UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

I.630

(02/99)

SÉRIE I: RÉSEAU NUMÉRIQUE À INTÉGRATION DE SERVICES

Principes de maintenance

Commutation de protection ATM

Recommandation UIT-T I.630

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE I

RÉSEAU NUMÉRIQUE À INTÉGRATION DE SERVICES

STRUCTURE GÉNÉRALE	
Terminologie	I.110–I.119
Description du RNIS	I.120–I.129
Méthodes générales de modélisation	I.130–I.139
Attributs des réseaux et des services de télécommunication	I.140–I.149
Description générale du mode de transfert asynchrone	I.150–I.199
CAPACITÉS DE SERVICE	
Aperçu général	I.200–I.209
Aspects généraux des services du RNIS	I.210–I.219
Aspects communs des services du RNIS	I.220–I.229
Services supports assurés par un RNIS	I.230–I.239
Téléservices assurés par un RNIS	I.240–I.249
Services complémentaires dans le RNIS	I.250–I.299
ASPECTS GÉNÉRAUX ET FONCTIONS GLOBALES DU RÉSEAU	
Principes fonctionnels du réseau	I.310–I.319
Modèles de référence	I.320–I.329
Numérotage, adressage et acheminement	I.330–I.339
Types de connexion	I.340–I.349
Objectifs de performance	I.350–I.359
Caractéristiques des couches protocolaires	I.360–I.369
Fonctions et caractéristiques générales du réseau	I.370–I.399
INTERFACES UTILISATEUR-RÉSEAU RNIS	
Application des Recommandations de la série I aux interfaces utilisateur-réseau RNIS	I.420–I.429
Recommandations relatives à la couche 1	I.430–I.439
Recommandations relatives à la couche 2	I.440–I.449
Recommandations relatives à la couche 3	I.450–I.459
Multiplexage, adaptation de débit et support d'interfaces existantes	I.460–I.469
Aspects du RNIS affectant les caractéristiques des terminaux	I.470–I.499
INTERFACES ENTRE RÉSEAUX	I.500–I.599
PRINCIPES DE MAINTENANCE	**I.600–I.699**
ASPECTS ÉQUIPEMENTS DU RNIS-LB	
Equipements ATM	I.730–I.739
Fonctions de transport	I.740–I.749
Gestion des équipements ATM	I.750–I.799

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

RECOMMANDATION UIT-T I.630

COMMUTATION DE PROTECTION ATM

Résumé

La présente Recommandation "Commutation de protection ATM" définit les architectures et les mécanismes de commutation de protection au niveau de la couche ATM. Cette architecture est définie par l'étendue et la configuration du domaine protégé. Les ressources de protection sont attribuées à l'avance. Le mécanisme de protection fait intervenir des déclencheurs, des mécanismes de blocage et le protocole de commande de la commutation de protection.

La présente Recommandation décrit la protection de VP/VC individuelle et aussi de groupe. La protection de VP/VC individuelle est une technique dans laquelle on utilise une seule connexion de réseau ou de sous-réseau pour l'entité active et l'entité de protection. La protection de groupe est une technique dans laquelle un faisceau logique d'une ou plusieurs connexions de réseau ou de sous-réseau sont utilisées pour l'entité active et l'entité de protection.

Dans l'état actuel, la présente Recommandation décrit la commutation de protection bidirectionnelle 1+1 et 1:1 ainsi que la commutation de protection unidirectionnelle 1+1.

Source

La Recommandation UIT-T I.630, élaborée par la Commission d'études 13 (1997-2000) de l'UIT-T, a été approuvée le 26 février 1999 selon la procédure définie dans la Résolution n° 1 de la CMNT.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT avait 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 I.630

COMMUTATION DE PROTECTION ATM

(Genève, 1999)

1 Domaine d'application

La présente Recommandation définit les architectures et les mécanismes de commutation de protection ATM pour les VP/VC et la commutation de protection ATM pour les faisceaux VP. L'architecture décrit l'étendue et la configuration du domaine protégé ainsi que les politiques d'attribution des ressources. Le mécanisme décrit le déclencheur de commutation de protection, les mécanismes de blocage et le protocole de commande de la commutation de protection. La méthodologie de modélisation définie dans les Recommandations G.805 [2] et I.326 [4] est utilisée ici pour décrire l'architecture de commutation de protection ATM VP/VC et l'architecture de commutation de protection ATM de groupe VP/VC.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui de ce fait en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

[1] Recommandation UIT-T G.707 (1996), *Interface de nœud de réseau pour la hiérarchie numérique synchrone.*

[2] Recommandation UIT-T G.805 (1995), *Architecture fonctionnelle générale des réseaux de transport*.

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

[4] Recommandation UIT-T I.326 (1995), *Architecture fonctionnelle des réseaux de transport fondée sur le mode ATM*.

[5] Recommandation UIT-T I.610 (1999), *Principes et fonctions d'exploitation et de maintenance du RNIS à large bande.*

[6] Recommandation UIT-T I.732 (1996), *Caractéristiques fonctionnelles des équipements ATM*.

[7] Recommandation CCITT M.495 (1988), *Rétablissement de transmission et diversité de routage de transmission: terminologie et principes généraux.*

[8] Recommandation UIT-T M.3010 (1996), *Principes des réseaux de gestion des télécommunications.*

[9] Recommandation UIT-T M.3300 (1998), *Prescriptions pour l'interface F du réseau de gestion des télécommunications.*

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 VCC de commutation automatique de protection (APS): connexion par canal virtuel (VCC) utilisée pour la commande, définie sur l'étendue du domaine protégé et faisant partie d'un groupe de canaux virtuels, (VCG). Elle aide à l'évaluation de la qualité du VCG associé et sert de conduit pour les messages du protocole de commande de commutation de protection. Il y a une connexion VCC d'APS pour chaque groupe VCG_W et une connexion VCC d'APS pour chaque groupe VCG_P. La transmission des messages protocolaires de commande de commutation de protection se fait toujours sur la connexion VCC d'APS VCG_P.

