – La commutation unidirectionnelle en architecture alternée (normalement appliquée dans les liaisons par radio/satellite) nécessite le fonctionnement d'un protocole entre les deux extrémités du domaine protégé.

2) Dans une architecture 1+1, la commutation unidirectionnelle peut être plus rapide que la commutation de protection bidirectionnelle parce qu'elle n'exige pas de protocole.

3) En condition de pannes multiples, il y a une plus grande probabilité de restaurer le trafic par commutation de protection si la commutation unidirectionnelle est utilisée plutôt que la commutation de protection bidirectionnelle.

4) La commutation unidirectionnelle permet une réalisation simple d'un réseau fiable au moyen d'une cascade de sous-réseaux protégés. Deux sous-réseaux sont connectés dans une architecture d'interconnexion de paires de nœuds/interfonctionnement de paires de sous réseaux.

Dans le type de commutation bidirectionnelle, les avantages possibles sont les suivants:

1) en commutation de protection bidirectionnelle, le même équipement est utilisé dans les deux sens de transmission après une panne. C'est-à-dire qu'il y aura moins d'interruptions du service pour réparation et retour au trajet de service original. En commutation unidirectionnelle, les commutations suivantes se produisent:

   i) commutation de protection;

   ii) commutation forcée dans le sens non affecté par la panne;

   iii) commutation réversible.

En commutation bidirectionnelle, seules deux commutations se produiront:

i) commutation de protection;

ii) commutation réversible.

Chaque commutation se traduira par 1 ou 2 secondes gravement erronées (SES, *severely errored second*). Un moindre nombre de secondes SES résultera d'une commutation bidirectionnelle.

2) En commutation de protection bidirectionnelle, s'il y a un défaut dans une entité de transport du réseau, la transmission des deux entités de transport entre les nœuds affectés est commutée en boucle dans l'autre sens du réseau. Aucun trafic n'est donc transmis sur la section défectueuse du réseau, qui peut donc être réparée sans autre commutation de protection.

3) La commutation de protection bidirectionnelle est plus facile à gérer parce que les deux sens de transmission utilisent le même équipement sur toute la longueur de l'entité de transport.

4) La commutation de protection bidirectionnelle maintient des temps de propagation égaux dans les deux sens de transmission, ce qui peut être important lorsqu'il y a une nette différence de longueur entre les entités de transport, par exemple dans les liaisons intercontinentales où une des entités de transport utilise une liaison par satellite et l'autre une liaison par câble.

5) La commutation de protection bidirectionnelle permet également de transporter du trafic supplémentaire sur l'entité de transport en protection.

9 Types de fonctionnement

Le fonctionnement en protection peut être de type irréversible ou réversible.

En fonctionnement **réversible**, le signal de trafic (service) revient toujours à l'entité de transport en service (ou y reste toujours) si les requêtes de commutation sont terminées, c'est-à-dire lorsque l'entité de transport en service s'est rétablie après le défaut ou lorsque la requête externe est relevée.

En fonctionnement **irréversible**, le signal de trafic (service) ne revient pas à l'entité de transport en service si les requêtes de commutation sont terminées.

Certains procédés de sécurisation sont intrinsèquement réversibles. Dans d'autres procédés, un fonctionnement réversible ou irréversible est possible. Un avantage du fonctionnement irréversible est qu'en général il aura moins d'influence sur la capacité d'écoulement du trafic. Il y a cependant des situations où un fonctionnement réversible peut être préféré. Exemples de cas où un fonctionnement réversible peut être approprié:

1) lorsque des parties de l'entité de transport en protection peuvent être réservées afin de fournir la capacité de répondre à un besoin plus urgent. Par exemple lorsque l'entité de transport en protection peut être mise hors service afin de libérer de la capacité à utiliser et de restaurer un autre trafic;

2) lorsque l'entité de transport en protection peut être soumise à de fréquents repositionnements. Par exemple, lorsqu'un réseau a une capacité limitée et que les itinéraires de protection sont fréquemment repositionnés afin de maximiser l'efficacité du réseau si des modifications se produisent dans le réseau;

3) lorsque l'entité de transport en protection est de qualité nettement inférieure par rapport à l'entité de transport en service. Par exemple si l'entité de transport en protection a, par rapport à l'entité de transport en service, une moins bonne qualité en termes d'erreurs ou un temps de propagation plus long;

4) lorsqu'un opérateur a besoin de savoir quelles entités de transport sont en train de transporter du trafic normal afin de simplifier la gestion du réseau.

10 Types de protocole

Sauf dans le cas de la commutation 1+1 unidirectionnelle, tous les types de protection nécessitent que les deux extrémités, A et Z, du domaine protégé coordonnent leurs actions de dérivation et d'extraction. Différents protocoles sont requis, selon le type de protection et les types d'extracteur et de dérivation. Les nœuds A et Z communiquent donc l'un avec l'autre au moyen du canal de commutation automatique de protection (APS).

Il y a deux exigences de base pour un protocole de protection:

1) la prévention des erreurs de connexion;

2) la minimisation du nombre de cycles de communication entre les extrémités A et Z du domaine protégé afin de minimiser le temps de commutation sur protection. La communication peut avoir lieu une seule fois (Z → A), deux fois (Z → A et A → Z), ou trois fois (Z → A, A → Z et Z→ A), ce qui est appelé *protocole à 1 phase, à 2 phases ou à 3 phases.*

Les conditions dans lesquelles les différents types de protocole peuvent être utilisés sont indiquées dans le Tableau 1.

Tableau 1/G.808.1 – Types de protocole associés aux types d'architecture de protection et d'extracteur/de dérivation

Type de protocole	Types de protection utilisant un protocole	Type de dérivation	Type d'extracteur
Aucun protocole	1+1 unidirectionnelle	Permanente	Divergent
1 phase	$(1:1)^n$ unidirectionnelle	Par extracteur	Divergent ou convergent
	Architectures en 1 + 1 seulement	Permanente	Divergent
2 phases	$(1:1)^n$ unidirectionnelle	Par extracteur	Divergent ou convergent
	Architectures en 1+1 seulement	Permanente	Divergent
3 phases	Tous types d'architecture	Tout type	Divergent
		Par extracteur	Convergent (techniques en mode cellule/paquet)

Le type de protocole à trois phases offre les avantages possibles suivants:

1) il fonctionne dans tout type d'architecture;

2) il empêche l'apparition d'une erreur de connexion en toutes circonstances;

3) il n'actionne un extracteur ou une dérivation qu'après confirmation de priorité avec l'autre extrémité du domaine protégé.

Dans le type de protocole à trois phases, les inconvénients possibles sont les suivants:

4) un triple échange de messages est nécessaire entre deux extrémités de domaine protégé, ce qui augmente le temps de commutation.

Le type de protocole à deux phases offre les avantages possibles suivants:

1) temps de commutation réduit par rapport au protocole à trois phases;

2) fonctionne dans les architectures en 1+1 et $(1:1)^n$.

Le type de protocole à une phase offre les avantages possibles suivants:

1) temps de commutation court, étant donné qu'un seul échange de messages est nécessaire entre deux extrémités de domaine protégé;

2) fonctionne dans les architectures en 1+1 et en $(1:1)^n$.

Le type de protocole à une phase offre les inconvénients possibles suivants:

3) il nécessite l'établissement de "n" entités de transport supplémentaires (par rapport à l'architecture alternée) dans la largeur de bande de protection, afin d'éviter l'apparition d'erreurs de connexion;

4) il actionne une dérivation/un extracteur avant que la priorité soit confirmée par l'autre extrémité du domaine protégé. En tant que telle, une action de commutation peut devoir être inversée et remplacée par une autre action de dérivation/d'extraction lancée par l'autre extrémité;

5) il est plus complexe car il y a "n" types de protection 1:1 parallèles.

11 Classes et sous-classes de protection

11.1 Protection de chemin

La protection de chemin est une classe de protection servant à protéger un chemin dans un réseau d'opérateur entier ou dans de multiples réseaux d'opérateur. C'est une architecture de protection spécialisée de bout en bout qui peut être utilisée dans différentes structures de réseau: réseaux maillés, anneaux, etc. Comme la protection de chemin est un mécanisme de protection spécialisée, il n'y a aucune limitation fondamentale du nombre d'éléments de réseau dans les chemins.

La protection de chemin fonctionne dans toutes les combinaisons d'architecture de protection, de commutation et de fonctionnement.

La protection de chemin offre une protection générique contre les défauts dans la couche serveur, ainsi que contre les défauts de connexité et les dégradations de qualité dans la couche client.

Dans le cas de la protection de chemin, l'information adaptée (AI, *adapted information*) (c'est-à-dire la charge utile de l'information caractéristique (CI, *characteristic information*) de la couche de réseau) est protégée. Voir la Figure 8.

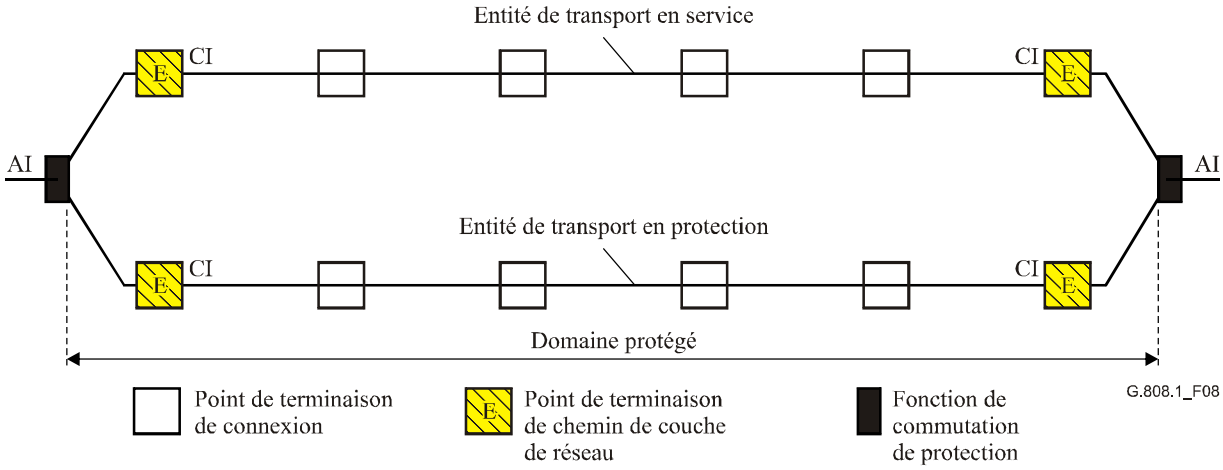


Figure 8/G.808.1 – Concept générique de protection de chemin

NOTE 1 – Etant donné que les protections de chemin en 1:1, en 1:n et en m:n sont des mécanismes de protection linéaire, les fonctions de terminaison de chemin pour trafic normal et trafic supplémentaire sont situées dans le même élément de réseau. Dans une application de réseau, cela implique que les structures de trafic normal et de trafic supplémentaire doivent toujours coïncider.

La protection de chemin ne prend pas en charge les architectures de réseau qui font appel à des sous-réseaux protégés en cascade dans la même couche. Par conséquent, le trafic ne peut être rétabli qu'en condition de défaut isolé. Afin de rétablir le trafic en condition de défaut multiple, la protection de connexion SNC doit être utilisée, ou la protection de chemin doit être complétée par une protection au niveau des couches serveur.

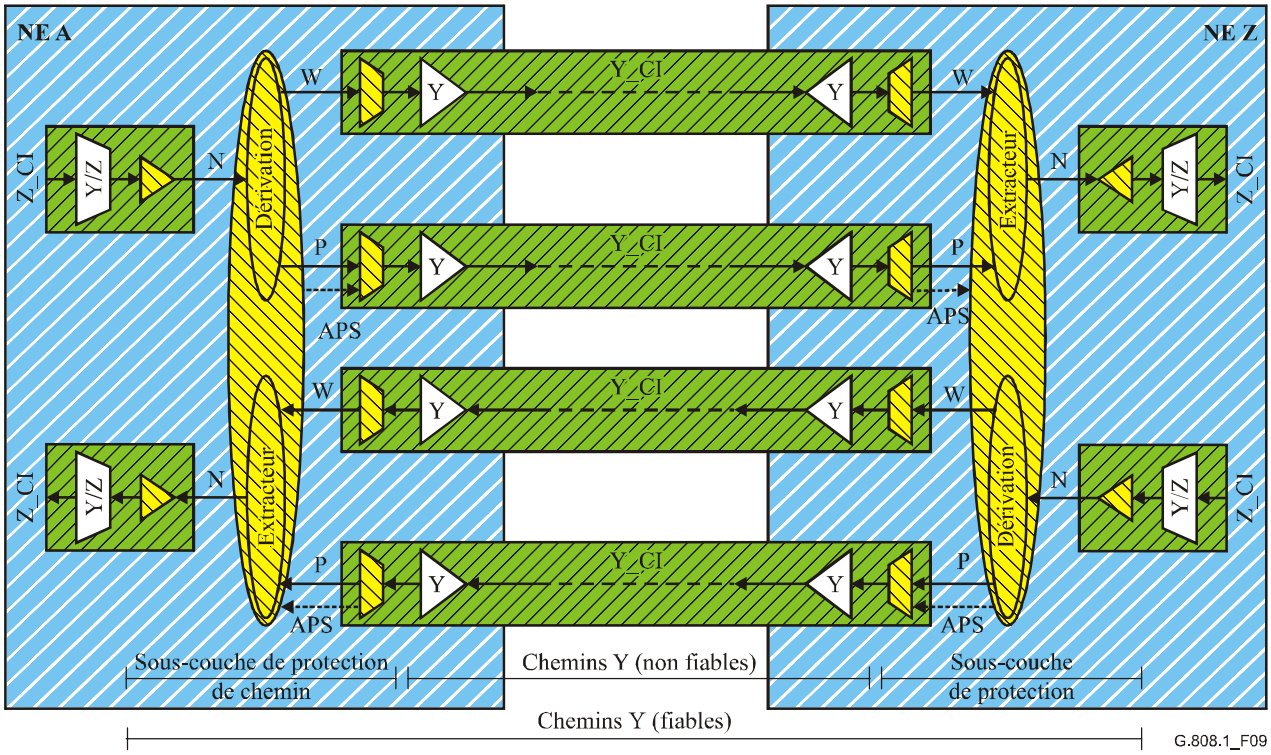
NOTE 2 – Dans le cas d'une architecture en 1:1, m:n ou $(1:1)^n$ dans un réseau en mode ATM, le ou les chemins de protection devraient contenir un signal permettant une surveillance précise de leur état. En condition de trafic normal, où le signal de trafic normal est transporté au moyen du chemin de service, il n'y a aucun signal à transporter au moyen des entités de protection. Si le contrôle de continuité (CC) est inactif, un tel chemin de protection ne transportera pas d'informations en condition normales d'absence de défaut. Lorsqu'un défaut se produit, des cellules de signal AIS sont insérées. Lorsque le défaut n'est présent que pendant une brève période (par exemple, en raison d'une "action de protection dans la couche Physique"), le détecteur de défaut AIS situé à l'extrémité du chemin de protection détectera la condition de défaut AIS pendant 2 à 3 secondes conformément à la définition de l'état AIS figurant dans la Rec. UIT-T I.610. Si le contrôle CC est activé, la condition de défaut AIS sera relevée dès réception d'une cellule CC, c'est-à-dire dans une période de 1 s après que l'interruption de trafic a été relevée.

NOTE 3 – Si la protection de chemin est utilisée au niveau d'un conduit, il peut en résulter la prise en charge d'un accès supplémentaire dans une matrice de commutation par rapport à la protection de connexion SNC. C'est le cas lorsque l'extracteur de protection est situé dans l'accès de sortie de l'équipement.

11.1.1 Protection de chemin individuel

La Figure 9 décrit le cas de la protection 1+1 (doublée) de chemin et de la protection 1:1 (alternée) de chemin sans trafic supplémentaire entre arrivée et départ du domaine protégé entre les éléments de réseau A et Z. Deux chemins indépendants existent (dans la couche de réseau Y) et jouent le rôle d'entités de transport en service et en protection pour le signal (protégé) de (charge utile de) trafic normal. Les fonctions de terminaison de chemin (TT) produisent/insèrent et surveillent/extraient les informations de flux OAM/de surdébit d'extrémité à extrémité afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur le chemin de protection, sauf dans le cas de la commutation 1+1 unidirectionnelle.

Le cas des architectures en 1:n, m:n et $(1:1)^n$ avec/sans trafic supplémentaire sont des extensions de l'architecture 1+1/1:1, conformément aux descriptions des types d'architecture du § 7.



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 9/G.808.1 – Modèle fonctionnel de protection de chemin en 1+1/1:1

11.1.2 Protection de groupe de chemins

La Figure 10 décrit le cas de la protection 1+1/1:1 d'un groupe de chemins entre éléments de réseau A et Z. Dans cet exemple, deux fois trois chemins indépendants parallèles existent (dans la couche de réseau Y) et jouent le rôle de groupes d'entités de transport en service et en protection pour les trois signaux (protégés) de (charge utile de) trafic normal. Les trois signaux parallèles de trafic normal dans le groupe sont protégés conjointement par la fonction de connexion de sous-couche de protection de chemin. Les fonctions de terminaison d'extrémité (TT) produisent/insèrent et surveillent/extraient les informations de flux OAM/de surdébit d'extrémité à extrémité afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur un des chemins de protection, sauf dans le cas de la commutation 1+1 unidirectionnelle.

Le cas des architectures en 1:n, m:n et $(1:1)^n$ avec/sans trafic supplémentaire sont des extensions de l'architecture 1+1/1:1, conformément aux descriptions des types d'architecture du § 7.

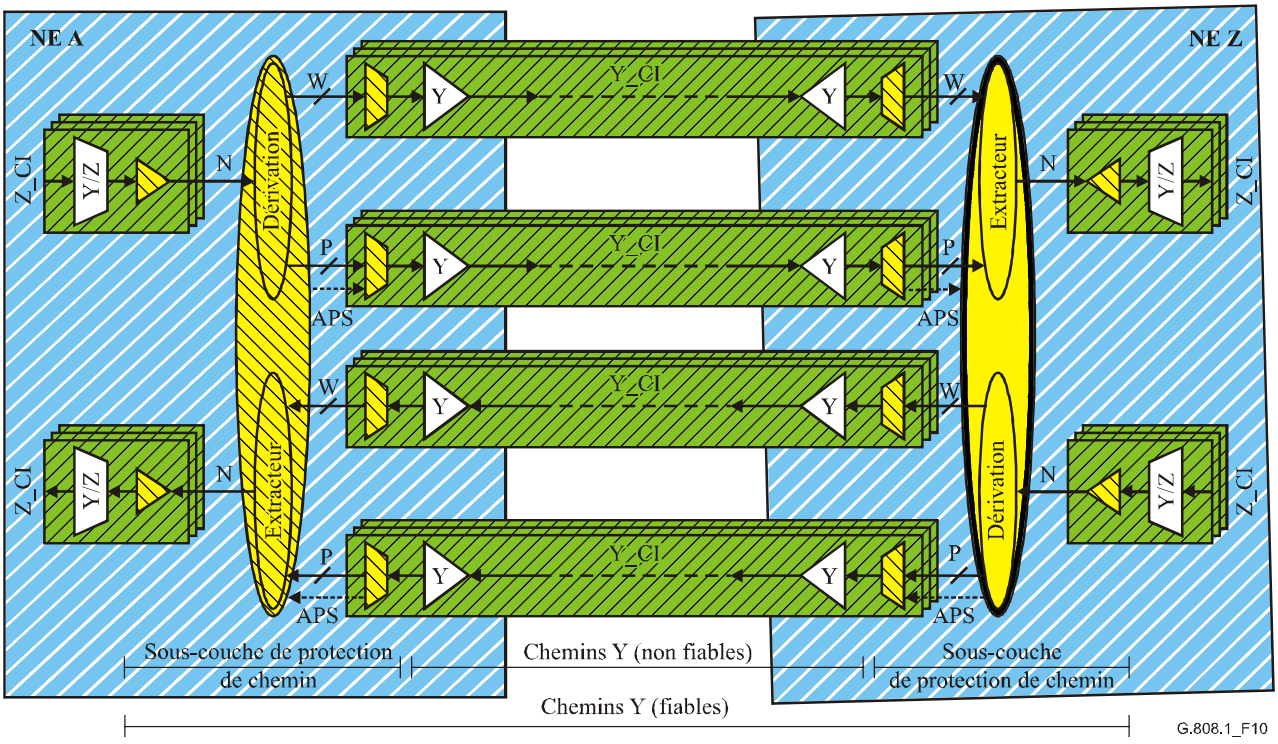


Figure 10/G.808.1 – Modèle fonctionnel de protection de groupe de chemins en 1+1/1:1

La Figure 11 présente des détails supplémentaires sur ces processus de fonction de connexion de protection. Le processus logique de groupe SFG/SDG est spécifique pour la protection de groupe. Ce processus "fusionne" les trois signaux individuels de défaillance de signal d'un chemin (TSF, *trail signal fail*) en une seule défaillance de signal de groupe (SFG, *signal fail group*) et les signaux individuels de dégradation de signal d'un chemin (TSD, *trail signal degrade*) en un seul groupe de dégradations de signal (SDG, *signal degrade groups*).

La logique de groupe SFG/SDG peut fonctionner dans différents modes:

- W-SFG = W1-TSF ou W2-TSF ou W3-TSF
  P-SFG = P1-TSF ou P2-TSF ou P3-TSF;
- W-SFG = W1-TSF
  P-SFG = P1-TSF;
- W-SFG = X% des signaux Wi-TSF sont actifs
  P-SFG = X% des signaux Pi-TSF sont actifs;
- idem pour SDG.