3.2 VPC de commutation automatique de protection (APS): connexion par conduit virtuel (VPC) utilisée pour la commande, définie sur l'étendue du domaine protégé et faisant partie d'un groupe de conduits virtuels (VPG). Elle aide à l'évaluation de la qualité du VPG associé et sert de conduit aux messages du protocole de commande de commutation de protection. Il y a une connexion VPC d'APS pour chaque groupe VPG_W et une connexion VPC d'APS pour chaque groupe VPG_P. La transmission des messages protocolaires de commande de commutation de protection se fait toujours sur la connexion VPC d'APS VPG_P.

3.3 commutation de protection bidirectionnelle: architecture de commutation de protection dans laquelle une panne unidirectionnelle déclenche une commutation de protection sur les deux sens (du "cheminement", de la "connexion de sous-réseau", etc.), à savoir sur le sens affecté et sur le sens non affecté.

3.4 pont: (Pour une configuration 1+1) action ou fonction consistant à transmettre un trafic identique à la fois sur les entités en service et sur les entités de protection. (Pour une configuration 1:n) A définir.

3.5 point de connexion (CP, *connection point*): (voir Note 2 au 3.38.) points de référence définis sur une connexion de réseau et spécifiés sur une couche de réseau donnée. Les points de connexion définis sur la couche ATM sur une VPC (ou une VCC) sont situés à l'entrée et à la sortie d'un élément de réseau ATM (ou d'un équipement client), c'est-à-dire aux points où les fonctions de terminaison de liaison par VP (ou par VC) opèrent.

3.6 préattribution de ressources de protection spécialisées: politique d'attribution des ressources dans laquelle à la fois le trajet et la largeur de bande associés à l'entité de protection sont attribués à l'avance.

3.7 sortie: le point de sortie d'un élément de réseau ATM est représenté à la Figure 1.

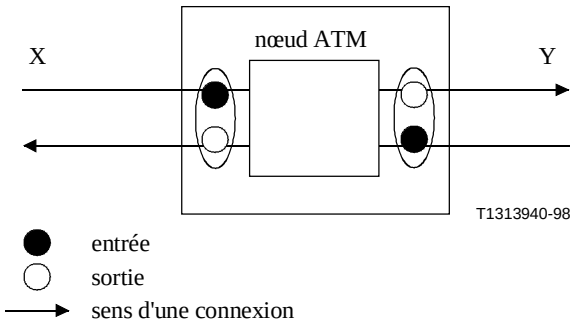


Figure 1/I.630 – Utilisation des termes entrée, sortie dans la Recommandation I.630

3.8 progressivité: se dit d'une action de survie de réseau déclenchée lorsque la fonction de survivabilité dans les couches inférieures n'a pas été exécutée.

3.9 trafic supplémentaire: trafic du priorité inférieure par rapport à celui qui est acheminé par l'entité active. Ce trafic est acheminé sur l'entité de protection, l'entité active étant en fonction. Le trafic supplémentaire n'est pas protégé, c'est-à-dire que lorsque l'entité de protection est sollicitée pour protéger le trafic acheminé sur l'entité active (en raison d'une panne ou d'une commutation forcée/manuelle), le trafic supplémentaire ne bénéficie d'aucune priorité.

3.10 commutation forcée pour l'entité active #n: action de commutation déclenchée par un opérateur. Cette action ne peut être déclenchée lorsqu'une panne de signal mobilise déjà l'entité de protection.

3.11 commutation de protection douce: commutation de protection qui ne provoque pas de perte ou de duplication de cellules, de désordre de cellule ou d'erreurs binaire.

3.12 temps de blocage: intervalle de temps qui s'écoule entre la détection d'une panne ou d'une dégradation de signal et sa confirmation en tant que condition nécessitant le lancement de la procédure de commutation de protection.

3.13 dégradation: défaut ou dégradation de performance qui peut conduire à une panne ou à une dégradation de signal.

3.14 entrée: point d'entrée d'un élément de réseau ATM illustré à la Figure 1.

3.15 nœud intermédiaire: nœud sur le trajet physique de l'entité active ou sur celui de l'entité de protection, situé entre la source et le puits du domaine protégé correspondant.

3.16 connexion de liaison: la définition se trouve dans la Recommandation G.805. Par exemple, une connexion de liaison par VP est délimitée par les points de connexion CP situés dans deux éléments de réseau ATM fonctionnant au niveau VP.

3.17 commutation manuelle: commutation déclenchée par un opérateur. Cette commutation est exécutée sauf si une requête de priorité plus élevée est en cours de traitement.

3.18 connexion matricielle: connexion de sous-réseau délimitée, pour la couche ATM, par les points CP situés à l'entrée et à la sortie d'un élément de réseau ATM (voir Note 2 au 3.38).

3.19 connexion de réseau: entité de transport utilisée pour transférer les informations d'utilisateur et les informations OAM entre les points d'extrémité de la connexion (TCP) (voir Note 2 au 3.38).

3.20 survivabilité du réseau: ensemble de capacités permettant à un réseau de rétablir le trafic affecté en cas d'une panne. Le degré de survivabilité est déterminé par la capacité du réseau à supporter des pannes simples, des pannes multiples et des pannes d'équipement.

3.21 commutation de protection non réversible: se dit d'une commutation de protection dans laquelle il n'y a pas d'action d'inversion (commutation permettant de revenir sur l'entité active) après réparation de l'entité active.

3.22 domaine protégé pour la couche ATM: définit par une ou plusieurs connexions VPC/VCC, ou bien par une partie ou bien par l'ensemble de ces connexions, pour lesquelles un mécanisme de survivabilité est assuré au cas où une dégradation affecterait une ou plusieurs de ces connexions selon le cas. Ce domaine commence après le sélecteur/pont d'un point d'extrémité et s'étend jusqu'au sélecteur/pont de l'autre point extrémité. Il exclut les fonctions de sélecteur/pont.

3.23 entité de protection: partie d'une connexion ATM VPC/VCC ou d'un groupe VPG/VCG à l'intérieur du domaine protégé en provenance duquel le trafic actif est reçu dans le puits du domaine protégé où une entité active est en dérangement.

3.24 commutation de protection: technique de survivabilité de réseau associée à une politique de préattribution des ressources de protection.

3.25 commutation de protection réversible: méthode de commutation de protection dans laquelle une action réversible (commutation avec retour à l'entité active) est prise après que l'entité active ait été réparée.

3.26 sélecteur: commutateur qui sélectionne le trafic en provenance de l'entité active ou de l'entité de protection.

3.27 connexion de sous-réseau: entité de transport correspondant à une partie d'une connexion de réseau. Une connexion de sous-réseau peut être scindée en une concaténation de connexions matricielles et de liaisons. Il existe un cas particulier dans lequel une connexion matricielle correspond à une connexion de sous-réseau unique (indivisible) (voir Note 2 au 3.38).

3.28 point de connexion de terminaison (TCP): points d'extrémité d'une connexion de réseau (voir Note 2 au 3.38).

3.29 chemin: "entité de transport" qui se compose d'une paire de "chemins unidirectionnels" associée capable de transférer simultanément de l'information dans des sens opposés, entre leurs entrées et sorties respectives (voir Note 2 au 3.38).

3.30 entité de transport: composante architecturelle qui transfère l'information entre ses entrées et ses sorties dans un réseau en couche (voir Note 2 au 3.38).

3.31 commutation de protection unidirectionnelle: architecture de commutation de protection dans laquelle une panne unidirectionnelle (c'est-à-dire une panne affectant simplement un sens de la transmission) déclenche une commutation de protection sur le sens affecté uniquement (du "chemin", de la "connexion de sous-réseau", etc.).

3.32 VCG_P: groupe VCG de remplacement physiquement diverse constitué de connexions de réseau ou de sous-réseau par VC de protection assignées à un ou à un ensemble de groupes VCG_W (dans le cas d'un fonctionnement de type 1:n).

3.33 VCG_W: groupe VCG constitué de connexions de réseau ou de sous-réseau par VC ATM actives acheminant le trafic protégé dans des conditions de fonctionnement normal.

3.34 groupe de canaux virtuels (VCG, *virtual channel group*): faisceau logique d'une ou de plusieurs connexions réseaux ou de sous-réseau par VC ATM qui partagent le ou les mêmes trajets à l'intérieur du domaine protégé.

3.35 groupe de conduits virtuels (VPG, *virtual path group*): faisceau logique d'une ou de plusieurs connexions réseaux ou de sous-réseau par VP ATM qui partagent le ou les mêmes trajets à l'intérieur du domaine protégé.

3.36 VPG_P: groupe VPG de remplacement physiquement divers constitué de connexions de réseau ou de sous-réseau VP de protection assignées à un ou à un ensemble de groupes VPG_W (dans le cas d'un fonctionnement de type 1:n).

3.37 VPG_W: groupe VPG constitué de connexions de réseau ou de sous-réseau par VP ATM actives acheminant le trafic protégé dans des conditions de fonctionnement normal.

3.38 entité active: partie de connexion par VPC/VCC ATM ou de groupe VPG/VCG ATM à l'intérieur du domaine protégé à partir de laquelle le trafic actif est reçu au niveau du puits du domaine protégé en l'absence de panne dans le mode réversible.

NOTE 1 – Cette fonction est différente de la fonction "pont" définie dans la Recommandation G.841 [3].

NOTE 2 – La Recommandation G.805 contient une définition plus générale et détaillée.

4 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes:

AIS	signal d'indication d'alarme (*alarm indication signal*)
AN	réseau d'accès (*access network*)
APS	commutation automatique de protection (*automatic protection switching*)
ATM	mode de transfert asynchrone (*asynchronous transfer mode*)
CP	point de connexion (*connection point*)
CPN	réseau du client (*customer premises network*)
e-t-e_VC-XX	cellule OAM assurant la fonction OAM "XX" pour une connexion VCC de bout en bout (exemple: e-t-e_VC-AIS ...)
e-t-e_VP-XX	cellule OAM assurant la fonction OAM "XX" pour une connexion VPC de bout en bout (exemple: e-t-e_VP-AIS ...)
e-t-e_XX	cellule OAM assurant la fonction OAM "XX" pour une connexion VPC ou VCC de bout en bout (exemple: e-t-e_VC-AIS ...)
MS	commutateur manuel (*manual switch*)
NIM	monitorage sans intrusion (*non-intrusive monitoring*)
OAM	exploitation et maintenance (*operations and maintenance*)
PS	commutation de protection (*protection switching*)
RGT	réseau de gestion des télécommunications
SD	dégradation du signal (*signal degrade*)
SDH	hiérarchie numérique synchrone (*synchronous digital hierarchy*)
seg_VC-XX	cellule OAM assurant la fonction OAM "XX" pour un segment VCC (exemple: seg_VC-AIS ...)
seg_VP-XX	cellule OAM assurant la fonction OAM "XX" pour un segment VPC (exemple: seg_VP-AIS ...)
seg_XX	cellule OAM assurant la fonction OAM "XX" pour un segment VPC ou VCC (exemple: seg_AIS ...)
SF	panne de signal (*signal fail*)
SN	sous-réseau (*subnetwork*)
SNC	connexion de sous-réseau (*subnetwork connection*)
TCP	point de connexion de terminaison (*termination connection point*)
TE	équipement terminal (*terminal equipment*)
VC	canal virtuel (*virtual channel*)
VCC	connexion par canal virtuel (*virtual channel connection*)
VCG	groupe de canaux virtuels (*virtual channel group*)
VCI	identificateur de canal virtuel (*virtual Channel identifier*)
VP	conduit virtuel (*virtual path*)

VPC connexion par conduit virtuel (*virtual path connection*)

VPG groupe de conduits virtuels (*virtual path group*)

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

5 Principes relatifs à la commutation de protection

Le concept de commutation de protection pour les conduits virtuels ou les canaux virtuels individuels s'applique essentiellement aux situations dans lesquelles il n'y a pas de commutation de protection de la couche Serveur. Il est utile de protéger seulement une partie des VP/VC qui doivent présenter une fiabilité élevée, les VP/VC restants demeurant sans protection. Cela permet de réduire la largeur de bande nécessaire pour la protection. Bien qu'elle puisse être utilisée pour la protection contre des défauts au niveau de la couche ATM et aussi pour les défauts au niveau de la couche Physique, la protection contre les défauts de la couche Physique uniquement n'est pas exclue.