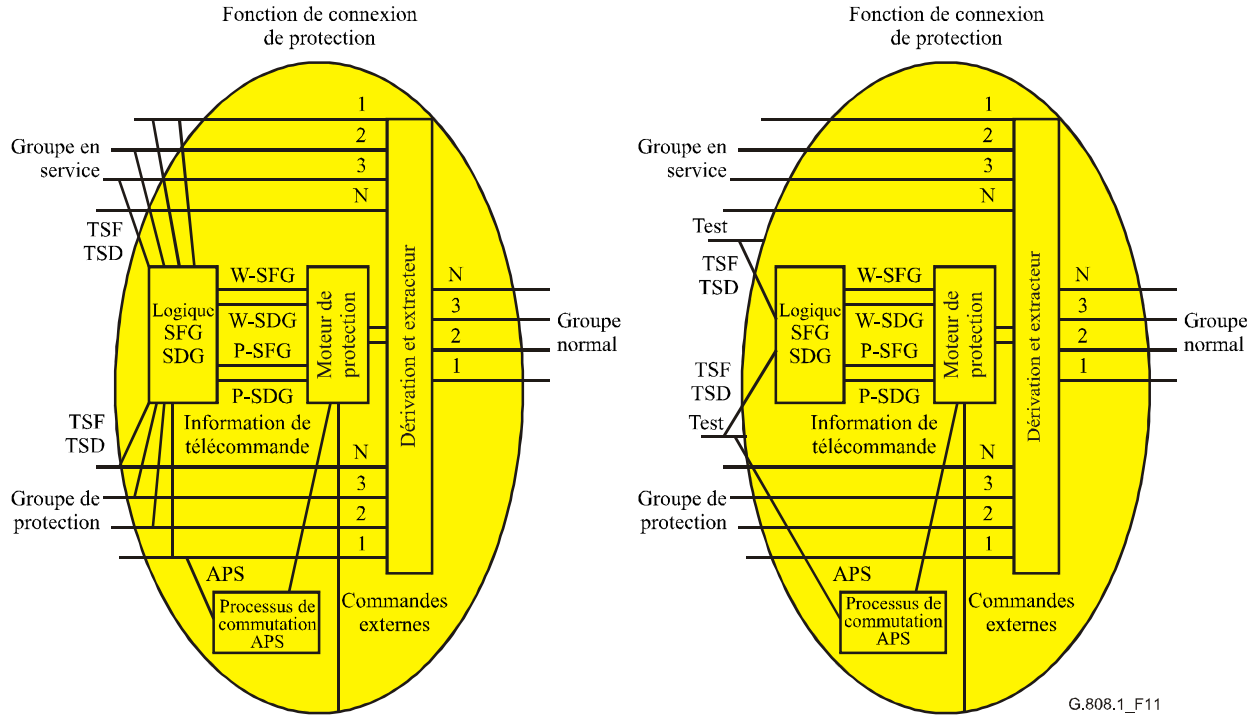


Figure 11/G.808.1 – Logique de groupe SFG/SDG dans un processus de protection de groupe

Compte tenu du grand nombre d'affluents élémentaires dans certaines techniques de transmission (par exemple en mode ATM), des affluents élémentaires supplémentaires peuvent être attribués dans les signaux de couche serveur en service et en protection afin de transporter des signaux d'essai au moyen d'entités de transport expérimentales (Figures 12, 13). Ces signaux d'essai (un par entité de service, un par entité de protection) peuvent être utilisés à la place des informations de groupe SFG/SDG comme décrit ci-dessus. Le signal de commutation APS est transporté au moyen de l'entité de transport en protection expérimentale.

La logique de groupe SFG/SDG fonctionne donc comme suit:

- W-SFG = Wt-TSF
  P-SFG = Pt-TSF;
- W-SDG = Wt-TSD
  P-SDG = Pt-TSD.

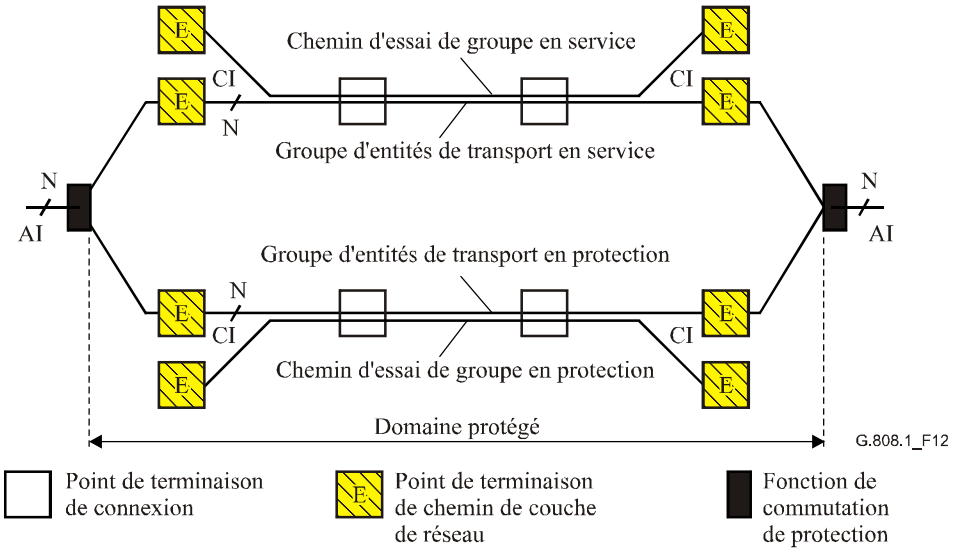


Figure 12/G.808.1 – Concept générique de protection de chemin/T groupé

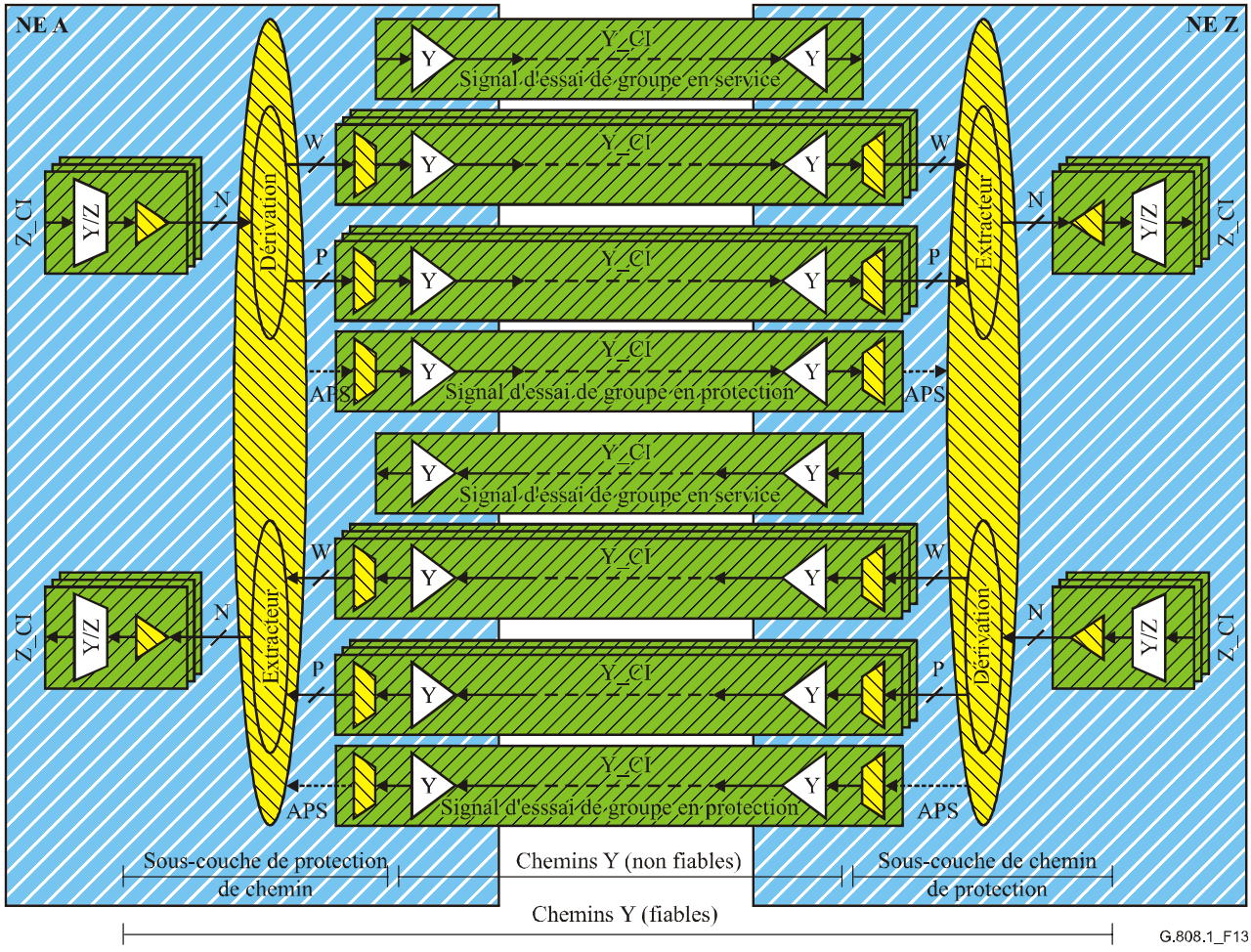


Figure 13/G.808.1 – Modèle fonctionnel de la protection en 1+1/1:1 de chemin/T groupé

11.2 Protection de connexion SNC

La protection de connexion SNC est la classe de protection qui sert à protéger une portion d'un chemin (par exemple, celle où deux routes distinctes sont disponibles) dans un réseau d'opérateur ou dans des réseaux d'opérateurs multiples.

La connexion de sous-réseau qui est protégée peut être établie entre deux points de connexion (CP, *connection point*) (Figure 14), entre un point CP et un point de connexion de terminaison (TCP, *termination connection point*) (Figure 15), ou peut être la chaîne de connexion de bout en bout du réseau entre deux points TCP (Figure 16).

Etant donné que la protection de connexion SNC est un mécanisme de protection spécialisée, celui-ci peut être utilisé dans toute structure physique (c'est-à-dire dans un réseau maillé, dans un réseau annulaire ou dans un réseau mixte). Il n'y a aucune limitation théorique quant au nombre d'éléments de réseau contenus dans la connexion de sous-réseau. Ce mécanisme peut être appliqué à une couche quelconque d'un réseau stratifié.

La protection de connexion SNC fonctionne dans toutes les combinaisons d'architecture de protection, de commutation et de fonctionnement.

La protection SNCP peut être encore subdivisée en sous-classes qui représentent les conditions de défaut qui contribuent à une panne SF/SD:

1) protection à surveillance intrinsèque: les fonctions de terminaison et d'adaptation de chemin de couche serveur servent à déterminer la condition de signal SF/SD. Elle ne prend en charge que la détection de conditions de défaut dans la couche serveur;
2) protection à surveillance non intrusive: des fonctions de surveillance non intrusive sont déployées afin de déterminer la condition de signal SF/SD;
    a) de bout en bout: détection de conditions de défaut dans la couche serveur, de conditions de défaut de continuité/connexité dans la couche de réseau, et de conditions de dégradation en terme d'erreurs dans la couche de réseau. Le flux OAM/surdébit de bout en bout est utilisé;
    b) de sous-couche: détection de conditions de défaut dans la couche serveur, de conditions de défaut de continuité/connexité dans la couche de réseau, et de conditions de dégradation en termes d'erreurs dans la couche de réseau. Le flux OAM/surdébit de sous-couche est utilisé;
3) protection à surveillance de sous-couche: des fonctions de sous-couche de connexions en cascade/de segments sont déployées afin de déterminer la condition de signal SF/SD. Elle prend en charge la détection de conditions de défaut dans la couche serveur, de conditions de défaut de continuité/connexité dans la couche de réseau, et de conditions de dégradation en termes d'erreurs dans la couche de réseau. Le flux OAM/surdébit de sous-couche est utilisé.

En général, la protection de connexion SNC nécessite la création de chemins de sous-couche (connexions en cascade, segments) dans les entités de transport en service et en protection afin de distinguer si un défaut ou une dégradation se produit "en face" par rapport à "l'intérieur" du domaine protégé. Lorsque le chemin de sous-couche se réduit à un seul chemin de couche serveur, ce chemin (fournissant une surveillance intrinsèque) peut être utilisé comme chemin de sous-couche. Si un chemin de sous-couche ne peut pas être créé ou si un seul chemin de couche serveur n'est pas disponible entre les points d'arrivée et de départ du trafic du domaine protégé, la protection de connexion SNC peut être réalisée par double injection du signal de trafic normal dans les deux entités de transport (service et protection), par surveillance non intrusive des deux copies du signal au point de départ et par comparaison de l'état SF/SD obtenu à partir des deux moniteurs. Si le défaut ou la dégradation s'est produit en face du domaine protégé, les deux moniteurs (service et protection) détecteront la dégradation et une action de commutation ne sera pas effectuée. Sinon,

un seul des deux moniteurs détectera une condition de signal SF/SD et le flux de trafic pourra être rétabli au moyen d'une action de commutation.

NOTE 1 – En hiérarchie SDH, en raison du traitement des pointeurs d'unité AU/TU en condition de panne TSF dans la couche serveur, une protection SNC/I de type 1+1 peut être déployée à la place de la protection SNC/N de type 1+1 si seuls des défauts de couche serveur doivent faire l'objet d'une protection.

Dans le cas de la protection de connexion SNC, l'information caractéristique (CI) (c'est-à-dire la charge utile et son surdébit de couche) est protégée. Voir les Figures 14 à 17.

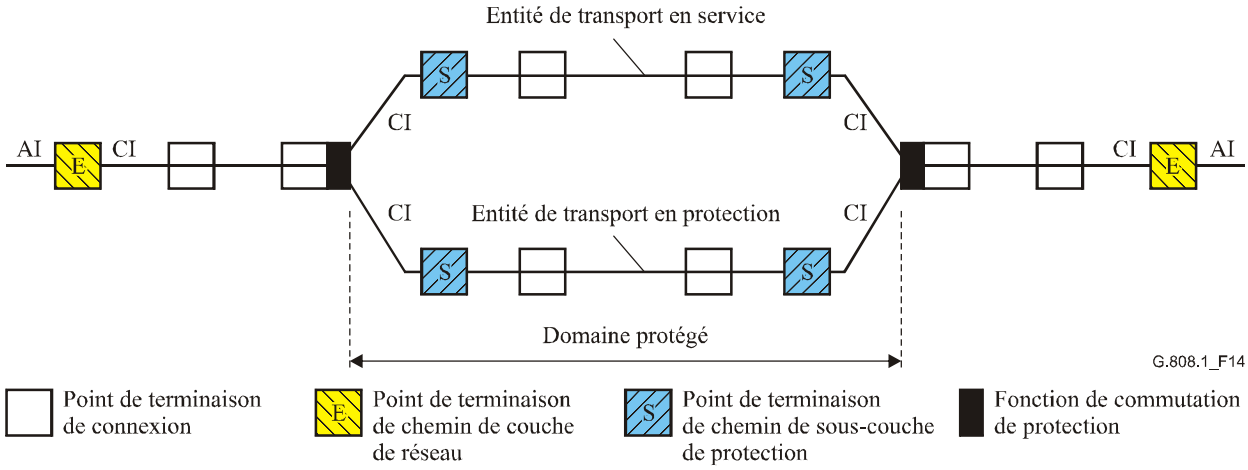


Figure 14/G.808.1 – Protection SNC/S – Exemple 1

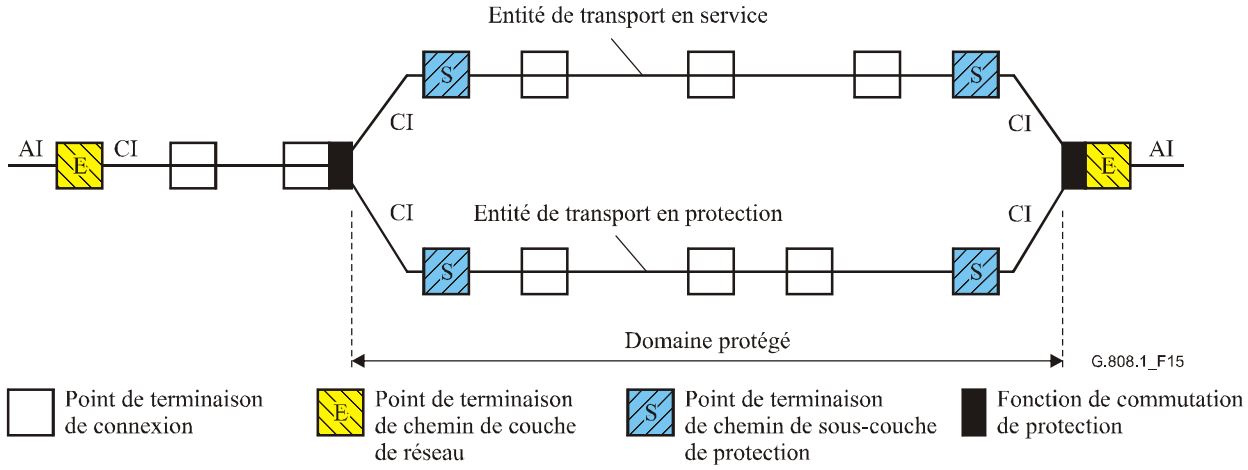


Figure 15/G.808.1 – Protection SNC/S – Exemple 2

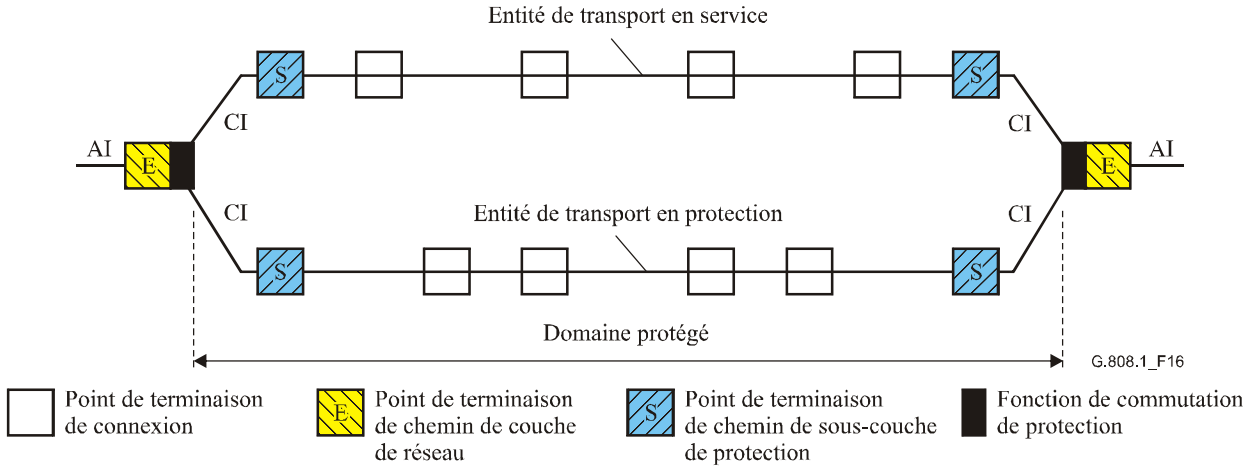


Figure 16/G.808.1 – Protection SNC/S – Exemple 3

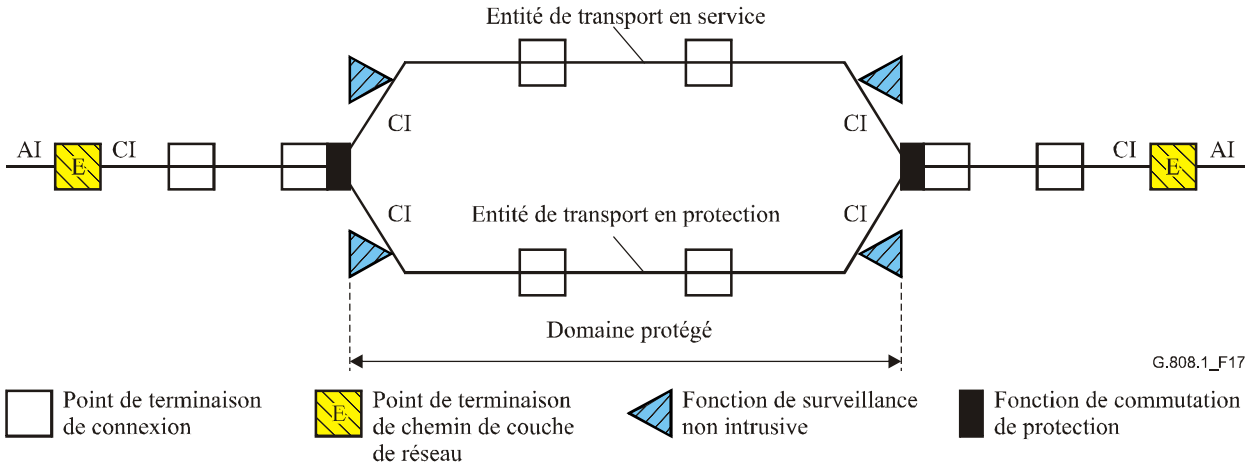


Figure 17/G.808.1 – Protection SNC/N de type 1+1

La protection de connexion SNC prend en charge les architectures de réseau qui font appel à des sous-réseaux protégés en cascade. De telles architectures de réseau sont en mesure de rétablir le trafic en cas de multiples défauts (un seul défaut par sous-réseau protégé); voir la Figure 18.

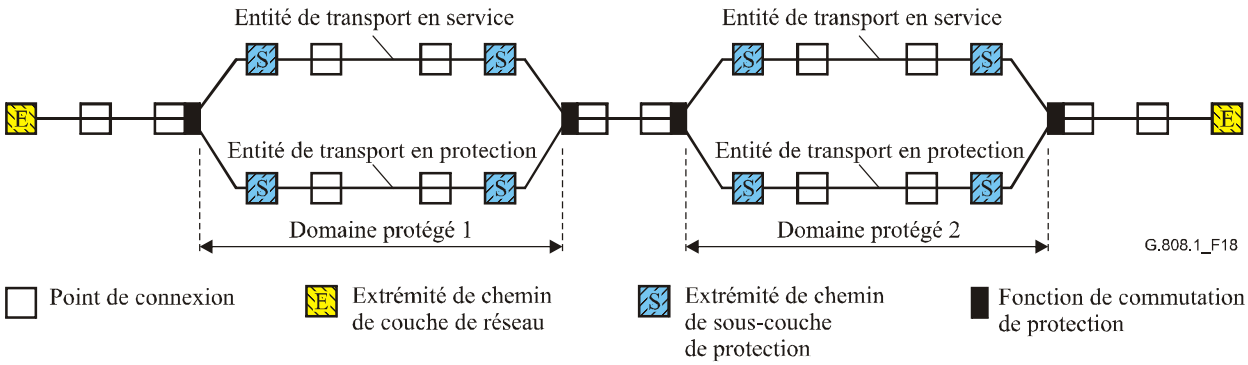


Figure 18/G.808.1 – Protection SNC/S en cascade

La tolérance aux défauts (et la fiabilité) des sous-réseaux protégés par SNC en cascade est augmentée lorsque l'interconnexion entre les sous-réseaux est doublée (Figure 19), le seul point de panne étant supprimé. Cette protection nécessite l'utilisation des types de protection 1+1, SNC/N commutée dans un seul sens ou SNC/I. L'utilisation de la commutation en 1:n, m:n, $(1:1)^n$ et/ou de la commutation bidirectionnelle n'est pas possible.