A l'origine, le concept de protection VPG/VCG avait été développé au niveau de la couche ATM pour accélérer la commutation de protection de couche ATM (c'est-à-dire obtenir des temps de commutation voisins de ceux obtenus pour la couche SDH) essentiellement pour des situations où la commutation de protection de la couche Serveur n'existe pas ou ne peut être mise en œuvre. La rapidité de commutation tient au fait que l'on considère un faisceau logique de connexions de réseau ou de sous-réseau par VP/VC comme une seule entité VPG/VCG après le début des actions de protection. La protection VPG/VCG a été essentiellement conçue pour faire face aux anomalies affectant la couche Physique, mais elle peut aussi être utilisée contre les anomalies affectant la couche ATM. La protection VPG/VCG peut également être utilisée en association avec les techniques de commutation de protection individuelle des VP/VC, qui peuvent être utilisés pour la protection des connexions VP/VC individuelles contre les anomalies affectant la couche ATM.

La commutation de protection est un mécanisme de protection entièrement déterministe utilisable sur toute topologie physique. Il est entièrement déterministe dans le sens où le trajet et la largeur de bande de l'entité de protection est réservée pour une entité active sélectionnée.

L'architecture de commutation de protection ATM peut être du type 1+1 ou du type *m:n*.

Dans une architecture de type 1+1, une entité de protection est affectée à chaque entité active, cette dernière étant pontée sur l'entité de protection à la source du domaine protégé. Le trafic sur les entités actives et les entités de protection est transmis simultanément vers le puits du domaine protégé où une sélection entre l'entité active et l'entité de protection est opérée sur la base de critères prédéterminés comme par exemple une indication d'une anomalie au niveau du serveur.

Dans une architecture de type *m:n*, *m* entités de protection spécialisées sont partagées par *n* entités actives, *m* étant en général inférieur ou égal à *n*. La largeur de bande de chaque entité de protection doit être attribuée de manière à pouvoir protéger l'une quelconque des *n* entités actives dans le cas où au moins une des *m* entités de protection est disponible. Lorsqu'on constate un dérangement au niveau d'une entité active, une entité de protection disponible lui est attribuée, suivie d'une transition de l'entité active à l'entité de protection à la fois à la source et au puits du domaine protégé. Il convient de noter que s'il y a plus de *m* entités actives en dérangement, seules *m* entités actives peuvent être protégées.

5.1 Principes généraux, spécifications et objectifs

Les principes, spécifications et objectifs suivants sont communs à la commutation de protection de VC, VP, VCG et VPG.

5.1.1 Principes généraux

Le présent sous-paragraphe contient une liste des principes généraux applicables aux architectures et mécanismes de protection ATM.

1) les techniques de protection ATM doivent pouvoir s'appliquer aux VPG, VP, VCG et VC;
2) les violations de la structure en couches du réseau doivent être évitées (par exemple, une anomalie au niveau VP ATM ne doit pas déclencher les alarmes de couche SDH);
3) en général, si les mécanismes de protection de couche inférieure (par exemple, SDH ou optique) sont utilisés en association avec les mécanismes de protection ATM, il faut offrir aux couches inférieures la possibilité de rétablir le trafic avant que la couche ATM déclenche les actions de protection. L'objectif ici est d'éviter des actions de protection intempestives et tout conflit;
4) les actions de commutation de protection dans un domaine protégé ne doivent pas affecter le fonctionnement et les performances du réseau dans les autres domaines;
5) le mécanisme de commutation de protection doit favoriser le rétablissement rapide du trafic actif afin de minimiser l'indisponibilité du réseau.

5.1.2 Spécifications générales et objectifs

1) protection des VP/VC et des connexions de sous-réseau (SNC);
2) protection des domaines protégés SNC qui sont indépendants ou alignés avec les flux F4 ou F5 des segments OAM (voir Recommandation I.610 [5]);
3) topologies physiques linéaires, maillées ou en anneau;
4) la détection d'une panne de signal (SF, *signal fail*) ou d'une dégradation de signal (SD, *signal degrade*) doit servir à déclencher la commutation de protection. Le déclenchement dans le cas d'une dégradation de signal appelle un complément d'étude;
5) le délai de détection d'une panne de signal doit être aussi court que possible;
6) attribution de priorités de protection aux pannes de signal, aux dégradations de signal et aux requêtes de commutation provenant de l'opérateur;
7) délai d'exécution de la commutation de protection: il faut pouvoir exécuter la commutation de protection au niveau de la couche interne dans les plus brefs délais. Par exemple, la rapidité revêt une très grande importance lorsque la couche Physique ne dispose pas de moyens de protection contre les pannes (ce qui est le cas par exemple dans une structure en anneau collectant le trafic des nœuds internes). La ou les valeurs exactes de ce délai appellent un complément d'étude;
8) coefficient de protection égal à 100%, c'est-à-dire que 100% du trafic actif dégradé est protégé contre une panne affectant une entité active;
9) il doit être possible de prendre en charge les modes de commutation de protection unidirectionnels 1+1 et bidirectionnels 1+1, 1:1 (le mode généralisé *n:m* appelle un complément d'étude concernant la technique d'attribution des ressources de protection);
10) capacité de traitement du trafic excédentaire si possible;
11) protocole de commande de la commutation de protection fondé dans la mesure du possible sur les principes et les caractéristiques APS SDH;
12) la stratégie d'échelonnement intercouche et intracouche doit pouvoir être prise en charge;
13) utilisation des outils OAM définis dans la Recommandation I.610 et éviter si possible l'introduction de nouveaux outils OAM;
14) pas d'interférence intempestive avec la protection de la couche Physique;

15) la combinaison de la commutation de protection individuelle VP/VC et VPG/VCG doit être possible;