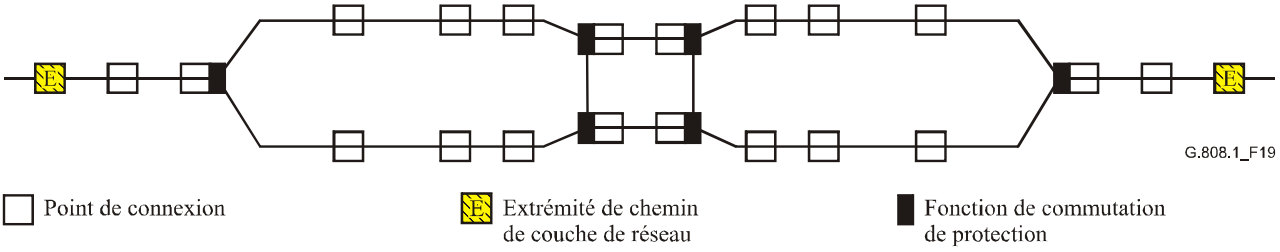


Figure 19/G.808.1 – Protection en série de connexion SNC de type 1+1 avec interconnexion d'un sous-réseau tolérant les défauts

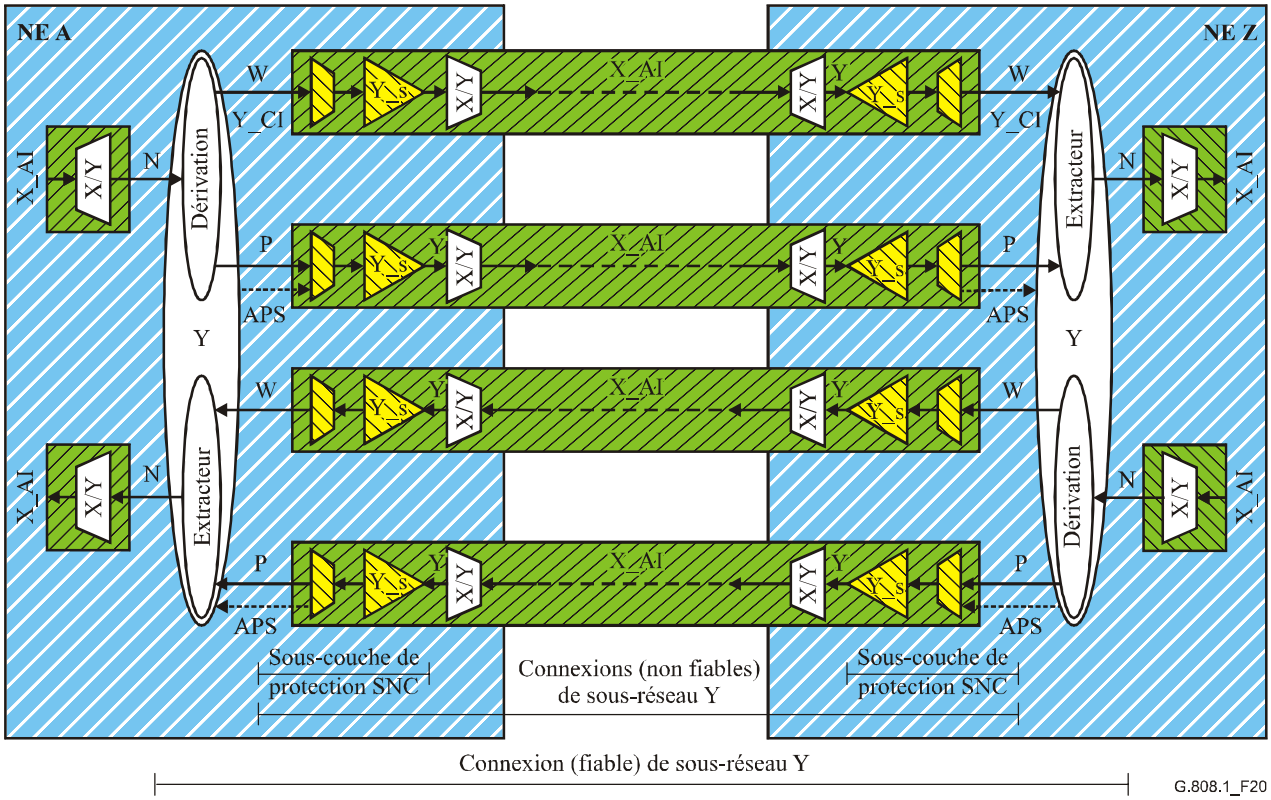
NOTE 2 – Dans le cas d'une architecture 1:1, m:n ou $(1:1)^n$ architecture dans un réseau en mode ATM, la ou les connexions de sous-réseau de protection devraient contenir un signal permettant une surveillance précise de son état. En condition de trafic normal, où le signal de trafic normal est transporté au moyen de la connexion SNC de service, il y a absence de signal à transporter en protection. Si le contrôle CC est inactif, une telle protection SNC ne transportera pas d'informations en condition normales d'absence de défaut. Lorsqu'un défaut se produit, des cellules de signal AIS sont insérées. Lorsque le défaut n'a été présent que pendant une brève période (par exemple, en raison d'une "action de protection dans la couche Physique"), le détecteur de défaut AIS à l'extrémité du segment de protection détectera la condition de défaut AIS pendant 2 à 3 secondes conformément à la définition de l'état AIS figurant dans la Rec. UIT-T I.610. Avec le contrôle CC activé, la condition de défaut AIS est relevée dès réception d'une cellule CC, c'est-à-dire dans une période de 1 seconde après que l'interruption de trafic a été relevée.

11.2.1 Protection de connexion SNC individuelle

11.2.1.1 Protection SNC/S de types 1+1, 1:n, m:n, $(1:1)^n$

La Figure 20 décrit le cas de la protection SNC/S de types 1+1 et 1:1 sans trafic supplémentaire entre entrée et sortie du domaine protégé entre éléments de réseau A et Z. Deux chemins de sous-couche indépendants existent et jouent le rôle d'entités de transport en service et en protection pour le signal (protégé) de trafic normal. Les fonctions TT de sous-couche produisent/insèrent et surveillent/extraient le flux OAM/surdébit des informations de sous-couche afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur la protection SNC, sauf dans le cas de la commutation 1+1 unidirectionnelle.

Les cas des architectures en 1:n, m:n et $(1:1)^n$ avec/sans trafic supplémentaire sont des extensions de l'architecture 1+1/1:1, conformément aux descriptions des types d'architecture du § 7.



NOTE – Le signal de commutation APS n'est pas aplicable au cas de la commutation 1+1 unidirectionnelle.

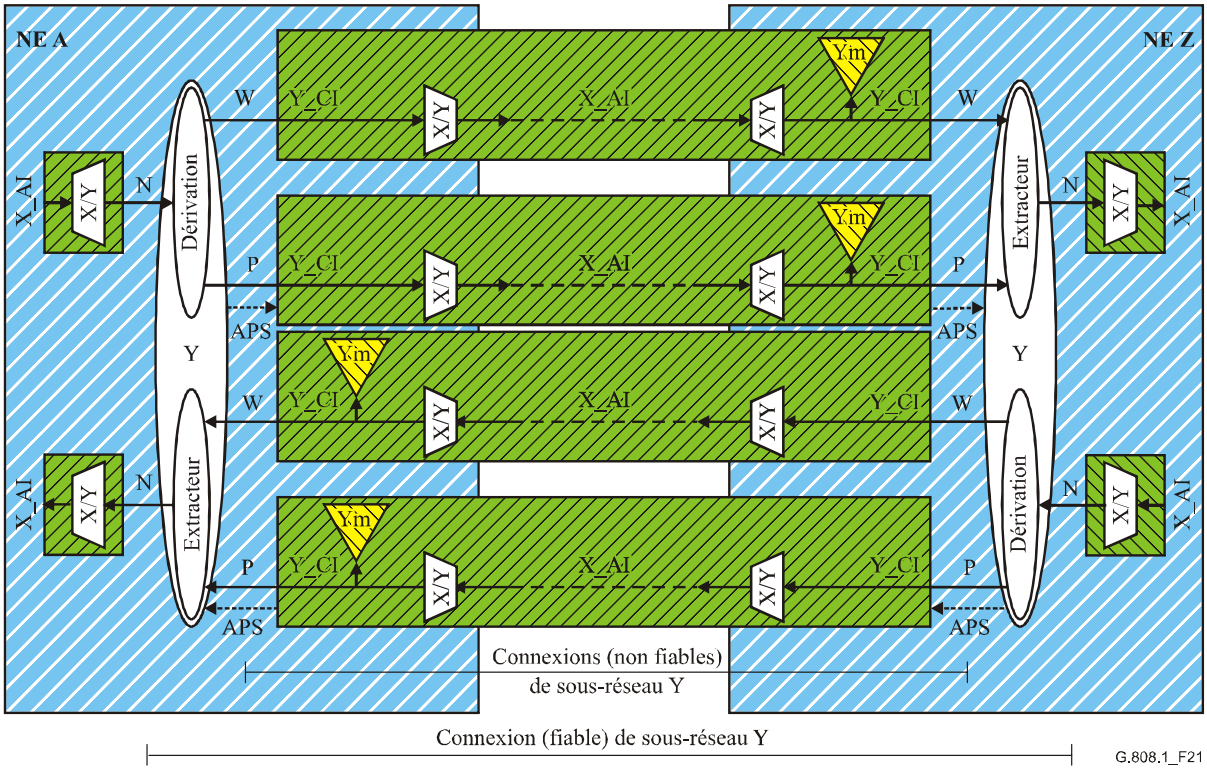
Figure 20/G.808.1 – Modèle fonctionnel de la protection SNC/S en 1+1/1:1

NOTE – Les fonctions de terminaison de chemin de sous-couche (par exemple, les fonctions de connexion en cascade/terminaison de segment) sont utilisées à des fins administratives (afin de surveiller la qualité de service du transport dans le domaine de réseau administratif) et à des fins de protection pour lesquelles l'emplacement des terminaisons de chemin de sous-couche est conforme aux figures relatives à la protection SNC/S. A des fins administratives, l'emplacement optimal est de l'autre côté de la fonction de connexion.

11.2.1.2 Protection SNC/N de type 1+1

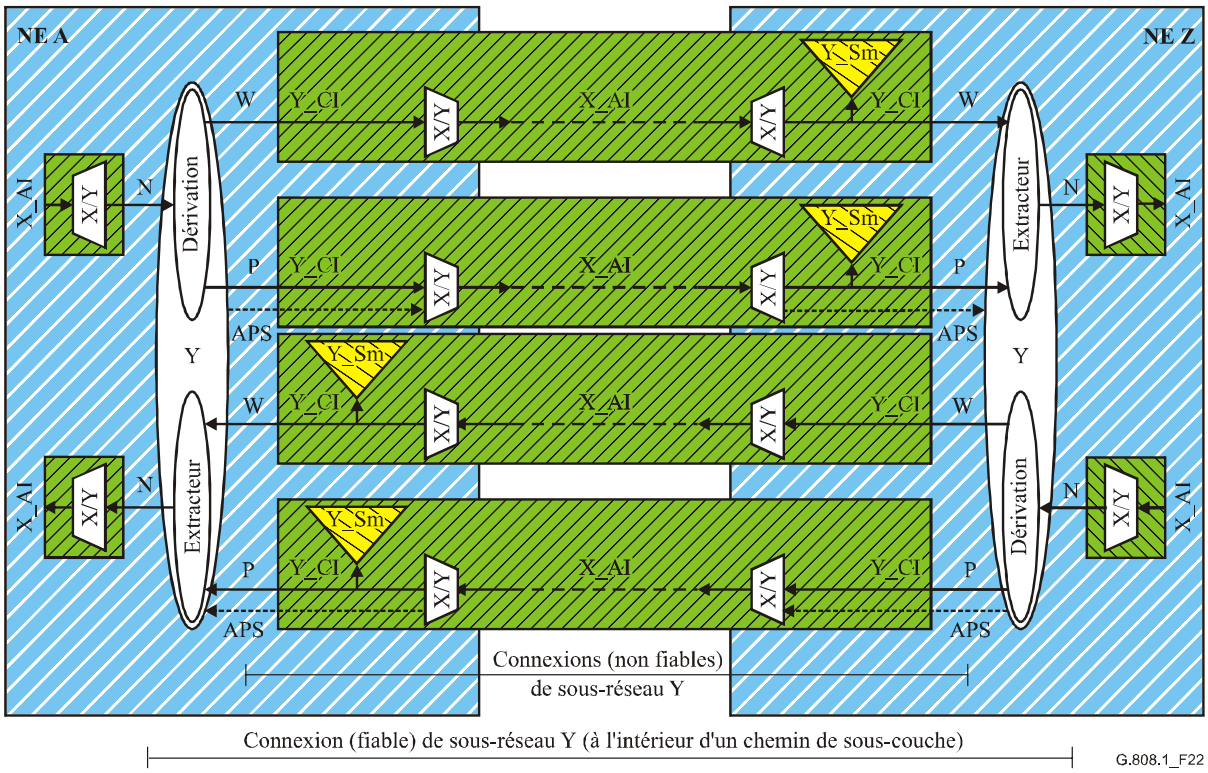
Dans le cas de la protection de connexion SNC de type 1+1, un procédé *à complexité réduite* est défini: SNC/N.

Les Figures 21 et 22 décrivent le cas de la protection SNC/N de type 1+1 entre arrivée et départ du domaine protégé entre éléments de réseau A et Z. Deux connexions de sous-réseau indépendantes existent et jouent le rôle d'entités de transport en service et en protection pour le signal (protégé) de trafic normal. Les fonctions de surveillance non intrusive (NIM, *non-intrusive monitoring*) (Ym_TT_Sk, Y_Sm_TT_Sk) surveillent les informations de surdébit/flux OAM de bout en bout (SNC/Ne) ou les informations de surdébit/flux OAM de sous-couche (SNC/Ns) afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur la protection SNC, sauf dans le cas de la commutation 1+1 unidirectionnelle.



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 21/G.808.1 – Modèle fonctionnel de la protection SNC/Ne de type 1+1



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 22/G.808.1 – Modèle fonctionnel de la protection SNC/Ns de type 1+1

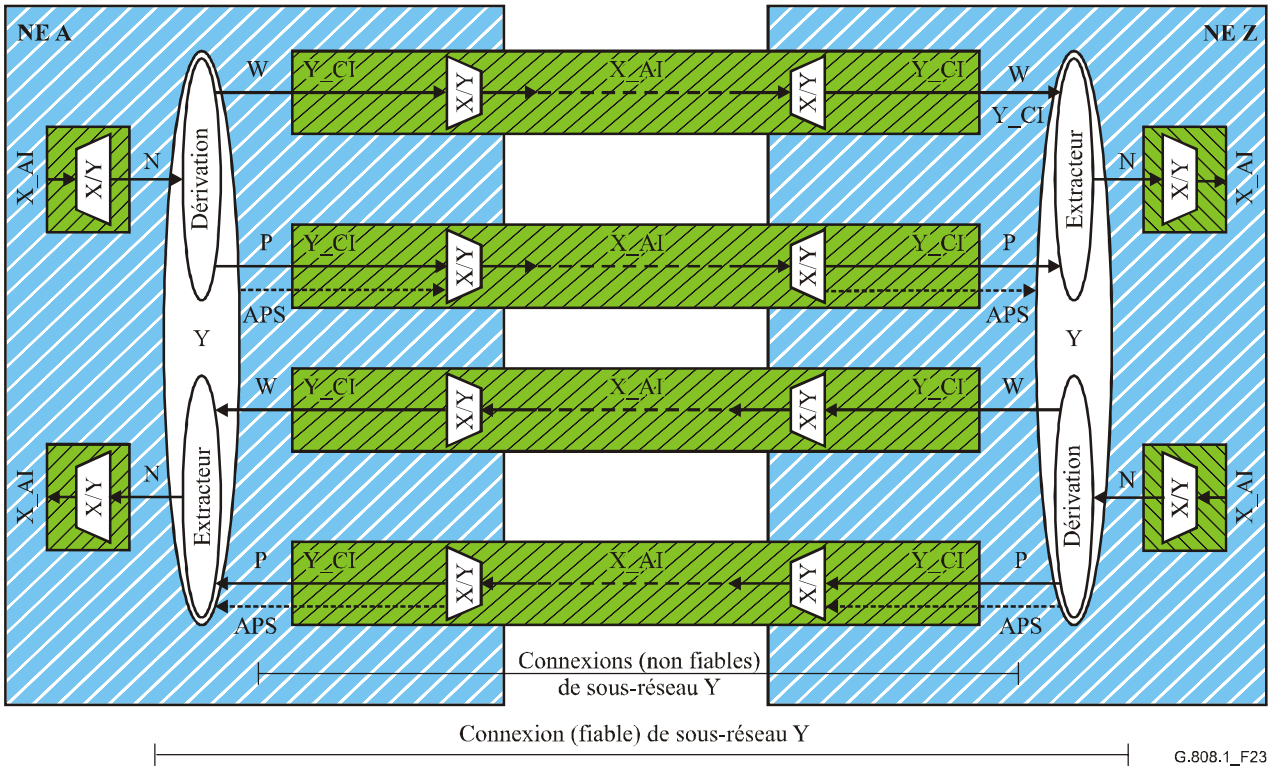
11.2.1.3 Protection SNC/I de type 1+1/1:n

Dans le cas de la protection de connexion SNC de type 1+1/1:n, un autre procédé à complexité réduite est le suivant: la protection SNC/I.

La Figure 23 décrit le cas de la protection SNC/I de type 1+1/1:1 entre entrée et sortie du domaine protégé entre éléments de réseau A et Z. Deux connexions de sous-réseau indépendantes existent et jouent le rôle d'entités de transport en service et en protection pour le signal (protégé) de trafic normal. Les fonctions d'adaptation X/Y surveillent les informations adaptées de la couche serveur quant à une panne du signal, afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur la protection SNC, sauf dans le cas de la commutation 1+1 unidirectionnelle.

En général, la protection SNC/I est un procédé de sécurisation pour une seule connexion de liaison (ne recouvrant qu'un seul chemin de couche serveur) car les fonctions d'adaptation extraient leurs conditions SSF et SSD à partir du signal TSF/TSD du chemin de couche serveur. L'état de panne TSF est réexpédié sous forme de signal de maintenance AIS/FDI de couche client et n'est pas visible en tant que tel par les fonctions d'adaptation situées en aval. Les informations de dégradation TSD ne sont pas réexpédiées.

Une exception existe pour la protection SNC/I de conteneurs VC-n en hiérarchie SDH: la protection SNC/I est en mesure de protéger une connexion de liaison composite en série car le signal de maintenance AIS est détecté dans chaque fonction d'adaptation située en aval du point d'insertion.



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

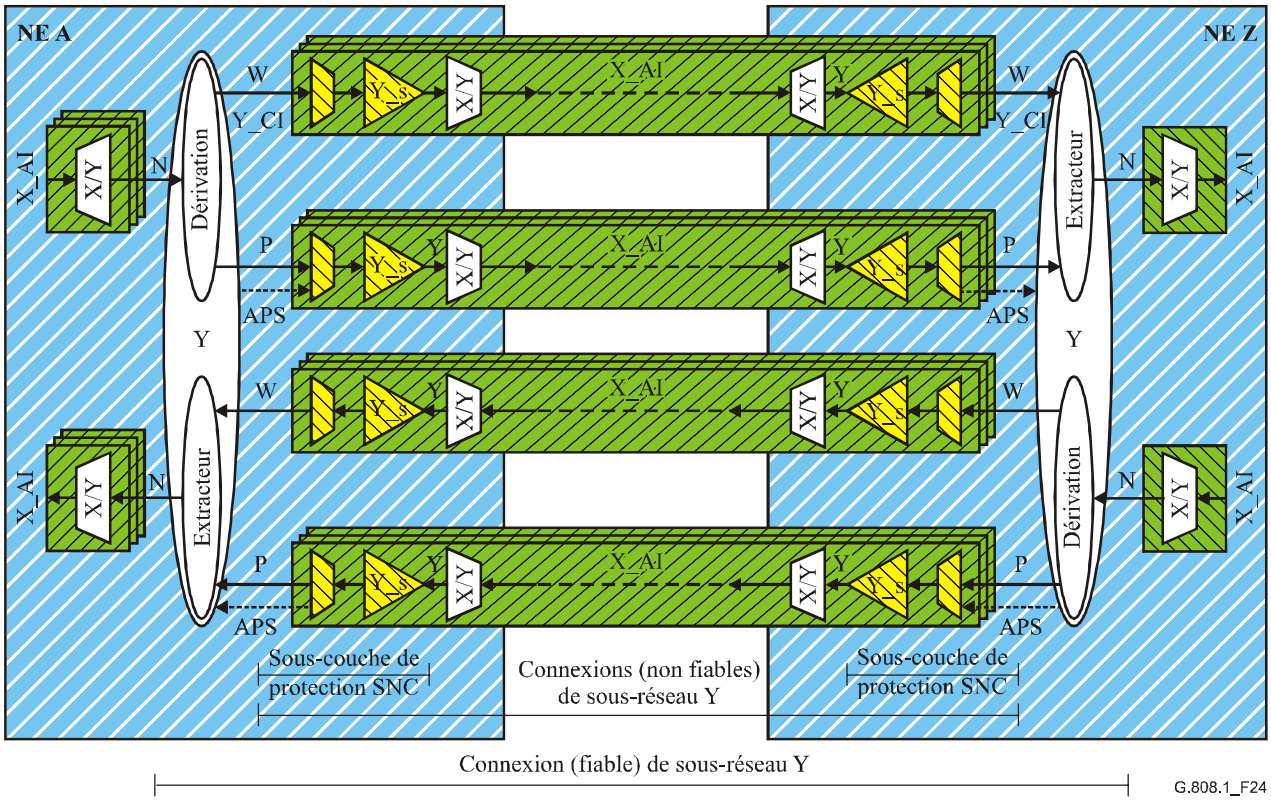
Figure 23/G.808.1 – Modèle fonctionnel de la protection SNC/I de type 1+1/1:1

11.2.2 Protection d'un groupe de connexions SNC

11.2.2.1 Protection SNC/S

La Figure 24 décrit le cas de la protection de groupe SNC/S de type 1+1/1:1 entre éléments de réseau A et Z. Dans cet exemple, deux fois trois connexions de sous-réseau parallèles et indépendantes, surveillées dans un chemin de sous-couche, existent et jouent le rôle de groupes d'entités de transport en service et en protection pour les trois signaux (protégés) de trafic normal. Les trois signaux parallèles de trafic normal contenus dans le groupe sont protégés conjointement par la fonction de connexion de couche. Les fonctions TT de sous-couche produisent/insèrent et surveillent/extraient le flux OAM/surdébit des informations de sous-couche afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur une des connexions SNC de protection, sauf dans le cas de la commutation 1+1 unidirectionnelle.

Les cas des architectures en 1:n, m:n et $(1:1)^n$ avec/sans trafic supplémentaire sont des extensions de l'architecture 1+1/1:1, conformément aux descriptions des types d'architecture du § 7.