16) l'opérateur de réseau doit pouvoir proposer en option une commutation de protection réversible et non réversible;

17) certaines commandes d'opérateur tel le blocage des commandes de commutation de protection forcée et manuelle doivent pouvoir être prises en charge;

18) une fonction générique de retardement doit être disponible de manière à différer le début de l'action de protection. Ce retardement doit être réglable par l'opérateur de réseau afin de déclencher l'action de protection dans les plus brefs délais possibles ou de la retarder de quelques secondes;

19) la connectivité de couche ATM de l'entité de protection doit être périodiquement vérifiée afin de s'assurer de la disponibilité lorsqu'il est nécessaire d'opérer une commutation de protection. La fréquence d'insertion des cellules APS est d'une cellule toutes les 5 secondes. Les fréquences d'insertion réglables feront l'objet d'un complément d'étude ainsi que la question de savoir s'il est necessaire de procéder á une vérification plus poussée (par exemple, largeur de bande, performance, etc.) de l'entité de protection.

    NOTE – La fréquence d'insertion a été déterminée suite à un compromis entre la largeur de bande requise pour les cellules APS et le retard additionnel qui se produit en cas de perte d'une cellule APS;

20) une protection imbriquée doit si possible être offerte;

21) dans la première version de la Recommandation I.630, la commutation de protection transparente n'est pas imposée.

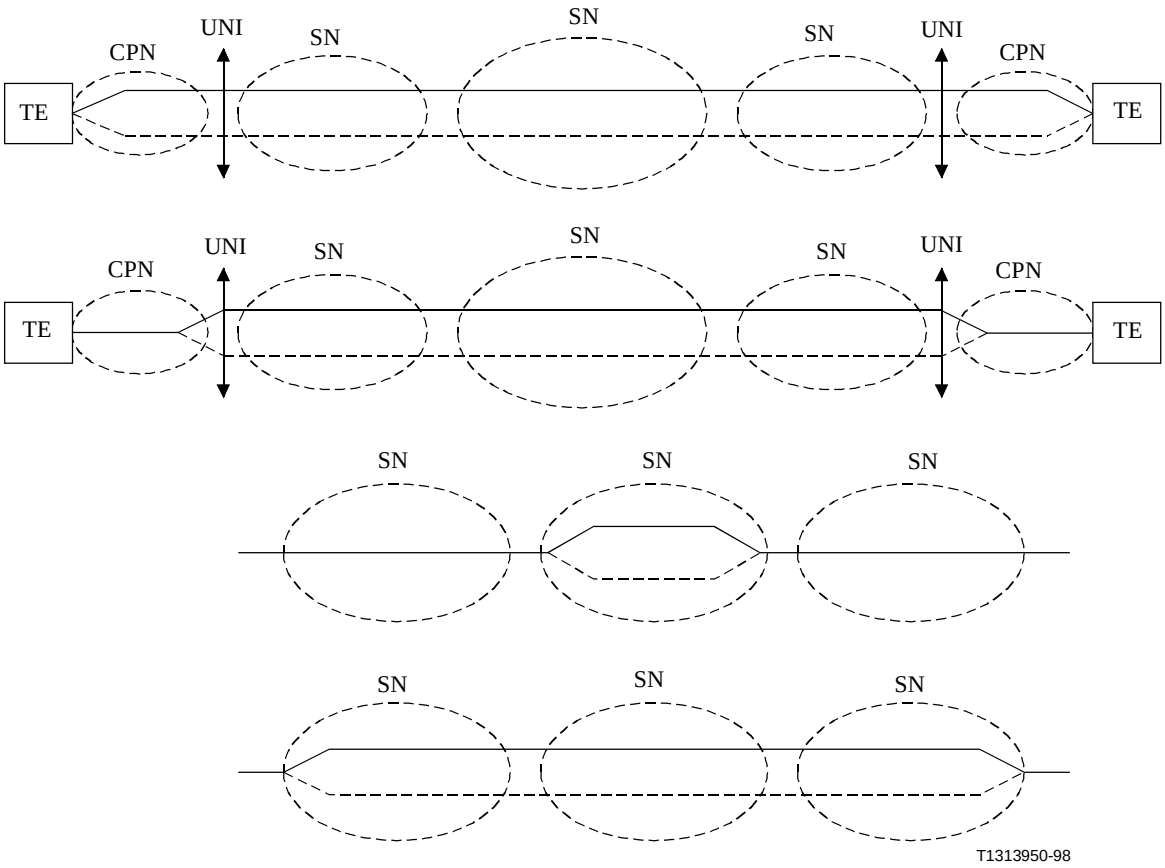
5.2 Exemples de domaines protégés de réseau

La Figure 2 contient plusieurs exemples de domaines protégés. Le domaine protégé peut s'étendre:

- sur une connexion de réseau;
- sur une connexion de sous-réseau;
- sur une connexion à liaison unique.

Le domaine protégé pour des connexions VPC/VCC peut coïncider avec les flux de segment ou de bout en bout OAM. La Recommandation I.732 [6] définit deux types de fonctionnalité de terminaison de segment. Dans le premier, la source se trouve devant la matrice et le puits associé derrière. Dans le second, la source se trouve derrière la matrice et le puits associé devant. Si les points d'extrémité du domaine protégé coïncident avec les points de terminaison du segment du second type, les mécanismes de commutation de protection ATM appliqués au domaine protégé peuvent utiliser les outils AOM pour les segments VPC/VCC.

Lorsque le domaine protégé ne coïncide pas avec l'étendue des flux de bout en bout ou de segment OAM, il peut être nécessaire d'utiliser les capacités telle la vérification sans intrusion des outils existants OAM pour les mécanismes de commutation de protection ATM appliqués au domaine protégé.



UNI interface utilisateur-réseau

Figure 2/I.630 – Exemples de domaines protégés

5.3 Etendue du domaine protégé

Dans ce qui suit, on utilise les termes suivant:

- protection de chemin 1+1/1:1 [connexion de bout en bout] – Dans ce mode, on utilise l'OAM de connexion de bout en bout pour superviser le chemin [la connexion de bout en bout] dans le domaine protégé;
- protection 1+1/1:1 de connexion de sous-réseau par monitorage de sous-couche (SNC/S) – Dans ce mode, il faut ajouter un domaine de protection supplémentaire ou une OAM de segment de contrôle de connexion supplémentaire pour superviser la connexion de sous-réseau à l'intérieur du domaine protégé;
- protection 1+1 sans intrusion par monitorage de connexion de sous-réseau (SNC/N) – Dans ce mode, il n'est pas exigé d'utiliser une OAM supplémentaire pour superviser la connexion de sous-réseau dans le domaine protégé; il est en tant que tel restreint au type de protection unidirectionnelle 1+1. Ce mode est applicable à la protection de VP/VC individuels et n'est pas applicable à la protection de groupes;
- protection 1+1/1:1 de connexion de sous-réseau par monitorage d'un chemin test (SNC/T) – Ce mode ne s'applique qu'à la protection de groupes; un chemin test supplémentaire (connexion de bout en bout) est établi entre la source et le puits du domaine protégé. L'état de ce chemin test est utilisé comme indication de panne ou de dégradation de signal du groupe.

NOTE 1 – Le chemin test pour la protection de groupe est appelé VPC/VCC APS dans le paragraphe 7.

NOTE 2 – Dans le cas général, les connexions de réseau et les connexions de sous-réseau acheminant du trafic d'utilisateur peuvent être assignées au même groupe.

- protection 1+1/1:1 par chemin test ou par chemin observé (chemin/T) – Ce mode ne s'applique qu'à la protection de groupes; un chemin test supplémentaire (connexion de bout en bout) est établi entre la source et le puits du domaine protégé. L'état de ce chemin test est utilisé comme indication de panne ou de dégradation de signal du groupe.

5.3.1 Protection de chemin

La Figure 3 illustre un exemple de protection de chemin 1+1 ou 1:1 individuelle VP/VC.

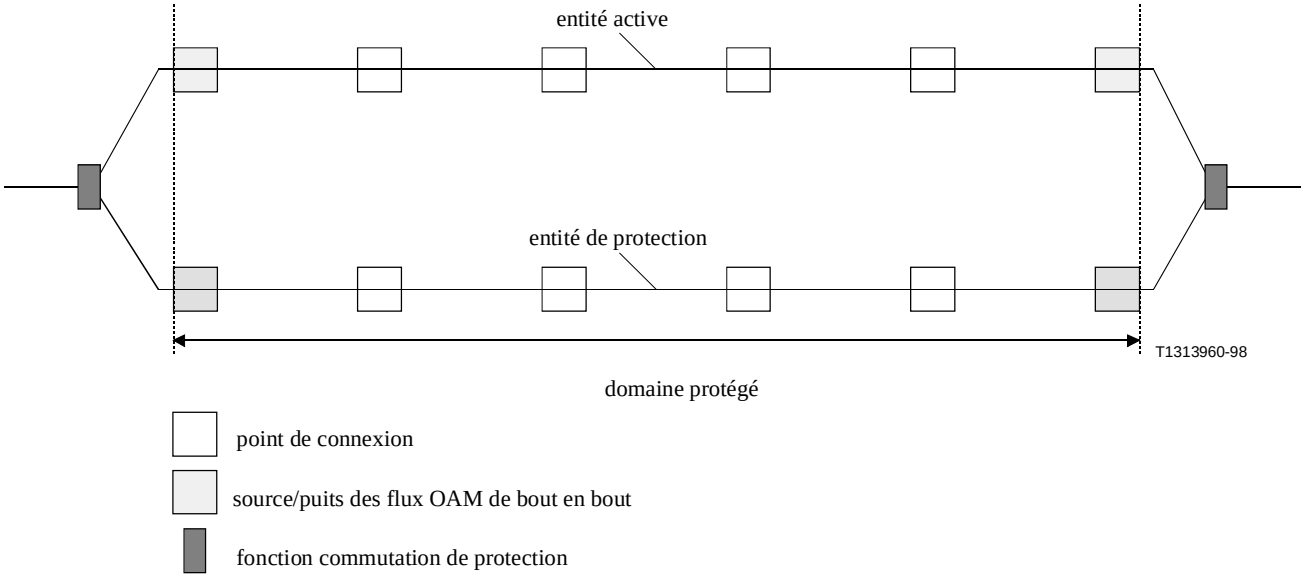


Figure 3/I.630 – Protection 1:1 ou 1+1 de chemins à VP/VC individuels

La Figure 4 illustre un exemple de protection 1+1 ou 1:1 de chemin/groupe T.