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 24/G.808.1 – Modèle fonctionnel de la protection de groupe SNC/S de type 1+1/1:1

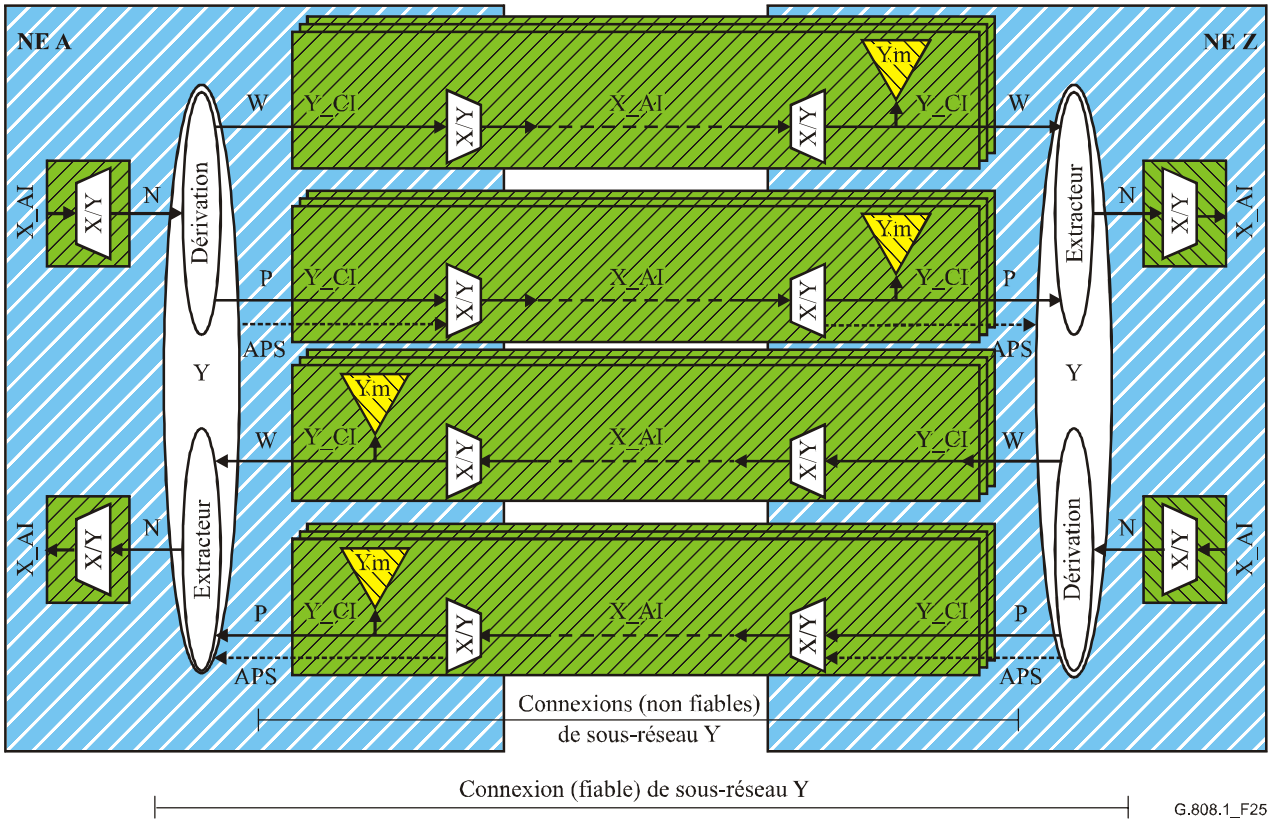
La Figure 11 présente des détails supplémentaires sur ces processus de fonction de connexion de protection. Le processus logique de groupe SFG/SDG est spécifique de la protection de groupe. Ce processus "fusionne" les trois signaux individuels de défaillance de signal d'un chemin (TSF) en une seule défaillance de signal de groupe (SFG) et fusionne les signaux individuels de dégradation de signal d'un chemin (TSD) en un seul groupe de dégradations de signal (SDG).

La logique de groupe SFG/SDG de la protection SNC/S peut fonctionner dans différents modes:

- W-SFG = W1-TSF ou W2-TSF ou W3-TSF; P-SFG = P1-TSF ou P2-TSF ou P3-TSF;
- W-SFG = W1-TSF; P-SFG = P1-TSF;
- W-SFG = X% des signaux Wi-TSF sont actifs; P-SFG = X% des signaux Pi-TSF sont actifs;
- idem pour SDG.

11.2.2.2 Protection SNC/N de type 1+1

La Figure 25 décrit le cas de la protection de groupe SNC/N de type 1+1 entre éléments de réseau A et Z. Dans cet exemple, deux fois trois connexions de sous-réseau parallèles et indépendantes existent et jouent le rôle de groupes d'entités de transport en service et en protection pour les trois signaux (protégés) de trafic normal. Les trois signaux parallèles de trafic normal dans le groupe sont protégés conjointement par la fonction de connexion de couche. Les fonctions de surveillance NIM surveillent les informations de surdébit/flux OAM de bout en bout (SNC/Ne) ou en sous-couche (SNC/Ns) afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur une des connexions SNC de protection, sauf dans le cas de la commutation 1+1 unidirectionnelle.



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 25/G.808.1 – Modèle fonctionnel de la protection de groupe SNC/Ne de type 1+1

La Figure 11 présente des détails supplémentaires sur ces processus de fonction de connexion de protection. Le processus logique de groupe SFG/SDG est spécifique de la protection 1+1 de groupe de connexions SNC/N. Ce processus "fusionne" les trois signaux individuels de défaillance de signal d'un chemin (TSF) en une seule défaillance de signal de groupe (SFG) et "fusionne" les signaux individuels de dégradation de signal d'un chemin (TSD) en un seul groupe de dégradations de signal (SDG).

La logique de groupe SFG/SDG de la protection SNC/N peut fonctionner dans différents modes:

- W-SFG = (W1-TSF et non P1-TSF) ou (W2-TSF et non P2-TSF) ou (W3-TSF et non P3-TSF);

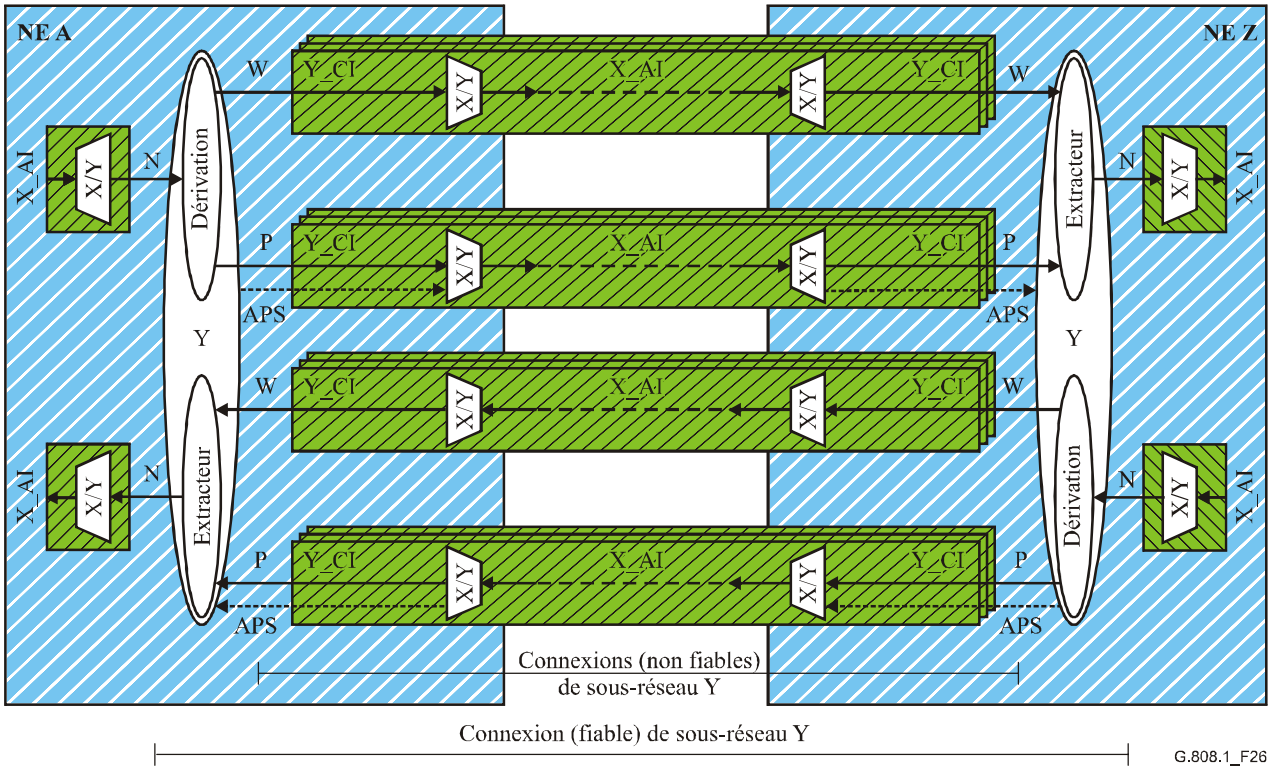
  P-SFG = (P1-TSF et non W1-TSF) ou (P2-TSF et non W2-TSF) ou (P3-TSF et non W3-TSF);
- W-SFG = (W1-TSF et non P1-TSF); P-SFG = (P1-TSF et non W1-TSF);
- W-SFG = X% des signaux (Wi-TSF et non Pi-TSF) sont actifs; P-SFG = X% des signaux (Pi-TSF et non Wi-TSF) sont actifs;
- idem pour SDG.

Pour les signaux de conteneurs virtuels VC-n concaténés en hiérarchie SDH (VC-n-Xv), les conditions de groupe SF et SD devraient être déclarées dès qu'un des signaux X contenus dans le groupe est défectueux ou dégradé.

- W-SFG = W1-TSF ou W2-TSF ou W3-TSF; P-SFG = P1-TSF ou P2-TSF ou P3-TSF;
- idem pour SDG.

11.2.2.3 Protection SNC/I de type 1+1

La Figure 26 décrit le cas de la protection de groupe SNC/I de type 1+1 entre éléments de réseau A et Z. Dans cet exemple, deux fois trois connexions de sous-réseau indépendantes et parallèles existent et jouent le rôle de groupes d'entités de transport en service et en protection pour les trois signaux (protégés) de trafic normal. Les trois signaux parallèles de trafic normal contenus dans le groupe sont protégés conjointement par la fonction de connexion de couche. Les fonctions d'adaptation X/Y surveillent les informations adaptées de la couche serveur quant à une panne du signal, afin de déterminer l'état des entités de transport en service et en protection. Les informations de commutation APS sont transportées sur une des connexions SNC de protection, sauf dans le cas de la commutation 1+1 unidirectionnelle.



NOTE – Le signal de commutation APS n'est applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 26/G.808.1 – Modèle fonctionnel de la protection de groupe SNC/I de type 1+1

La Figure 11 présente des détails supplémentaires sur ces processus de fonction de connexion de protection. Le processus logique de groupe SFG est spécifique de la protection de groupe SNC/I de type 1+1. Ce processus "fusionne" les trois signaux individuels de défaillance de signal du serveur (SSF) en un seul groupe de dégradation de signal (SFG).

La logique de groupe SFG de protection SNC/I peut fonctionner dans différents modes:

- W-SFG = (W1-SSF et non P1-SSF) ou (W2-SSF et non P2-SSF) ou (W3-SSF et non P3-SSF);

  P-SFG = (P1-SSF et non W1-SSF) ou (P2-SSF et non W2-SSF) ou (P3-SSF et non W3-SSF);
- W-SFG = (W1-SSF et non P1-SSF); P-SFG = (P1-SSF et non W1-SSF);
- W-SFG = X% des signaux (Wi-SSF et non Pi-SSF) sont actifs; P-SFG = X% des signaux (Pi-SSF et non Wi-SSF) sont actifs.

Pour les signaux de conteneurs virtuels VC-n concaténés en hiérarchie SDH (VC-n-Xv), les conditions de groupe SF et SD devraient être déclarées dès qu'un des signaux X contenus dans le groupe est défectueux ou dégradé.

- W-SFG = W1-SSF ou W2-SSF ou W3-SSF; P-SFG = P1-SSF ou P2-SSF ou P3-SSF;
- idem pour SDG.

11.2.2.4 Protection SNC/T

Compte tenu du grand nombre d'affluents élémentaires dans certaines techniques de transmission (par exemple, en mode ATM), des affluents élémentaires supplémentaires peuvent être attribués dans les signaux de couche serveur en service et en protection afin de transporter les signaux d'essai au moyen d'entités de transport expérimentales (Figures 27, 29). Ces signaux d'essai (un par entité de service, un par entité de protection) peuvent être utilisés à la place des informations de groupe SFG/SDG comme décrit ci-dessus. Le signal de commutation APS est transporté au moyen de l'entité de transport en protection expérimentale.

La logique de groupe SFG/SDG fonctionne donc comme suit:

- W-SFG = Wt-TSF;
  P-SFG = Pt-TSF;
- W-SDG = Wt-TSD;
  P-SDG = Pt-TSD.

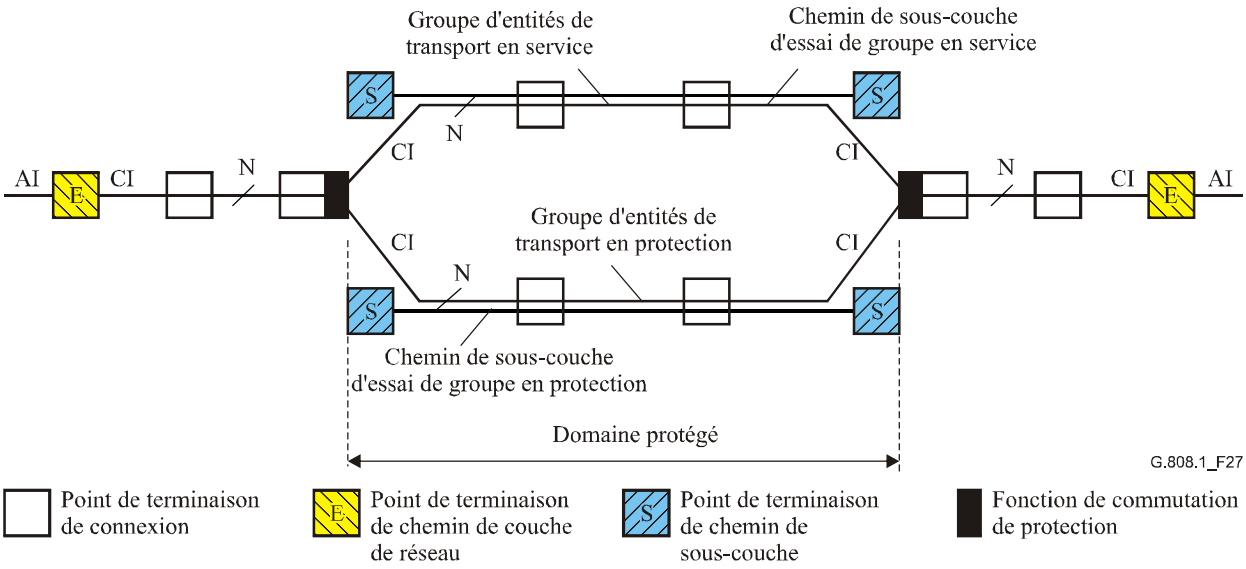


Figure 27/G.808.1 – Protection de groupe SNCTs en 1:1 ou 1+1 utilisant des terminaisons de chemin de sous-couche

La protection de groupe SNC/T peut également utiliser le flux OAM/le surdébit de bout en bout afin de créer un chemin de couche de réseau de bout en bout en tant que chemin d'essai (Figure 28). Les modèles d'équipement situent normalement ces fonctions de terminaison de couche à des unités d'interface se trouvant "de l'autre côté" de la fonction de connexion, c'est-à-dire non immédiatement disponibles aux fins d'un chemin d'essai de protection en groupe.

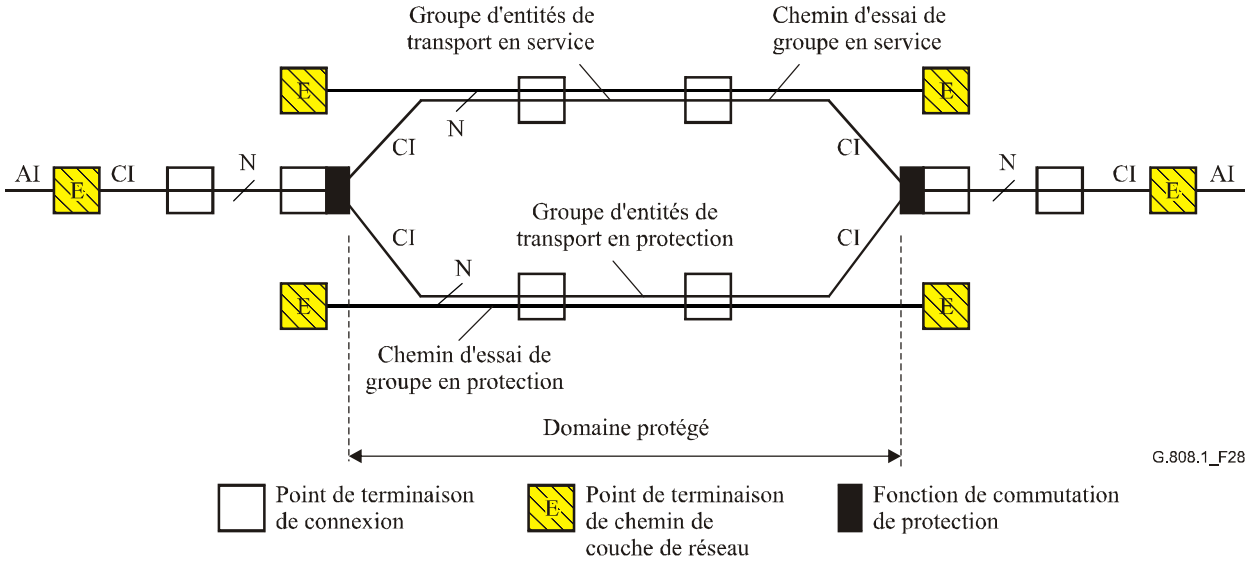
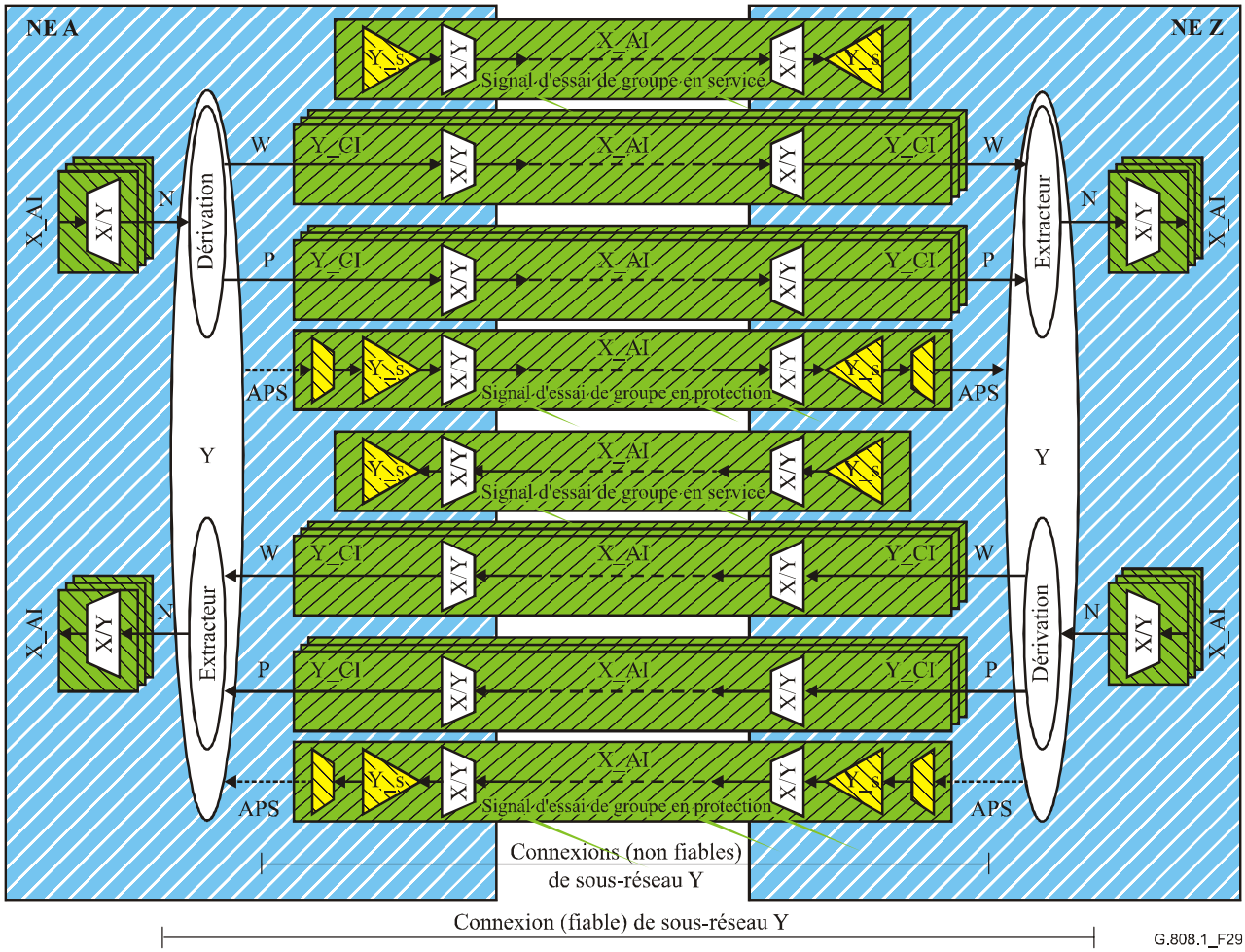