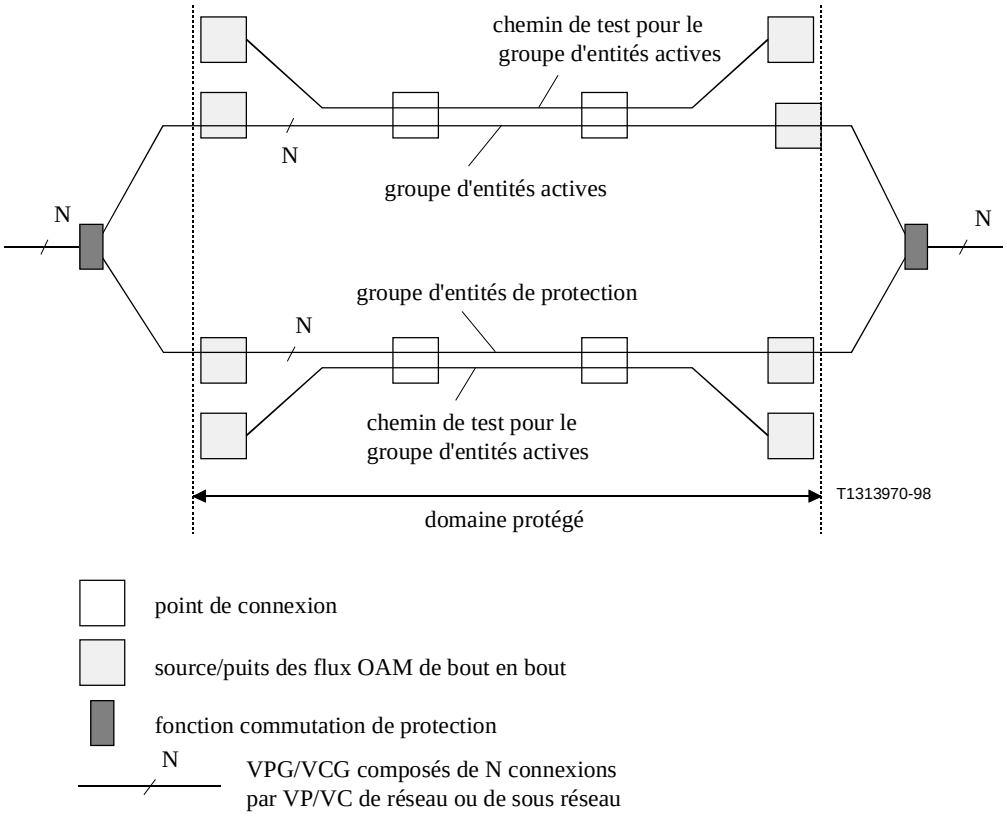


Figure 4/I.630 – Protection 1+1 ou 1:1 de chemin/groupe T

5.3.2 Protection de connexion de sous-réseau

La Figure 5 illustre un exemple de protection 1+1 ou 1:1 de type SNC/S de VP/VC individuels.

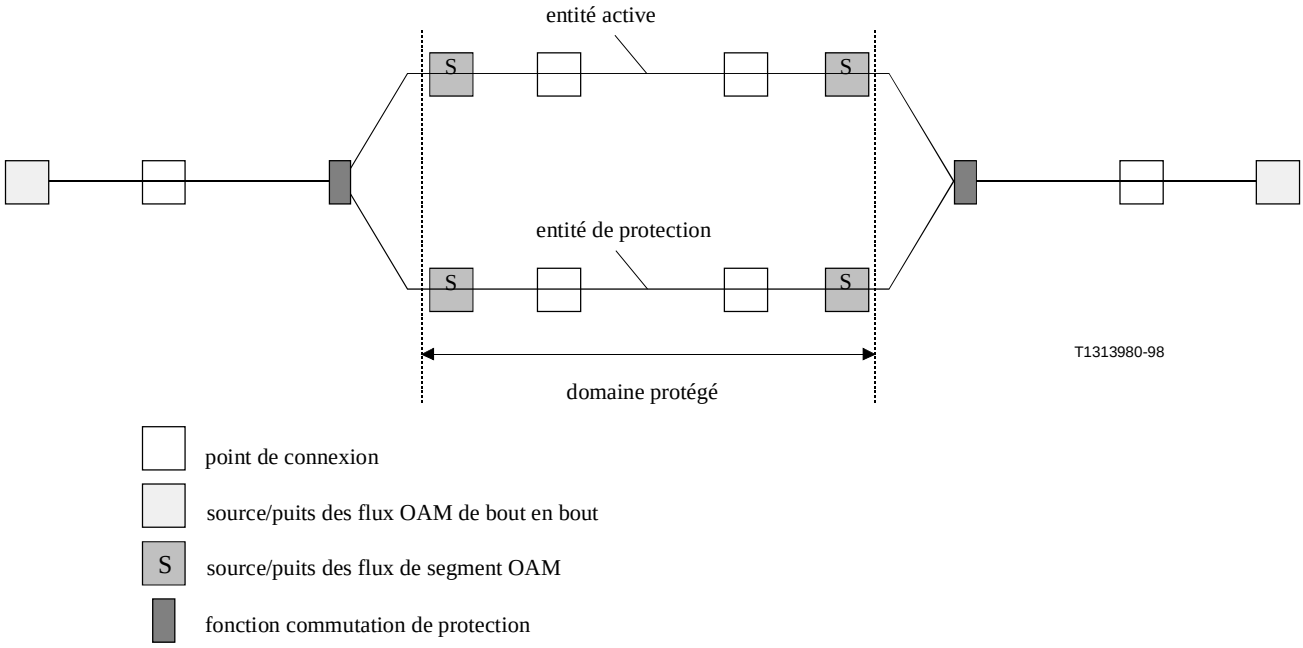


Figure 5/I.630 – Protection 1+1 ou 1:1 de type SNC/S de VP/VC individuels

La Figure 6 illustre un exemple de protection 1:1 ou 1+1 de SNC/groupe T.