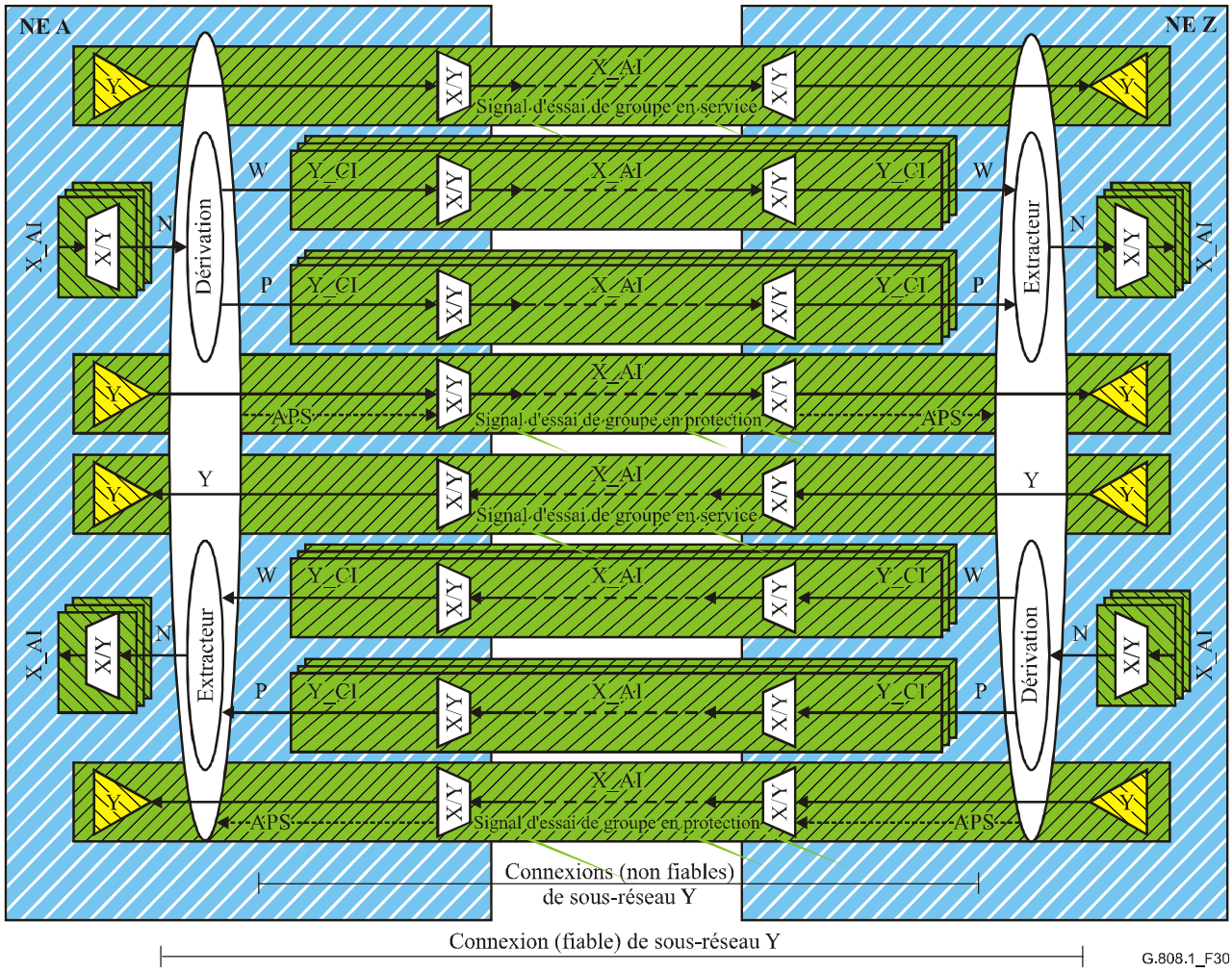
Figure 28/G.808.1 – Protection de groupe SNC/Te de type 1:1 ou 1+1 utilisant des terminaisons de chemin de couche de réseau



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 29/G.808.1 – Modèle fonctionnel de la protection de groupe SNC/Ts de type 1+1/1:1 utilisant des terminaisons de chemin de sous-couche

NOTE – Dans le cas du mode ATM, le chemin d'essai (en sous-couche) devrait contenir un signal d'essai dont le contrôle de continuité (CC) est activé. Si le contrôle CC est inactif, un tel chemin d'essai (en sous-couche) ne transportera aucune information en condition normales d'absence de défaut. Lorsqu'un défaut se produit, des cellules de signal AIS sont insérées. Lorsque le défaut n'a été présent que pendant une brève période (par exemple, en raison d'une "action de protection dans la couche Physique"), le détecteur de défaut AIS situé à l'extrémité du chemin d'essai (en sous-couche) détectera la condition de défaut AIS pendant 2 à 3 secondes conformément à la définition de l'état AIS figurant dans la Rec. UIT-T I.610. Avec le contrôle CC activé, la condition de défaut AIS est relevée dès réception d'une cellule CC, c'est-à-dire dans une période de 1 seconde après que l'interruption de trafic a été relevée.



NOTE – Le signal de commutation APS n'est pas applicable au cas de la commutation 1+1 unidirectionnelle.

Figure 30/G.808.1 – Modèle fonctionnel de la protection de groupe SNC/Te de type 1+1/1:1 utilisant des terminaisons de chemin de couche de réseau

12 Autorétablissement de connexions de liaison à multiplexage inverse

Il existe plusieurs méthodes de transport permettant de prendre en charge le multiplexage inverse. Le multiplexage inverse peut être utilisé pour transporter un signal client en répartissant la charge utile et en transférant les fragments sur un certain nombre de chemins individuels à travers le réseau. Les différents chemins transportant les fragments peuvent être considérés comme étant les membres d'un groupe à multiplexage inverse (IMG, *inverse multiplexed group*).

Il est possible d'employer des mécanismes de multiplexage inverse permettant de s'accommoder de défauts du réseau (par exemple, concaténation virtuelle au moyen du procédé LCAS) pour assurer

l'autorétablissement d'un chemin de signal P-X dans l'ensemble d'un réseau d'opérateur ou dans plusieurs réseaux d'opérateur. Il s'agit d'une architecture d'autorétablissement de bout en bout pouvant s'appliquer à différentes topologies de réseau (par exemple, réseaux maillés, anneaux, etc.). Comme il s'agit d'un mécanisme spécialisé d'autorétablissement, il n'y a aucune limitation fondamentale du nombre d'éléments de réseau contenus dans les chemins.

Le procédé SIM fonctionne dans toutes les combinaisons d'architectures de protection, de commutation et de fonctionnement.

Le procédé SIM offre une protection générique contre les défauts dans la couche serveur et contre les défauts de connexité et les dégradations de qualité dans la couche client.

Le procédé SIM permet de protéger l'information adaptée (AI, *adapted information*) (c'est-à-dire la totalité de la charge utile de l'information caractéristique (CI, *characteristic information*) individuelle de la couche de réseau). Voir la Figure 31.

L'accommodation consiste à supprimer la fraction de la charge utile qui est transportée par un membre quelconque du groupe à multiplexage inverse (IMG) qui rencontre une condition de défaut d'entité de transport. Il en résulte une réduction de la longueur de charge utile d'information AI.

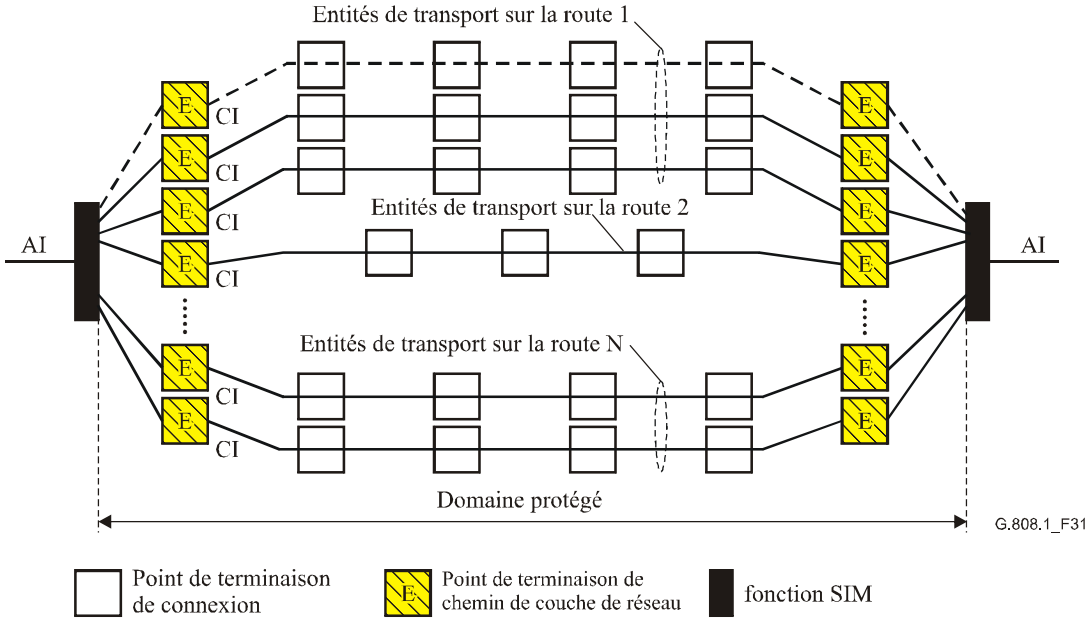


Figure 31/G.808.1 – Concept générique de capacité d'autorétablissement d'un chemin à multiplexage inverse

L'information AI est transportée au moyen d'un groupe à multiplexage inverse (IMG) ayant X membres, répartis sur N routes, où:

- N est le nombre de routes ($1 \leq N \leq X$) contenant chacune une ou plusieurs connexions de réseau dans le groupe IMG.
- X est le nombre de membres du groupe IMG appelés à transporter l'information AI sur la largeur de bande de couche client + capacité de trafic supplémentaire/de protection Z ($X \geq 1, Z \geq 0$).
- B est la largeur de bande totale des membres X+Z dans le groupe. $B = \sum_{i}^{X+Z} B_i$
- B_{ACT} est la charge utile effectivement transportée ($0 \leq B_{ACT} \leq B$); en raison de la panne d'un ou de plusieurs des chemins des membres, la largeur de bande d'un ou de plusieurs membres du groupe IMG ne sera pas utilisée pour transporter l'information AI.

Le procédé SIM est indépendant de la protection dans les couches serveur.

12.1 Modèle fonctionnel du procédé SIM

La Figure 32 décrit l'utilisation du procédé SIM pour le transport entre éléments de réseau A et Z. De multiples chemins indépendants (dans la couche de réseau Y) sont utilisés comme entités de transport pour le signal de trafic normal (charge utile) Z_CI. Les fonctions Y_TT de terminaison de X chemins produisent/insèrent et surveillent/extraient les informations de surdébit de bout en bout afin de déterminer l'état des entités de transport individuelles. Les fonctions d'adaptation de multiplexage inverse Y-Xv/Y-X_A produisent/insèrent et surveillent/extraient les informations de multiplexage inverse et de surdébit de bout en bout afin de déterminer et d'aligner les X membres dans le groupe IMG.

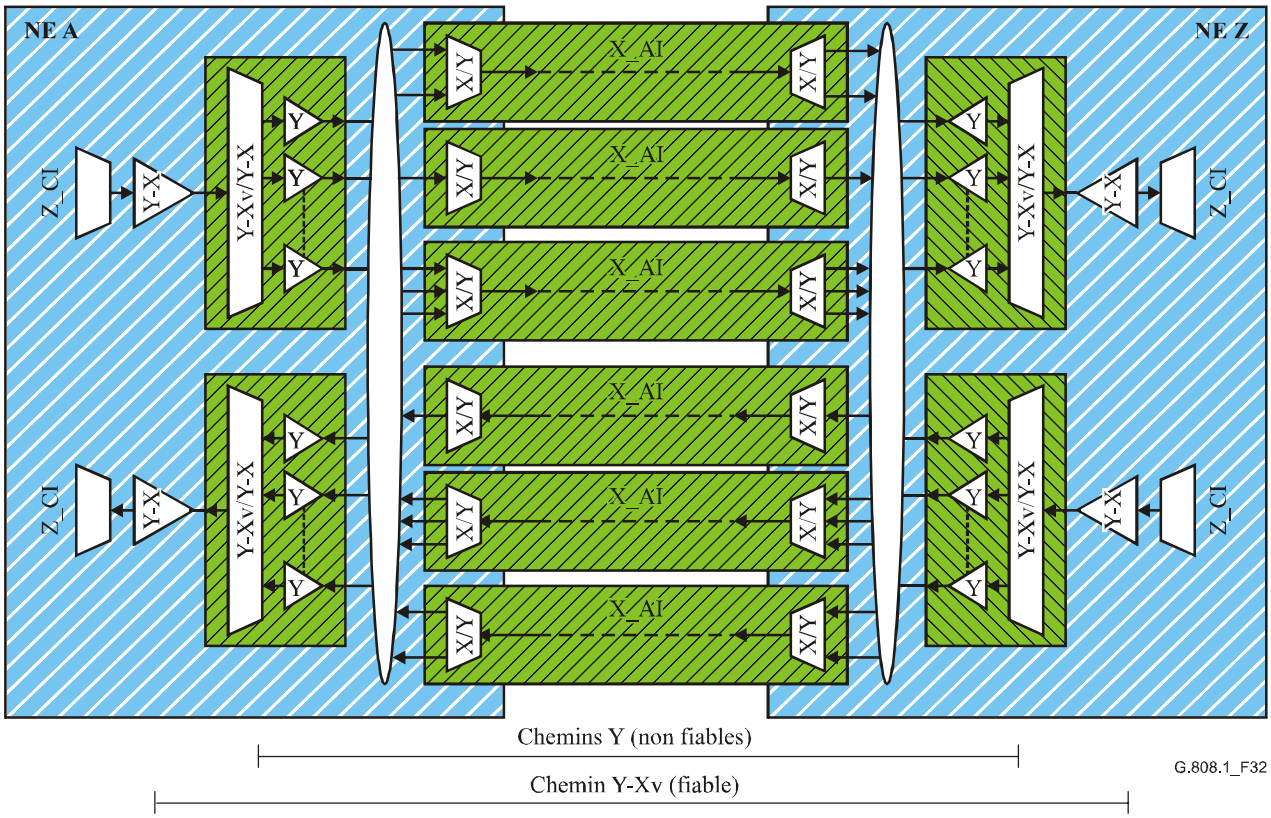


Figure 32/G.808.1 – Modèle fonctionnel du procédé SIM

Les fonctions d'adaptation de multiplexage inverse Y-Xv/Y-X_A distribuent/collectent la charge utile transportée au moyen des X_{ACT} chemins Y de couche de réseau disponibles, qui sont extraits des X chemins Y de couche de réseau configurés.

13 Qualité de la commutation de protection

Le modèle temporel de commutation de protection extrait de la Rec. UIT-T M.495 est illustré dans la Figure 33. Les paramètres de ce modèle sont définis comme suit.

13.1 temps de détection, T_1: intervalle de temps entre l'apparition d'une dégradation du réseau et la détection de défaillance du signal (SF) ou de dégradation (SD) déclenché par cette dégradation du réseau.

13.2 temps d'attente de protection, T_2: intervalle de temps après la détection d'un signal SF ou SD et sa confirmation en tant que condition nécessitant la procédure de commutation de protection.

NOTE – La Rec. UIT-T M.495 désigne le temps T_2 comme étant le "temps d'attente".

13.3 temps de fonctionnement de commutation de protection, T_3: intervalle de temps entre la confirmation d'un signal SF ou SD et l'achèvement du traitement et de la transmission des signaux de commande requis afin d'effectuer la commutation de protection.

13.4 temps de transfert de commutation de protection, T_4: intervalle de temps entre d'une part l'achèvement du traitement et de la transmission des signaux de commande requis afin d'effectuer la commutation de protection et d'autre part l'achèvement des opérations de commutation de protection.

13.5 temps de rétablissement, T_5: intervalle de temps entre l'achèvement des opérations de commutation de protection et le plein rétablissement du trafic protégé.

NOTE – Cet intervalle peut comprendre la vérification des opérations de commutation, la resynchronisation de la transmission numérique, etc.

13.6 temps de confirmation, T_c: intervalle de temps à partir de l'apparition de la dégradation du réseau jusqu'au moment où le signal SF ou SD déclenché est confirmé comme nécessitant des opérations de commutation de protection: $T_c = T_1 + T_2$.

13.7 temps de transfert, T_t: intervalle de temps après la confirmation du fait qu'un signal SF ou SD nécessite des opérations de commutation de protection jusqu'à l'achèvement de ces opérations de commutation de protection: $T_t = T_3 + T_4$.

13.8 temps de rétablissement du trafic protégé, T_r: intervalle de temps à partir de l'apparition de la dégradation du réseau jusqu'au rétablissement du trafic protégé:

$$T_r = T_1 + T_2 + T_3 + T_4 + T_5 = T_c + T_t + T_5.$$

NOTE – Une apparente dégradation du réseau pourrait être détectée par un équipement et ne pas être confirmée après les opérations de confirmation. Dans ce cas, seuls les temps T_1 et T_2 sont pertinents.

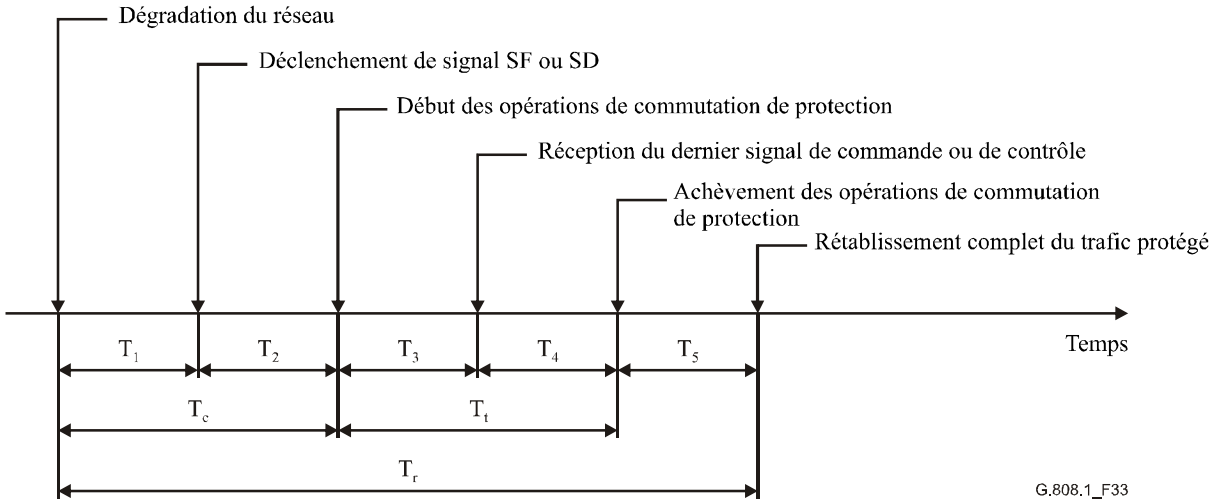


Figure 33/G.808.1 – Modèle chronologique de la commutation de protection

14 Temporisateur d'attente de protection

Les temporisateurs d'attente de protection sont destinés à fonctionner lorsqu'un signal fait l'objet d'une protection imbriquée. Ces dispositifs doivent permettre à un groupe de protection interne de rétablir le trafic avant que le groupe de protection externe tente de le faire, afin de limiter le nombre d'actions de commutation.

Les temporisateurs d'attente de protection sont également appliqués dans les types de protection SNC/N et SNC/I 1+1 afin d'éviter une commutation prématurée en raison de la différence de temps de propagation entre route brève et route longue.

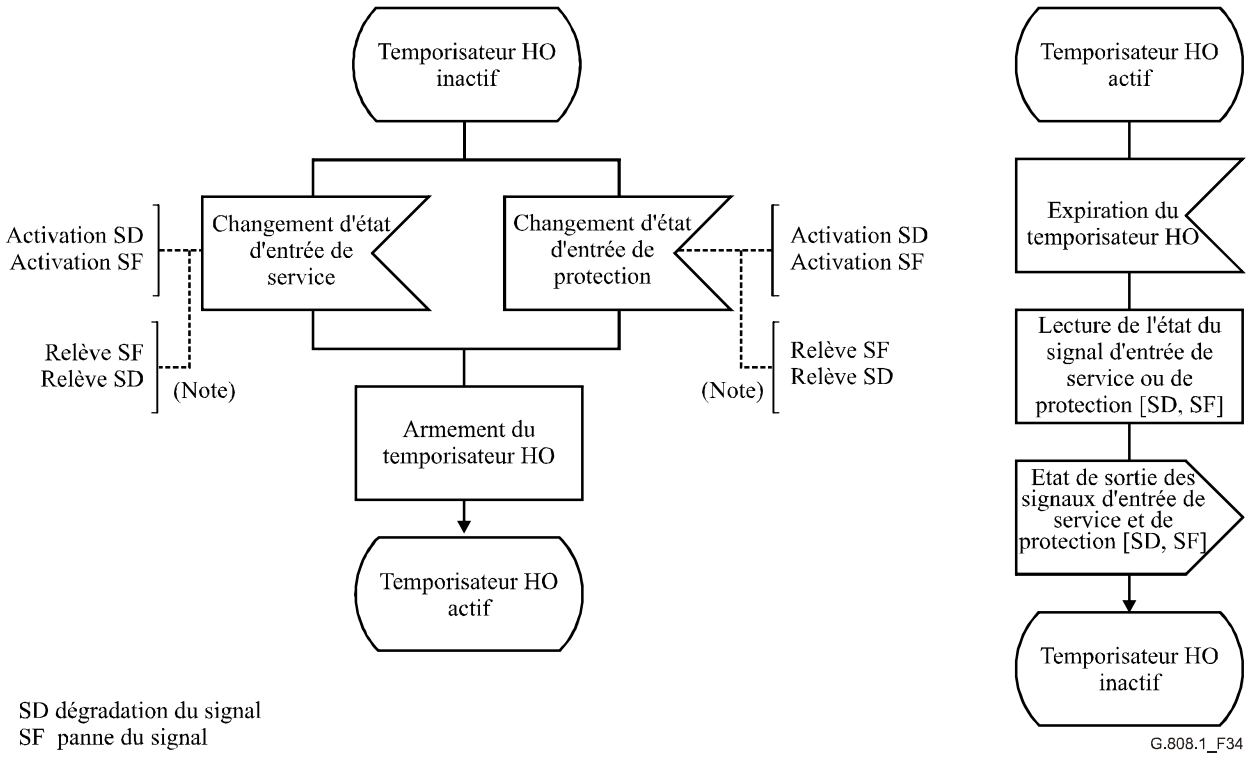
Chaque extracteur de protection peut avoir un temporisateur d'attente de protection.

Un temporisateur d'attente de protection est armé lorsqu'une ou plusieurs des conditions SF ou SD deviennent actives dans le groupe de protection et se prolongent pendant une période non réinitialisable qui est configurable de 0 à 10 s par échelons de X ms. La valeur de X est de 100 ms (en SDH, OTN) et de 500 ms (en ATM).

Pendant cette période, les états SF/SD modifiés ne sont pas transmis au processus de commutation de protection.

Lorsque le temporisateur arrive à expiration, l'état SF/SD de tous les signaux est lu et transmis jusqu'au processus de commutation de protection. A ce point, le processus de commutation de protection réagira au nouvel état SF/SD.

NOTE – Une condition de signal SF/SD n'est pas tenue d'être présente pendant toute la durée du temps d'attente car seul l'état à l'expiration du temporisateur d'attente de protection est pertinent. Par ailleurs, la condition de signal SF/SD qui déclenche le temporisateur d'attente de protection n'a pas besoin d'être la même qu'à l'expiration de l'intervalle de temps d'attente.



NOTE – L'utilisation des évènements de relève SF/SD comme déclencheurs d'armement du temporisateur d'attente de protection n'est pas obligatoire mais est recommandée afin de prévenir d'inutiles commutations de protection, qui pourraient autrement se produire dans certaines circonstances.

Figure 34/G.808.1 – Fonctionnement du temporisateur d'attente de protection

15 Temporisateur d'attente de rétablissement

En mode de fonctionnement réversible, afin d'éviter un fonctionnement fréquent de la commutation de protection en raison d'un défaut intermittent (par exemple, une fluctuation du taux BER autour du seuil SD), une entité de transport de service défectueuse doit toujours devenir exempte de défaut (par exemple, avec un taux BER inférieur à un seuil de rétablissement). Une fois que l'entité de transport de service défectueuse répond à ce critère, une période de temps fixe doit s'écouler avant qu'un signal de trafic normal l'utilise de nouveau. Cette période, appelée période d'attente de rétablissement (WTR, *wait-to-restore*), est de l'ordre de 5-12 minutes et devrait être réglable. Une condition de signal SF ou SD neutralisera la période WTR.

En mode de fonctionnement réversible, lorsque la protection n'est plus requise, c'est-à-dire lorsque l'entité de transport de service défectueuse n'est plus en condition de signal SD ou SF (et en supposant l'absence d'autres entités de transport requérantes), un état local d'attente de rétablissement est activé. Comme cet état devient le plus élevé en priorité, il est indiqué dans le signal de commutation APS (si applicable) et conserve, dans l'entité de transport en protection, le signal de trafic normal issu de la précédente entité de transport de service défectueuse. Cet état doit normalement arriver à expiration et devenir un signal vide d'absence de requête (ou un signal de trafic supplémentaire indiquant une absence de requête, si applicable). Le temporisateur d'attente de rétablissement se désarme plus tôt si une requête de priorité supérieure présélectionne cet état.

16 Signal de commutation automatique de protection (APS) signal

Un signal de commutation APS sert à synchroniser les actions aux extrémités A et Z du domaine protégé. Les informations communiquées sont les suivantes:

– type de requête/d'état;
– signal demandé;
– signal dérivé;
– configuration de protection.

Les informations de type de requête/d'état indiquent la condition de défaut, la commande externe ou l'état du processus de protection qui possède la priorité la plus élevée.

Les informations relatives au signal demandé et au signal dérivé indiquent, lorsqu'elles sont transportées dans un champ de n éléments binaires:

0 signal vide;
1.. $2^n - 2$ signal de trafic normal 1 à $2^n - 2$;
$2^n - 1$ signal de trafic supplémentaire.

Les informations relatives à la configuration de protection indiquent:

– l'utilisation d'un canal de commutation APS;
– l'architecture de protection (1+1, 1:n);
– le type de commutation (dans un sens ou dans les deux sens);
– le type de fonctionnement (irréversible, réversible).

Le signal de commutation APS est transporté au moyen du canal de commutation APS. En principe, il est possible d'attribuer un canal de commutation APS à chaque entité de transport. L'attribution de ce canal à une entité de transport en service n'offrira cependant pas une capacité d'autorétablissement suffisante; c'est-à-dire que lorsque l'entité de transport en service tombera en panne, la communication entre les deux extrémités tombera en panne également et la protection ne sera donc pas possible. Le canal de commutation APS est donc attribué à une ou à plusieurs entités de transport en protection.

17 Trafic non protégé et non réservable (NUT)

Le trafic non protégé et non réservable est une des trois classes de trafic contenues dans les procédés de sécurisation en (1:1) et $(1:1)^n$, les autres classes étant le trafic protégé et le trafic supplémentaire. Le trafic NUT n'est associé à aucune protection mais ne peut pas être extrait du réseau afin de permettre la protection d'un autre trafic.

L'accès à un canal de trafic supplémentaire ou de protection permet d'utiliser des entités de protection afin de transporter du trafic supplémentaire en fonctionnement normal dans les architectures en (1:1) ou $(1:1)^n$. Ce trafic est extrait lorsqu'une commutation de protection se produit. Le trafic supplémentaire offre un service plus économique que le trafic protégé ou que le trafic non protégé et non réservable. Il n'a aucun rapport avec le trafic protégé car il provient d'un client différent et peut par exemple servir à fournir une surcapacité en réponse à un événement majeur.

18 Entité de transport (en protection) du traffic supplémentaire utilisant le surdébit/flux OAM

Dans le cas de la protection SNC/S en $(1:1)^n$ avec trafic supplémentaire, l'entité de transport (en protection) du trafic supplémentaire n'exige pas l'adjonction d'une terminaison de chemin de sous-couche. L'entité de transport (en protection) du trafic supplémentaire contient un affluent élémentaire spécialisé dans le signal résultant, distinct des affluents élémentaires contenus dans les entités de transport utilisées en protection pour acheminer un signal de trafic normal.

L'état de l'entité de transport (en protection) du trafic supplémentaire n'a pas d'incidence sur le fonctionnement de la commutation de protection, de sorte qu'il n'est pas nécessaire de surveiller cette entité de transport.

19 Commandes externes

Le comportement autonome du processus de commutation de protection lors des conditions de défaut de ses entités de transport peut être modifié au moyen de commandes externes (de commutation) par lesquelles une commande externe (de commutation) envoie une requête externe appropriée au processus de protection.

NOTE – Une seule commande externe (de commutation) peut être émise par groupe de protection. Les commandes externes qui sont présélectionnées ou refusées par d'autres conditions, états ou requêtes de priorité supérieure sont rejetées.

Les commandes externes sont définies de façon à permettre les types d'action suivants (voir au § 3.3.8 ci-dessus les définitions exactes des commandes externes):

1) modifications de configuration et maintenance à effectuer dans le groupe de protection ou ses entités de transport:
   - le **verrouillage de protection** désactive temporairement l'accès à l'entité de transport en protection pour tous les signaux;
   - la **commutation forcée du signal #i** force temporairement le routage du signal #i sur l'entité de transport en protection;
   - la **commutation manuelle du signal #i** route temporairement le signal #i sur l'entité de transport en protection, à moins qu'un état de défaut (SF, SD) ne nécessite le routage d'un autre signal sur cette entité de transport;

2) verrouillage de signaux à partir du processus de protection:
   - le **verrouillage du signal #i** désactive temporairement l'accès à l'entité de transport en protection pour le signal spécifique;
   - **acquittement du verrouillage du signal #i**.

3) Gel du processus de protection:
   - le **gel** empêche temporairement d'effectuer une quelconque action de commutation et, en tant que tel, gèle l'état actuel. Jusqu'à ce que le gel soit relevé, les nouvelles commandes externes de l'extrémité locale sont rejetées et les transitions d'état de défaut ainsi que les messages de commutation APS reçus sont ignorés;
   - **relève du gel**: lorsque la commande de gel est relevée, l'état du groupe de protection est recalculé sur la base des conditions de défaut et des messages de commutation APS reçus.

4) Essais du processus de protection et du canal de commutation APS entre les deux extrémités:
   - l'**essai préalable** simule une requête de commutation sans exécuter l'action de commutation proprement dite, à moins que l'entité de transport en protection ne soit en cours d'utilisation.

5) Relève une précédente commande externe (de commutation):
   - la **relève** libère toutes les commandes de commutation.

20 Etats du processus de commutation de protection

Les états suivants du processus de commutation de protection existent:

maintien irréversible du signal de trafic normal #i (DNR #i) – En fonctionnement irréversible, cet état sert à maintenir un signal de trafic normal à extraire de l'entité de transport en protection;

absence de requête (NR) – Tous les signaux de trafic normal sont extraits de leurs entités de transport en service respectives. L'entité de transport en protection achemine soit le signal vide, du trafic supplémentaire ou une dérivation du seul signal de trafic normal dans un groupe de protection 1+1;

période d'attente de rétablissement signal de trafic normal #i (WTR) – En fonctionnement réversible, après la relève d'une alarme SF ou SD de l'entité de transport en service #i, cet état maintient le signal de trafic normal #i tel qu'il a été extrait de l'entité de transport en protection jusqu'à ce qu'un temporisateur d'attente de rétablissement arrive à expiration. Si le temporisateur arrive à expiration avant tout autre événement ou toute autre commande, l'état passe à NR (absence de requête). Cet état sert à éviter un fonctionnement fréquent de l'extracteur en cas de pannes intermittentes.

21 Priorité

Les conditions de défaut, les commandes externes et les états de protection sont définis comme ayant une relation de priorité les uns avec les autres. L'ordre de priorité est appliqué localement à ces conditions/commandes/états, à chaque extrémité et entre les deux extrémités.

Voir les Recommandations particulières à la commutation de protection pour ces priorités.

22 Conditions de déclenchement des signaux SF et SD

Une condition de signal SF est une panne TSF ou SSF, selon le type de protection.

La Figure 35 décrit les règles de combinaison par défaut. Une panne SSF est indiquée par des défauts relevant de la fonction d'adaptation et par une information AI_TSF. Une panne TSF est indiquée par tout défaut du chemin de couche de réseau et par une information CI_SSF.

Une condition de déclenchement SF est soit directement détectée par la fonction de terminaison de chemin de la couche de réseau protégée ou est transmise dans une ou plusieurs couches selon les règles de combinaison de défauts spécifiques et selon les informations CI_SSF et AI_TSF.

Une dégradation TSD est la seule condition de déclenchement du signal SD. Cette condition est émise à la détection d'une dégradation dDEG. Une condition TSD est toujours localisée dans une fonction de terminaison de chemin, c'est-à-dire qu'elle ne traverse pas les frontières de couche.

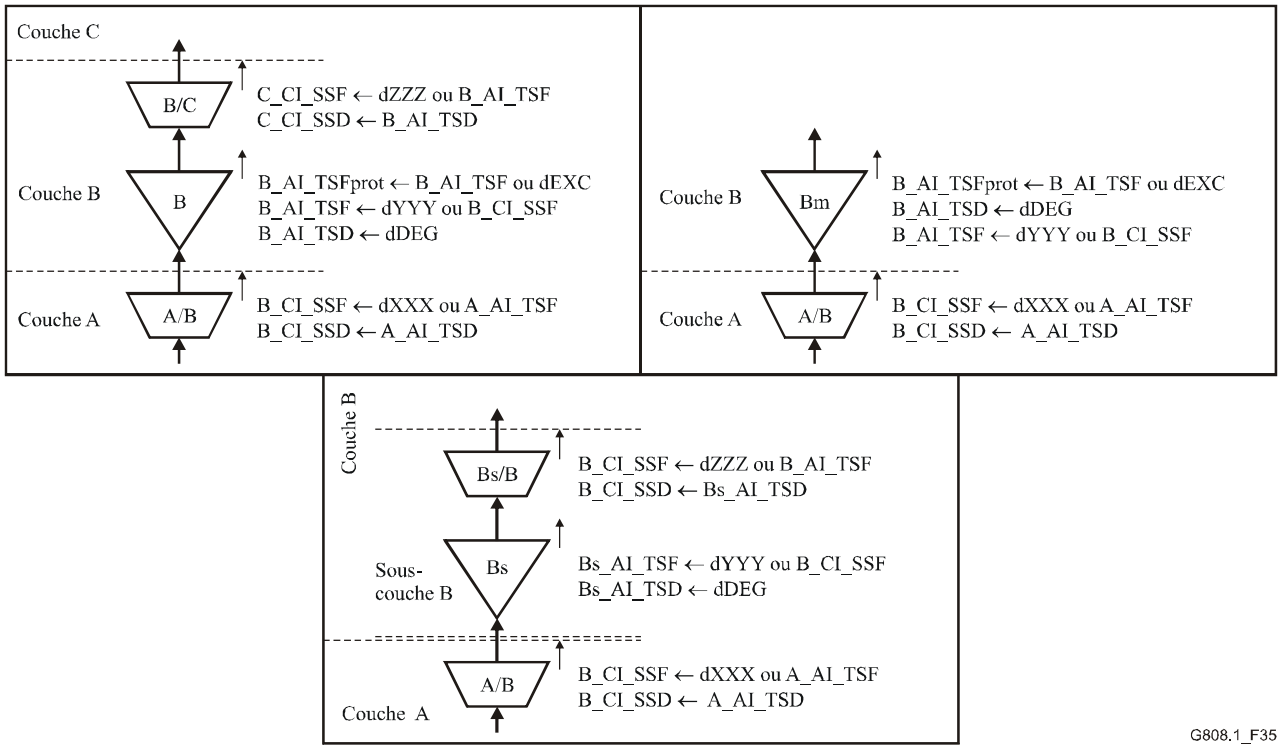


Figure 35/G.808.1 – Règles de combinaison des défauts

22.1 Aperçu général des conditions de déclenchement du signal SF

Le Tableau 2 présente un aperçu général des défauts qui contribuent aux conditions de déclenchement du signal SF dans plusieurs techniques de transmission. Voir les Recommandations relatives aux équipements (par exemple, Recommendations UIT-T G.783, G.798, I.732) concernant les spécifications particulières au signal SF.

Tableau 2/G.808.1 – Aperçu général de défauts contribuant à la condition de signal SF

	ATM	OTN	SDH
Défauts de continuité	LOC	LOS, LOS-P, LCK, LTC	LOS, LTC
Défauts de connexité	Néant	TIM, OCI	TIM, UNEQ
Défauts d'adaptation	LCD	MSIM, LOM, PLM, LOFLOM	LOF, LOM, LOP, PLM
Défauts amont de couche serveur (Note 1)	AIS	FDI, FDI-P	AIS
Chemin à taux d'erreurs excessif			EXC (Note 2)
Défauts de concaténation virtuelle (Note 3)		LOM, LOA	LOM, LOA
NOTE 1 – Tout défaut détecté provoque la production d'un signal AIS/FDI de couche client qui est transporté en aval. Selon la couche spécifique, un signal AIS/FDI peut être détecté par une fonction collectrice d'adaptation ou de terminaison de chemin. NOTE 2 – Le défaut EXC ne contribue pas à une condition TSF et ne constitue donc qu'une condition de déclenchement local dans la couche de réseau protégée (par TSFprot) et non dans toute couche client. NOTE 3 – Les défauts de concaténation virtuelle ne sont applicables que dans le procédé LCAS.			

22.2 Aperçu général des conditions de déclenchement du signal SD

Le Tableau 3 présente un aperçu général des défauts qui contribuent aux conditions de déclenchement du signal SD dans plusieurs techniques de transmission. Voir les Recommandations relatives aux équipements (par exemple, Recommendations UIT-T G.783, G.798) concernant les spécifications particulières au signal SD.

Tableau 3/G.808.1 – Aperçu général des défauts contribuant à la condition de signal SD

	ATM	OTN	SDH
Dégradations numériques	Néant	DEG	DEG
Dégradations optiques	Non applicable	A étudier (Note)	Néant
NOTE – Les seuils des dégradations optiques feront l'objet d'une étude complémentaire. La question de savoir si les défauts du signal de surdébit de réseau OTN (OOS) contribuent ou non à la condition SD fera l'objet d'une étude complémentaire car le signal OOS n'est pas encore spécifié.			

23 Attribution des circuits de service et de protection

La commutation de protection linéaire 1+1 (doublée) peut être utilisée en tant qu'application de protection d'un anneau physique. Comme l'anneau fait souvent partie d'un plus grand réseau et que seule une portion du chemin traverse l'anneau, cette application est normalement utilisée pour des entités de transport sur une connexion de sous-réseau.

Le trafic dans les deux sens peut être configuré de deux façons:

- les entités de transport en service dans les deux sens peuvent suivre **différents** trajets physiques et l'ensemble de l'anneau peut être utilisé. Cette application est appelée anneau de commutation de trajet unidirectionnelle (UPSR, *unidirectional path switch ring*) et est représentée à la Figure 36. Elle est définie dans le réseau SONET. En général, elle peut être utilisée dans les architectures de protection SNC/I et SNC/N. Elle ne devrait pas être utilisée dans les architectures de protection SNC/S et de protection de chemin.

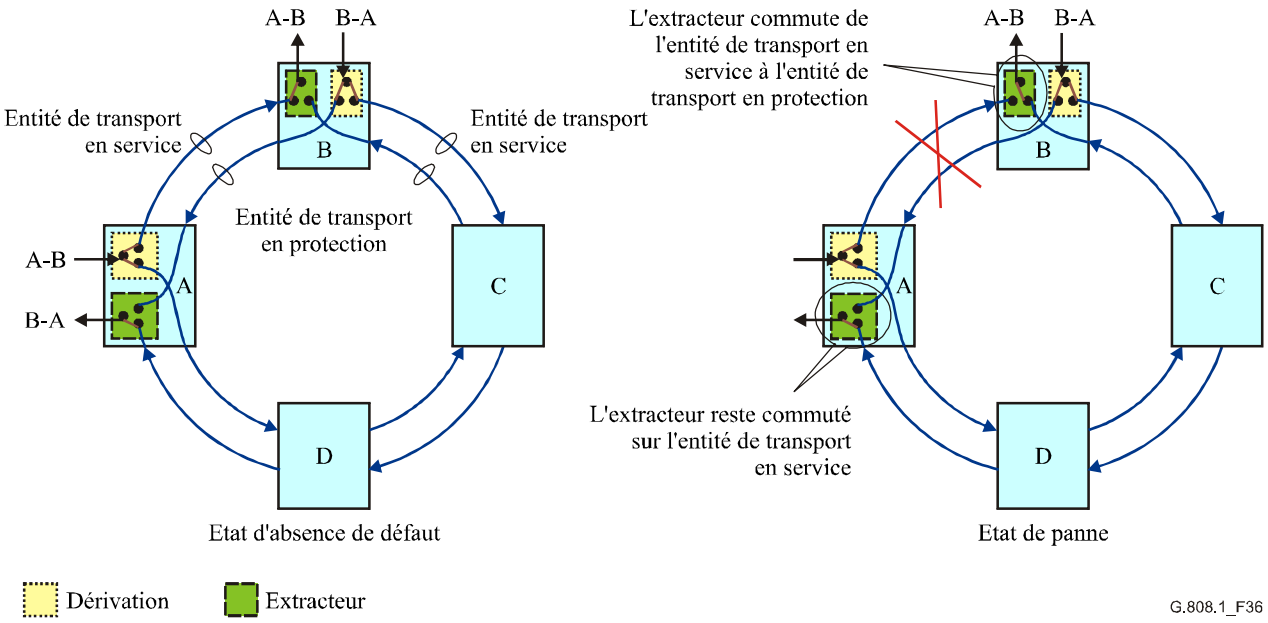


Figure 36/G.808.1 – Anneau de commutation de trajet unidirectionnelle (UPSR)

- Les entités de transport en service dans les deux sens suivent le **même** trajet physique, normalement le plus court. Les entités de transport en protection utiliseront l'autre portion de l'anneau. Cette application est représentée à la Figure 37 et est appelée protection de connexion *SNC* (SNCP, *subnetwork connection protection*). Dans une situation exempte de défaut, cette application minimise le temps de transfert et est identique dans les deux sens. Elle est définie dans les réseaux SDH, OTN et ATM, et peut être utilisée dans toutes les architectures de protection. Les anneaux de commutation de trajet dans un seul sens peuvent également être actionnés de cette façon.

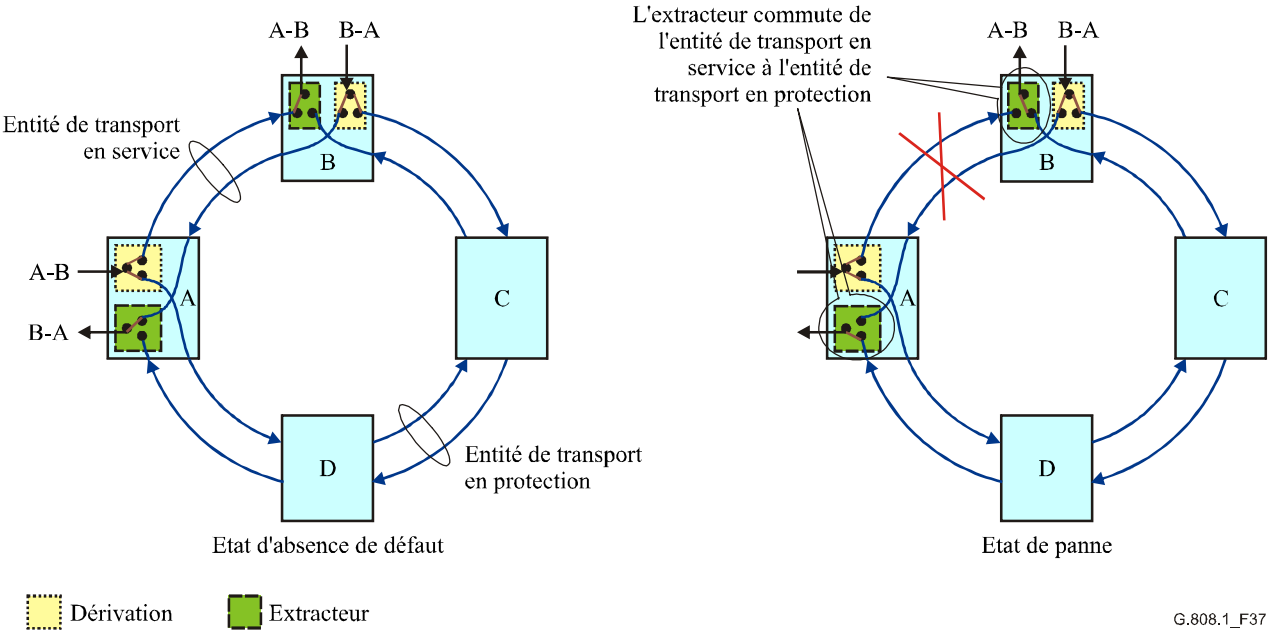


Figure 37/G.808.1 – Anneau de protection de connexion SNC (SNCP)

24 Protocole de commutation APS

Les définitions génériques des types de protocole de commutation APS sont traitées au § 3.3.2. Le présent paragraphe concerne les caractéristiques comportementales des protocoles et leur applicabilité aux différentes architectures de protection définies par la présente Recommandation. Les détails exacts des procédés de codage protocolaire et l'identification des canaux de surdébit utilisés pour le transport des protocoles sont définis par les Recommandations traitant spécifiquement des techniques de commutation de protection (par exemple, les Recommandations UIT-T G.841, G.873.1 et I.630).

Protocole à 3 phases

– pour tous types d'architecture;

– empêche une erreur de connexion en toutes circonstances;

– n'actionne un extracteur ou une dérivation qu'après confirmation de priorité.

Protocole à 2 phases

– pour architectures en 1+1 et $(1:1)^n$;

– temps de protection de commutation plus court.

Protocole à 1 phase

– pour architectures en 1+1 et $(1:1)^n$;

– temps de protection de commutation le plus court;

– actionne la dérivation ou l'extracteur avant confirmation de priorité;

– protocole plus complexe.

24.1 Protocole à 1 phase

Moyen d'aligner les deux extrémités du domaine protégé par l'échange d'un seul message (Z → A).

Applicable aux architectures en $(1:1)^n$ et 1+1.

La dérivation ou l'extracteur se trouvant au nœud Z est actionné avant de savoir si la condition du nœud Z a priorité sur la condition au nœud A.

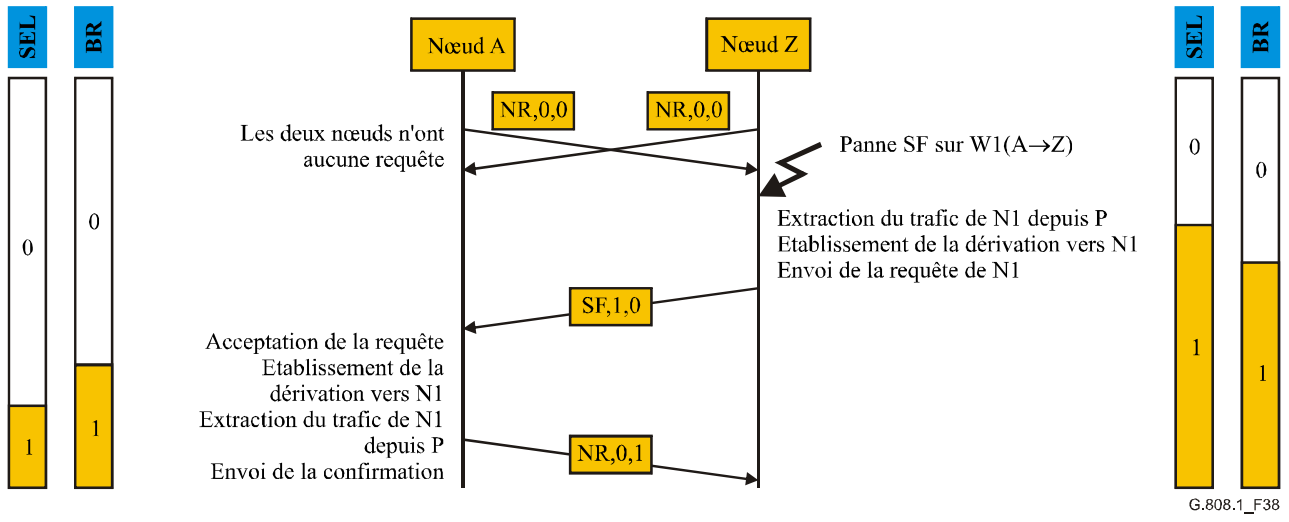


Figure 38/G.808.1 – Exemple de protocole à 1 phase

24.2 Protocole à 2 phases

Moyen d'aligner les deux extrémités du domaine protégé par l'échange de deux messages (Z → A, A → Z).

Applicable dans les architectures en $(1:1)^n$ et en 1+1 avec leurs dérivations permanentes.

En architecture en $(1:1)^n$, le nœud Z n'effectue aucune commutation jusqu'à ce que le nœud A confirme la priorité de la condition se trouvant en Z. Lorsque le nœud A confirme la priorité, il actionne l'extracteur et la dérivation. Dès réception de la confirmation, Z actionne son extracteur et la dérivation.

En architecture en 1+1 avec dérivation permanente, l'extracteur est actionné uniquement comme indiqué pour l'architecture en $(1:1)^n$.

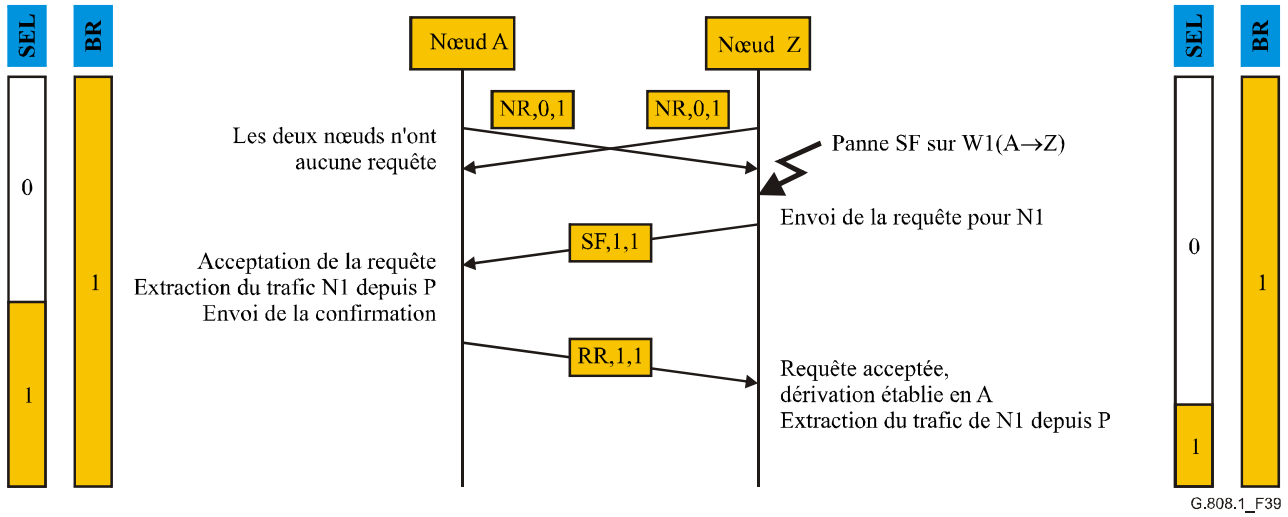


Figure 39/G.808.1 – Exemple de protocole à 2 phases

24.3 Protocole à 3 phases

Moyen d'aligner les deux extrémités du domaine protégé par l'échange de trois messages (Z → A, A → Z, Z → A).

Applicable aux architectures en 1:n et m:n ainsi qu'aux architectures en 1+1 avec leurs dérivations permanentes.

Dans le cas des architectures en 1:n et m:n, le nœud Z n'effectue aucune commutation jusqu'à ce que le nœud A confirme la priorité de la condition se trouvant en Z. Lorsque le nœud A confirme la priorité, il actionne la dérivation. Dès réception de la confirmation, Z actionne son extracteur et la dérivation puis indique l'action de dérivation à A qui, finalement, actionne son extracteur.

Dans le cas de l'architecture 1+1 avec ses dérivations permanentes, les extracteurs ne sont actionnés que comme décrit pour le cas 1:n.

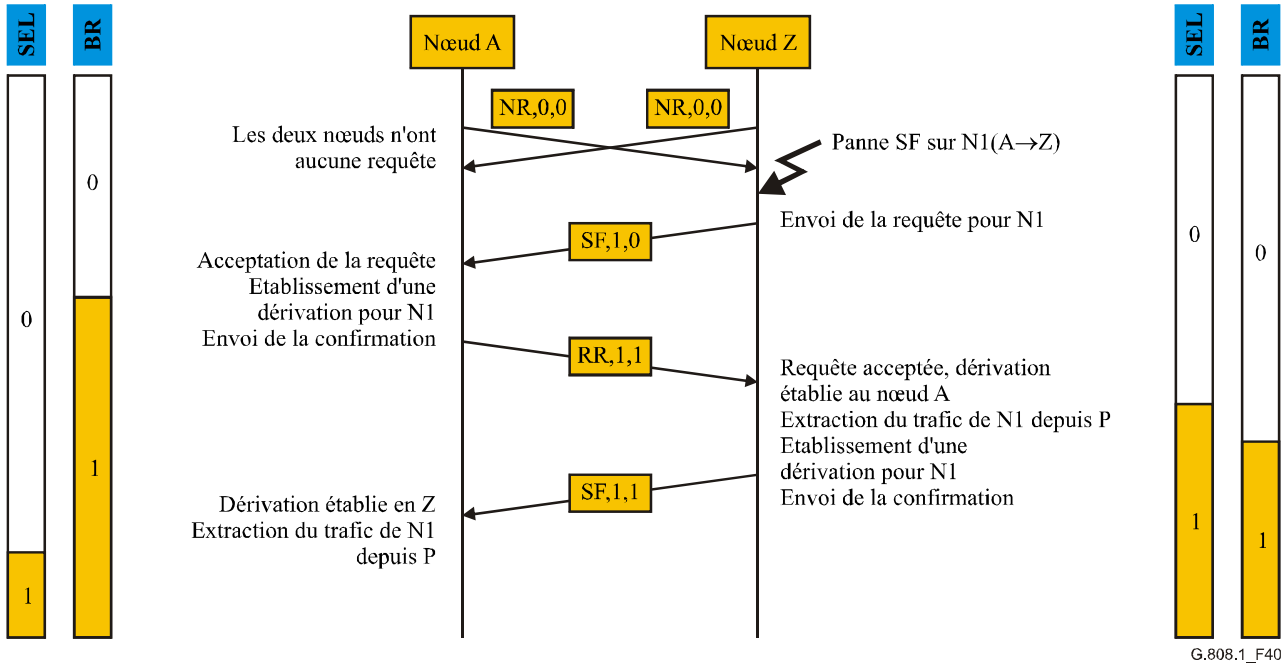


Figure 40/G.808.1 – Exemple de protocole à 3 phases

Appendice I

Implémentation du temporisateur d'attente de protection

Une implémentation d'un temporisateur d'attente de protection peut utiliser un compteur, qui est décrémenté toutes les X millisecondes. Cette quantification apporte une limite de précision lors de la détermination du temps d'attente de protection. La Figure I.1 présente deux exemples d'action de décrémentation: toutes les 10 ms [25 ms]. Pour un temps d'attente de protection de 100 ms, le compteur de temps d'attente peut être chargé avec une valeur de 10 [4] au moment de l'apparition de la condition SF/SD, peut être décrémenté à la fin de chaque période de décrémentation toutes les 10 ms [25 ms] et arrive à expiration lorsqu'il atteint la valeur 0. Le temps d'attente de protection déterminé dans cette implémentation est de 95 ± 5 ms [82,5 ± 12,5 ms].

NOTE – Dans le cas d'une période de décrémentation de 100 ms, le temps d'attente de protection de 100 ms est en fait de 50 ± 50 ms, c'est-à-dire compris entre 0 ms et 100 ms.

Au lieu d'être chargé avec une valeur de 10 [4], le compteur peut être chargé avec une valeur de 11 [5], ce qui détermine un temps d'attente de protection de 105 ± 5 ms [112,5 ± 12,5 ms].

La précision de ce type de temporisateur d'attente de protection est 0,5 fois la période de décrémentation.

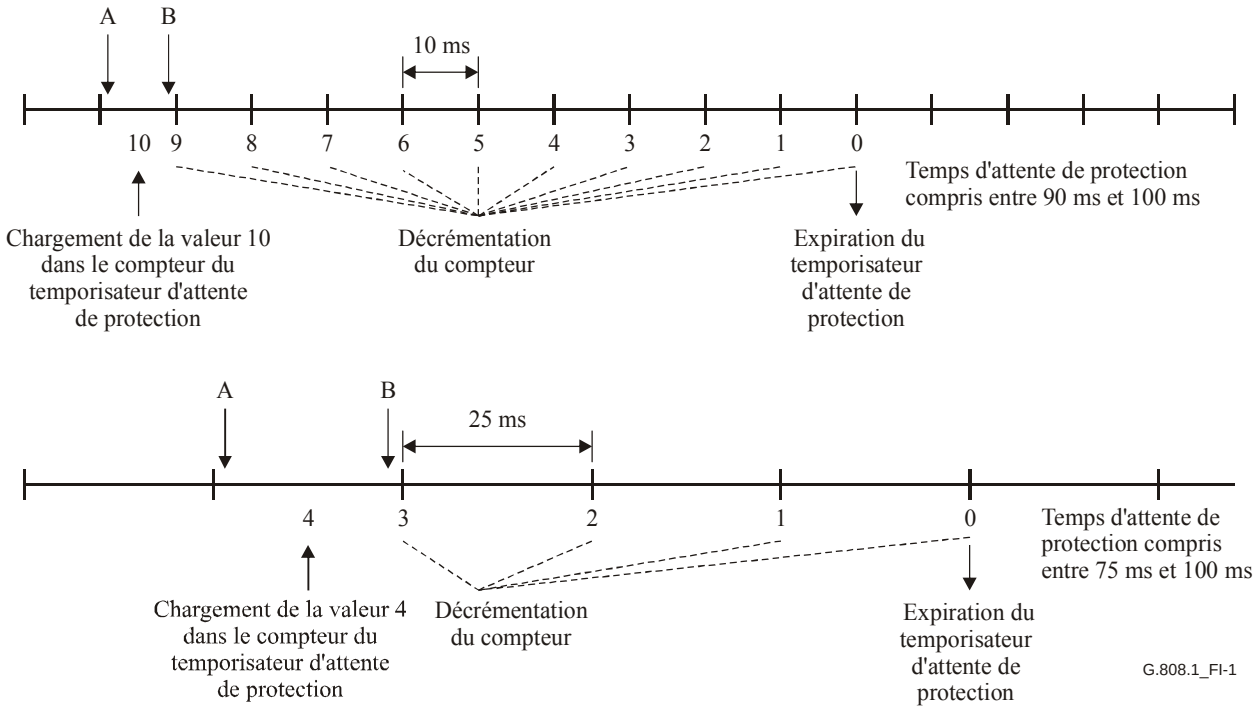


Figure I.1/G.808.1 – Précision du temporisateur d'attente de protection

Avec une période de décrémentation de 10 ms, l'effet des différences de temps de transfert entre entités de transport en service et en protection dans une protection SNC/I ou SNC/N de type 1+1 peut être compensé lorsqu'un temps d'attente de protection égal à "0" est extrait. Lorsque le temporisateur d'attente de protection est réellement utilisé (au lieu d'être désactivé) et lorsque le compteur est chargé avec une valeur de "2", des intervalles différentiels de 10 ms peuvent être compensés. Voir la Rec. UIT-T G.873.1.

Appendice II

Conditions automatiques (SF, SD) en protection de groupe de connexions SNC

En protection SNC/N [et SNC/I] de type 1+1, les conditions SF et SD pour le groupe sont celles des groupes SFG et SDG qui entrent dans le processus de protection de connexion SNC. La logique de calcul des conditions des groupes SFG et SDG fonctionne comme suit:

- groupe SFG d'entités en service = (W-SF1 et non P-SF1) ou (W-SF2 et non P-SF2) ou etc.
- groupe SFG d'entités en protection = (P-SF1 et non W-SF1) ou (P-SF2 et non W-SF2) ou etc.
- groupe SDG d'entités en service = (W-SD1 et non P-SD1) ou (W-SD2 et non P-SD2) ou etc.
- groupe SDG d'entités en protection = (P-SD1 et non W-SD1) ou (P-SD2 et non W-SD2) ou etc.

Cette définition des groupes SFG et SDG permet de différencier un défaut se produisant "en face" ou "à l'intérieur" du domaine protégé. Un défaut dans un certain signal en face du domaine protégé va n'activer ni W-SFG [SDG] ni P-SFG [SDG], alors que le terme SF-i sera activé dans les deux faisceaux W et P; les termes "(W-SF-i et non P-SF-i)" et "(P-SF-i et non W-SF-i)" auront cependant la valeur "faux".

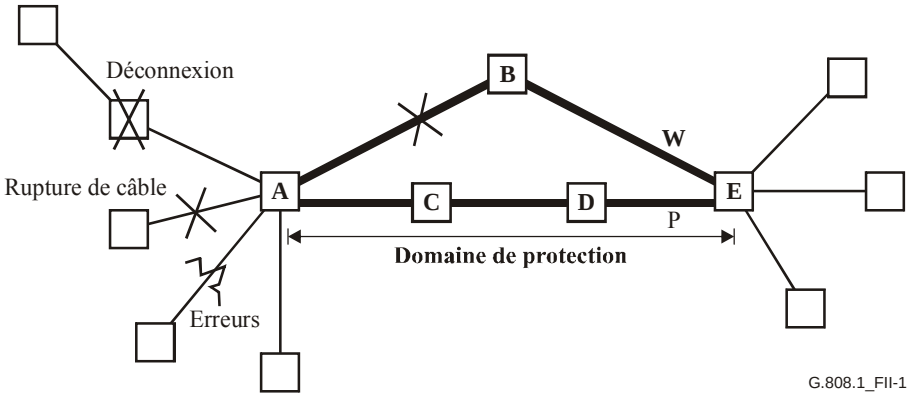


Figure II.1/G.808.1 – Exemple de défaut à l'intérieur du domaine protégé

Un défaut entre éléments de réseau (NE) en A et en B (Figure II.1) provoquera l'activation du groupe W-SFG [ou W-SDG]. S'il s'agit d'un défaut de signal serveur, tous les signaux contenus dans le faisceau rencontreront une condition de signal SF. S'il s'agit d'un défaut de connexité, un signal donné peut rencontrer une condition de signal SF. Les deux situations provoqueront l'activation du groupe W-SFG.

Si par exemple une déconnexion ou une rupture de câble se produit en même temps avant l'élément de réseau A (et touche un des signaux du groupe), les termes W-SF-i et P-SF-i seront actifs. Si le défaut apparaissant dans le domaine de protection est un défaut de couche serveur, le groupe W-SFG reste actif et le groupe P-SFG est inactif. Dans l'autre cas (défaut de connexité dans le domaine de protection), le groupe sera commuté si les signaux défectueux situés en face et à l'intérieur du domaine de protection sont différents.

NOTE – Le cas particulier où tous les signaux sont déjà devenus défectueux avant d'atteindre le domaine de protection provoque l'inactivation des groupes W-SFG et P-SFG. Mais ce cas particulier ne perturbe pas le fonctionnement du processus de protection car il ne reste plus rien à protéger.

Les erreurs/défauts dans le domaine protégé qui déclenchent des signaux AIS et DEG effectuent cette action pour tous les membres du groupe au même moment (en supposant que tous les signaux dans le groupe soient tenus d'être *transportés dans le même signal serveur)*. En tant que telle, la "combinaison par opérateur OU" des conditions SF et SD individuelles peut être utilisée comme déclencheur.

Concernant une perte de signal (par exemple, perte de continuité, conteneur non équipé) ou un défaut de connexité (par exemple, discordance entre identificateurs de repérage), ce comportement de groupe pourrait être absent. Les signaux sont (en principe) brassés individuellement dans chaque élément de réseau. En tant que telle, la combinaison par opérateur OU des signaux individuels déclenchera une commutation de protection pour le groupe lorsqu'un seul (ou un sous-ensemble) des signaux présente une condition de défaut par perte de signal. C'est la *conséquence de la réduction de complexité*.

Appendice III

Observations relatives à l'implémentation

On possède et on utilise actuellement une technologie dans laquelle des éléments de réseau en hiérarchie SDH ou en un autre mode (par exemple, ATM, OTN) se composent "d'unités d'interface (PU, *port unit*)" et "d'unités de commutation". Les unités de commutation effectuent le brassage/la commutation, tandis que les unités d'interface effectuent tout le traitement nécessaire du surdébit de la hiérarchie SDH [ou PDH] (et du flux OAM en mode ATM).

Dans des éléments de réseau (NE, *network element*) brassant des conteneurs VC-12 en hiérarchie SDH, une unité d'interface effectuera le traitement du surdébit de section (SOH, *section overhead*), du pointeur des unités AU4, du surdébit des conteneurs VC-4 et du pointeur des unités TU12 (Figure III.1). Après ce traitement, les signaux de conteneurs VC-12 en hiérarchie SDH résultants sont transférés à l'unité de commutation afin d'être routés vers leurs unités d'interface de sortie respectives.

Il est possible d'utiliser la même unité de terminaison lorsque cette terminaison n'est pas le point d'aboutissement du conteneur VC-4, mais un point de retransmission en transit de ce conteneur.

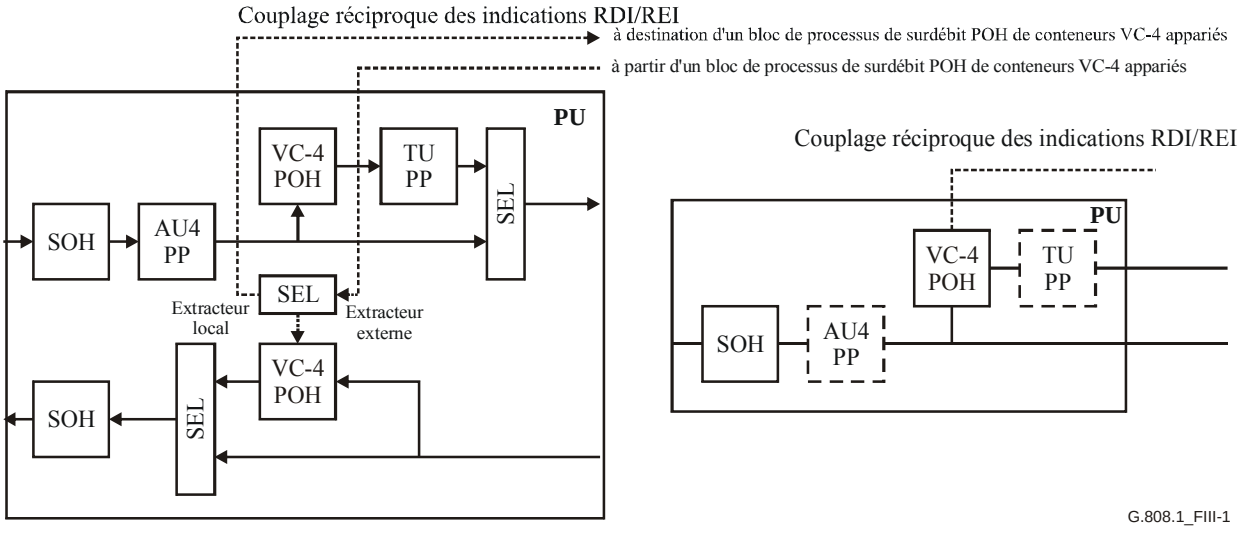


Figure III.1/G.808.1 – Vue détaillée (à gauche) et vue comprimée (à droite) d'une unité d'interface (fonctionnalité de base seulement)

III.1 Analyse

Considérons par exemple le cas de la protection doublée d'une section multiplex (Figure III.2); deux unités d'interface sont utilisées à cette fin, chacune avec un dispositif matériel exécutant le traitement du surdébit de section, des pointeurs d'unité AU, du surdébit de conduit de conteneurs VC-4 et des pointeurs d'unité TU, tandis que la commutation de protection est réalisée par l'unité de commutation pour tout le groupe de signaux de conteneurs d'ordre inférieur (LOVC).

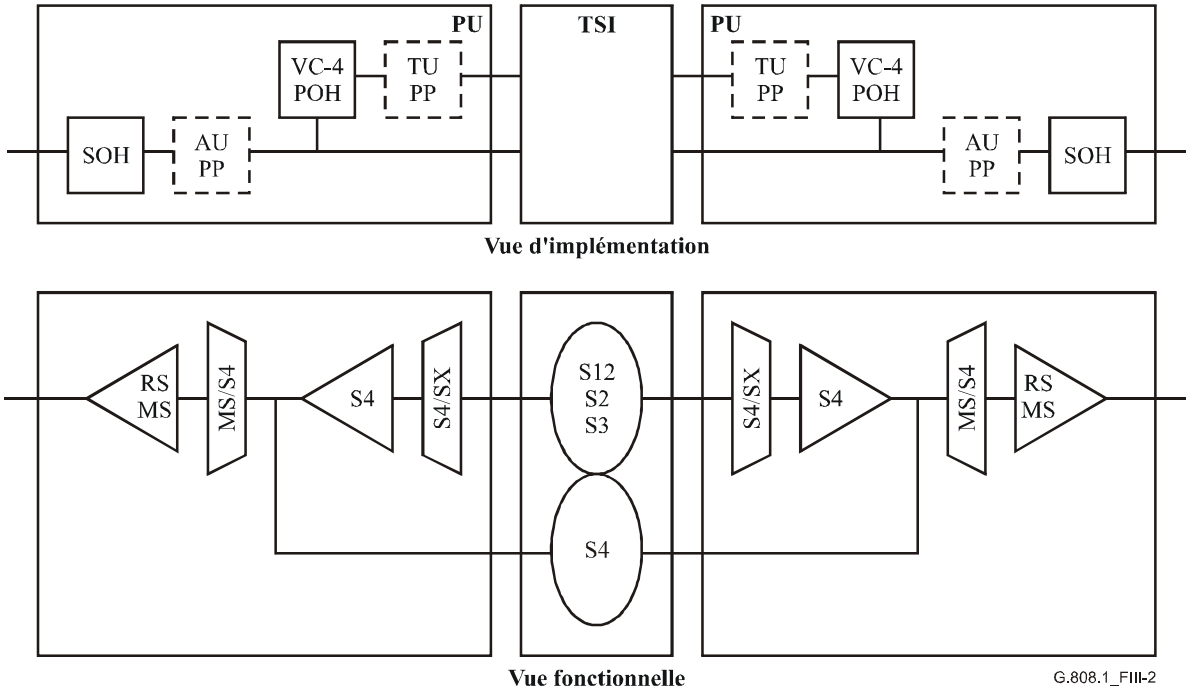


Figure III.2/G.808.1 – Mappage de la vue d'implémentation dans la vue fonctionnelle: fonctionnement de base

Conformément au modèle fonctionnel, un trop grand nombre de fonctions sont présentes (Figure III.3); c'est-à-dire que le traitement de surdébit de section devrait être présent deux fois, alors que le traitement des pointeurs AU, du surdébit de conduit VC-4 et des pointeurs TU ne devrait être présent qu'une seule fois.

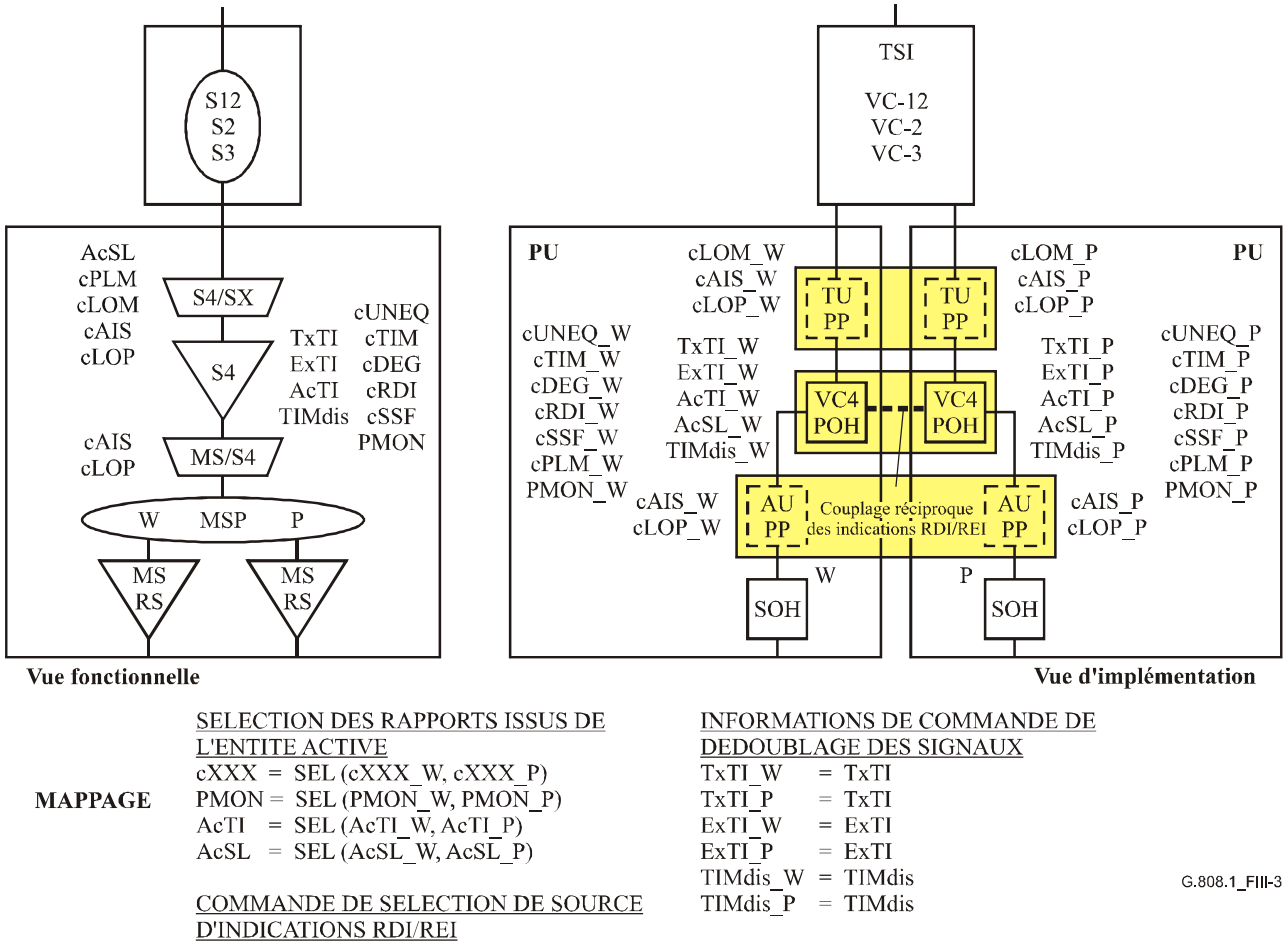


Figure III.3/G.808.1 – Mappage de la vue d'implémentation dans la vue fonctionnelle: protection de section multiplex

Avec ce logiciel, un élément de réseau peut présenter la fonctionnalité attendue; il masque au gestionnaire les processus en réserve de traitement de pointeurs AU, de surdébit POH de conteneurs VC-4 et de pointeurs TU.

Un masquage est également requis pour les interfaces de transmission; les deux unités d'interface avec les modules STM-N sont appelées à produire les mêmes unités AU4, les mêmes conteneurs VC-4 et les mêmes unités TU.

L'implémentation la plus simple produira des unités AU et TU "différentes" en ce sens que la valeur réelle du pointeur n'est pas tenue d'être la même dans les signaux de module STM-N en service et en protection.

Le fait que les valeurs de pointeur d'unité AU/TU peuvent être différentes n'a aucune incidence sur le fonctionnement du réseau. C'est-à-dire que cette "non-conformité" au sens propre est sans conséquence et ne requiert aucune compensation.

Tel n'est cependant pas le cas pour le traitement du surdébit de conduit de conteneurs VC-4, où il est nécessaire de s'assurer que les signaux d'indication RDI et REI, produits au moyen des deux unités d'interface avec les modules STM-N, sont identiques. C'est-à-dire que le processus de surveillance du surdébit POH des conteneurs VC-4, situé dans l'unité d'interface active avec les modules STM-N, doit toujours réexpédier ses signaux RI_RDI/RI_REI vers les processus de production de préfixe POH de VC-4 des deux unités d'interface (service et protection).

Le même traitement est requis lorsque la protection de connexion SNC de conteneurs VC-4 est sélectionnée à la place de la protection de section multiplex (Figure III.4).

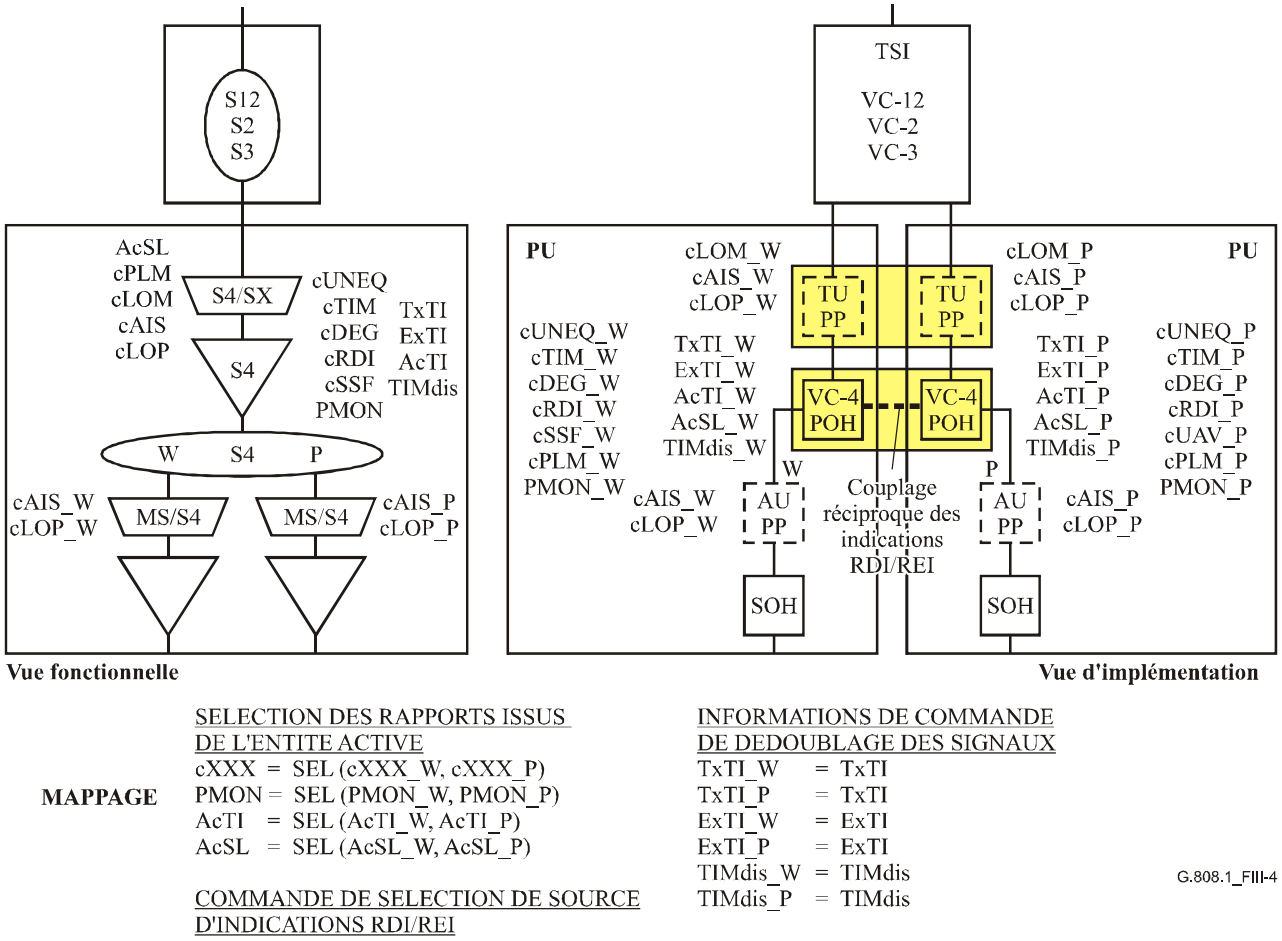


Figure III.4/G.808.1 – Mappage de la vue d'implémentation dans la vue fonctionnelle: protection SNC/I de VC-4

Si le couplage réciproque d'indications RDI/REI n'est pas implémenté, il n'est pas possible d'ajouter la surveillance de qualité selon la Rec. UIT-T G.826 aux réseaux dans lesquels les implémentations de protection ci-dessus sont opérationnelles. La Rec. UIT-T G.826 prescrit que la surveillance de qualité (sur la base des services) doit être prise en charge dans les deux sens, ce qui nécessite l'utilisation des informations distantes, qui doivent toujours représenter les erreurs/défauts détectés dans le trajet du signal qui transporte réellement les informations de couche client.

La commutation unidirectionnelle conduit chaque extrémité de l'arc de protection à effectuer une sélection indépendante entre chemins/connexions SNC de service et de protection. Si la connexion SNC de VC-4 en service est sélectionnée dans le sens A → Z et la connexion SNC de VC-4 sélectionnée en protection dans le sens Z → A, les informations distantes extraites à chaque extrémité sont insérées par le générateur de surdébit POH de VC-4 dans l'unité d'interface en réserve, c'est-à-dire dans celle qui n'est pas sélectionnée à cette extrémité. Si cette unité utilisait (maintenant) ses signaux RI_RDI/RI_REI locaux (à la place de ses signaux RI_RDI/RI_REI jumelés), l'extrémité distante recevrait des informations distantes sans relation avec le conteneur VC-4 réellement sélectionné.

Les journaux de surveillance de qualité bidirectionnelle représenteraient (dans ce cas) des informations erronées et ne pourraient donc pas être utilisés.

Le même problème se pose évidemment avec les journaux distants de surveillance unidirectionnelle (sur la base de la maintenance).

Dans le cas d'un élément de réseau en routage à 64 kbit/s comportant des interfaces avec des modules STM-N, le même problème se pose au niveau des conteneurs VC-12.

NOTE – Les Figures III.3 et III.4 ne représentent la situation que du point de vue des indications RDI/REI. Ces figures ne montrent pas les fonctions de surveillance de terminaison de connexion en cascade/de segment, ou de surveillance non intrusive, qui sont appelées à commander la commutation de protection.

Appendice IV

Exemple de protection $(1:1)^n$ (multidoublée)

Le présent appendice donne un exemple de commutation de protection en $(1:1)^n$ (multidoublée) (avec n = 3) dans un réseau en mode ATM. Dans ce cas, il y a trois entités de trafic routées en diversité et protégées par une seule entité de protection qui, en fonctionnement normal, transporte du trafic supplémentaire. L'entité de protection doit toujours avoir une largeur de bande suffisante afin de transporter le plus grand des trois signaux de trafic normal ou le signal de trafic supplémentaire. Chacune des entités de trafic est un conduit virtuel ATM dont la largeur et l'identificateur de conduit virtuel (VPI, *virtual path identifier*) sont indiqués dans la Figure IV.1.

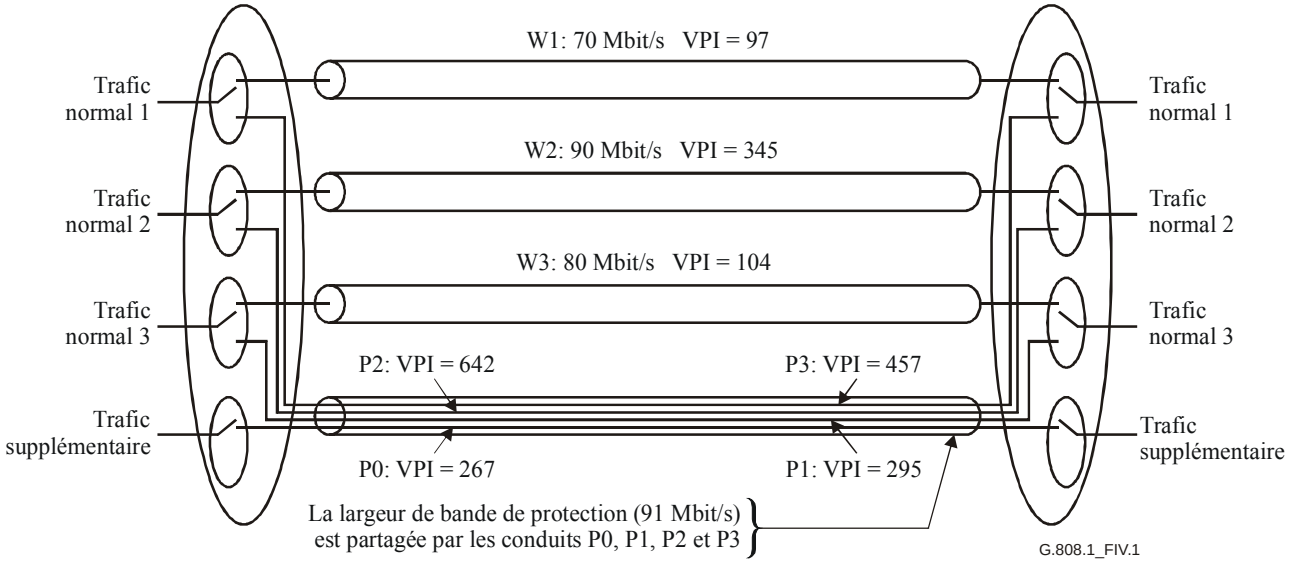


Figure IV.1/G.808.1 – Exemple de protection (1:1)n (multidoublée)

Dans cet exemple, un débit de 90 Mbit/s plus les cellules OAM pour les conduits P0 (contenant le flux OAM de commutation VP-APS), P1, P2 et P3 est tenu d'assurer la commutation de protection. Dans le cas d'une commutation unidirectionnelle, un protocole à 1 phase peut être utilisé parce que, lorsqu'un état de défaut est détecté, il suffit qu'un signal soit envoyé par l'extrémité Z à l'extrémité A afin de déclencher la commutation au niveau de la dérivation. Aucune erreur de connexion ne peut se produire étant donné que ce signal, qui se trouve sur l'entité de protection, est identifié sans équivoque par son VPI.

Appendice V

Cas particuliers d'autorétablissement de chemins à multiplexage inverse

V.1 Capacité d'autorétablissement offerte par le procédé LCAS

Lorsqu'on utilise la capacité de multiplexage inverse VCAT + LCAS où Y = Y-Xv et Z = Y-Xc et lorsque le groupe IMG est équivalent à un groupe VCG, on obtient le cas particulier suivant.

L'information AI est transportée au moyen d'un groupe de concaténations virtuelles (VCG, *virtual concatenation group*) ayant X membres (conteneurs VC_n_Xv, unités ODUk_Xv), répartis sur N routes, où

- tous les membres appartenant au groupe VCG ont la même largeur de bande;
- la largeur de bande du groupe VCG est proportionnelle au nombre de membres actifs;
- N est le nombre de routes ($1 \leq N \leq X$) contenant chacune une ou plusieurs connexions de réseau dans le groupe VCG;
- X est le nombre de membres du groupe VCG appelés à transporter l'information AI sur la largeur de bande de couche client + capacité de trafic supplémentaire/de protection Z ($X \geq 1, Z \geq 0$);
- X_{ACT} est la charge utile effectivement transportée ($0 \leq X_{ACT} \leq X$); en raison de la panne d'un ou de plusieurs des chemins, la largeur de bande d'un ou de plusieurs membres du groupe VCG ne sera pas utilisée afin de transporter l'information AI.

Pour transporter un signal à 10 Mbit/s, un conteneur VC-12-5v est requis. Cinq chemins de conteneurs VC-12 sont établis dans ce groupe VCG, dont deux sont aiguillés vers la route 1 et trois vers la route 2 (Figure V.1). Dans ce cas particulier, la largeur de bande autorétablissable est de 2 × VC-12 ou 40% et la largeur de bande non autorétablissable est de 3 × VC-12 ou 60%. Si un chemin supplémentaire de conteneurs VC-12 avait été configuré (E = 1) et aiguillé vers la route 1, la largeur de bande autorétablissable aurait été de 3 × VC-12 ou 60% et la largeur de bande non protégée aurait été de 2 × VC-12 ou 40%.

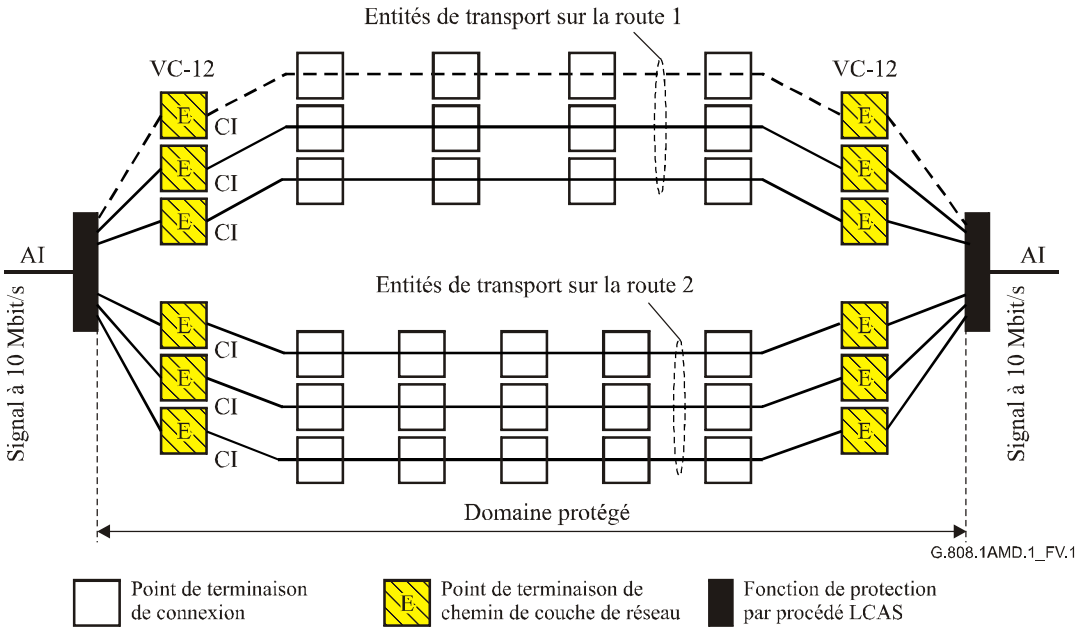


Figure V.1/G.808.1 – Exemple de capacité d'autorétablissement par procédé LCAS pour un signal à 10 Mbit/s sur des chemins VC-12-(X+E)v (X = 5, E = 0,1)

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2007