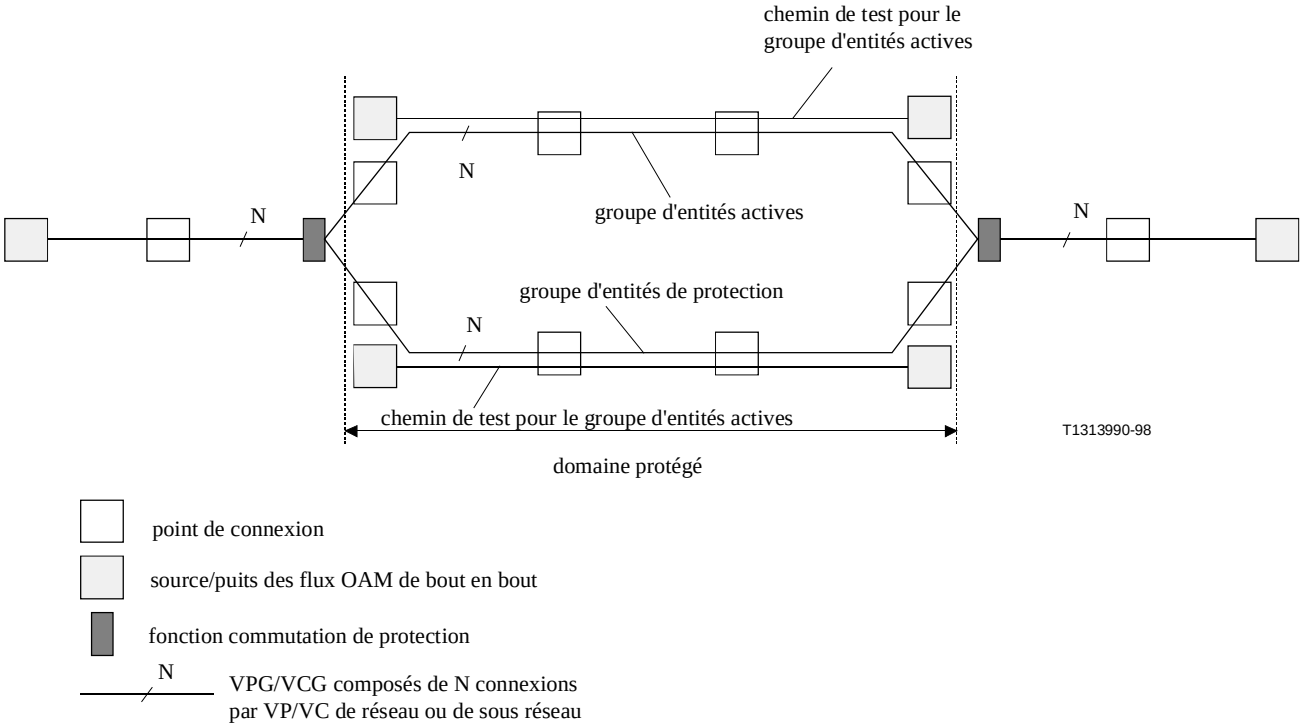


Figure 6/I.630 – Protection 1:1 ou 1+1 SNC/groupe T

5.3.3 Protection 1+1 de connexion de sous-réseau supervisée sans intrusion (SNC/N)

La Figure 7 illustre un exemple de protection 1+1 de connexion de sous-réseau par VP/VC individuels non supervisée (SNC/N).

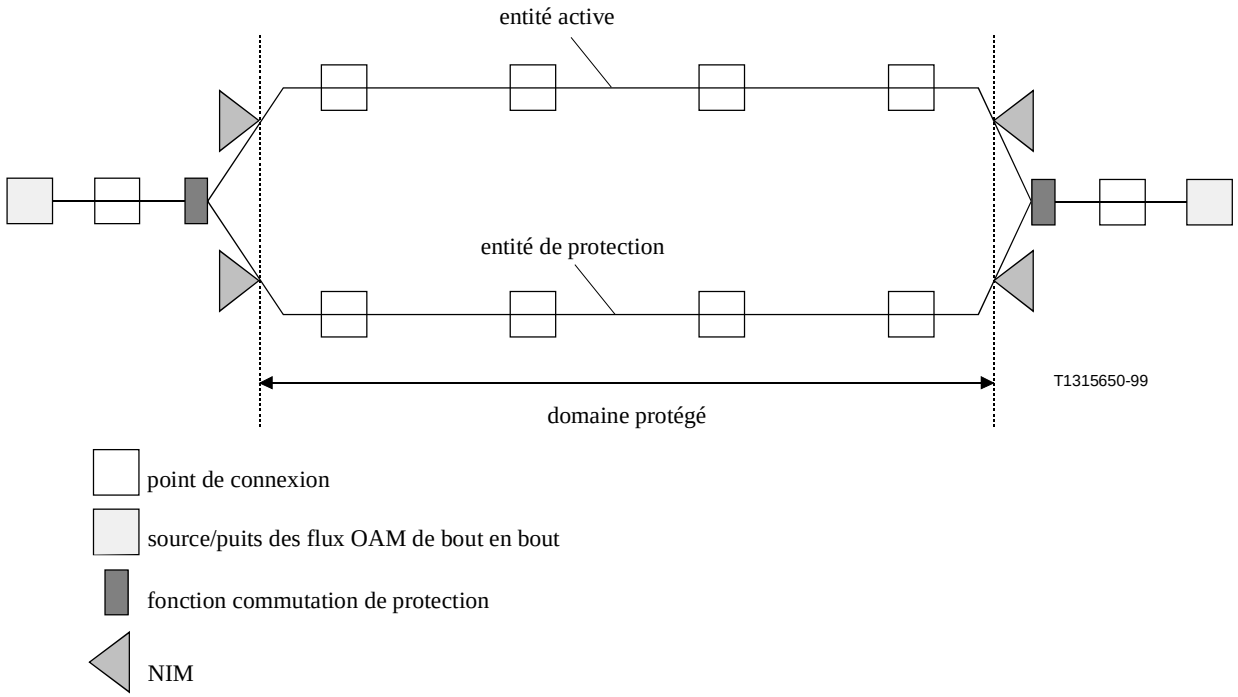


Figure 7/I.630 – Protection SNC/N 1+1 par supervision sans intrusion de connexion de sous-réseau par VP/VC individuels

5.3.4 Relations entre le domaine protégé et l'étendue des flux OAM

La configuration dans laquelle un domaine protégé et un segment OAM se chevauchent ne peut être prise en charge. La configuration dans laquelle deux domaines protégés se chevauchent ne peut pas être prise en charge pour la commutation de protection bidirectionnelle. Il convient de noter que les domaines protégés qui se chevauchent peuvent être pris en charge pour la commutation de protection unidirectionnelle 1+1.

5.4 Fiabilité de la configuration de réseau de couche Physique

Normalement, les entités de protection et les entités actives doivent être acheminées sur des entités de transport physiquement diverses.

5.5 Configurations de commutation de protection

5.5.1 Configuration (1:1)

Une entité de protection est spécialement assignée à chaque entité active. L'entité de protection n'achemine le trafic que si l'entité active est en dérangement ou s'il y a eu commutation forcée/commutation manuelle concernant l'entité active. Dans les autres cas elle n'achemine pas le trafic, mais elle est susceptible d'acheminer du trafic supplémentaire.

5.5.2 Configuration (1+1)

Une entité de protection est attribuée à chaque entité active. L'entité active et son entité de protection acheminent le trafic simultanément.

5.5.3 Configuration (1:n)

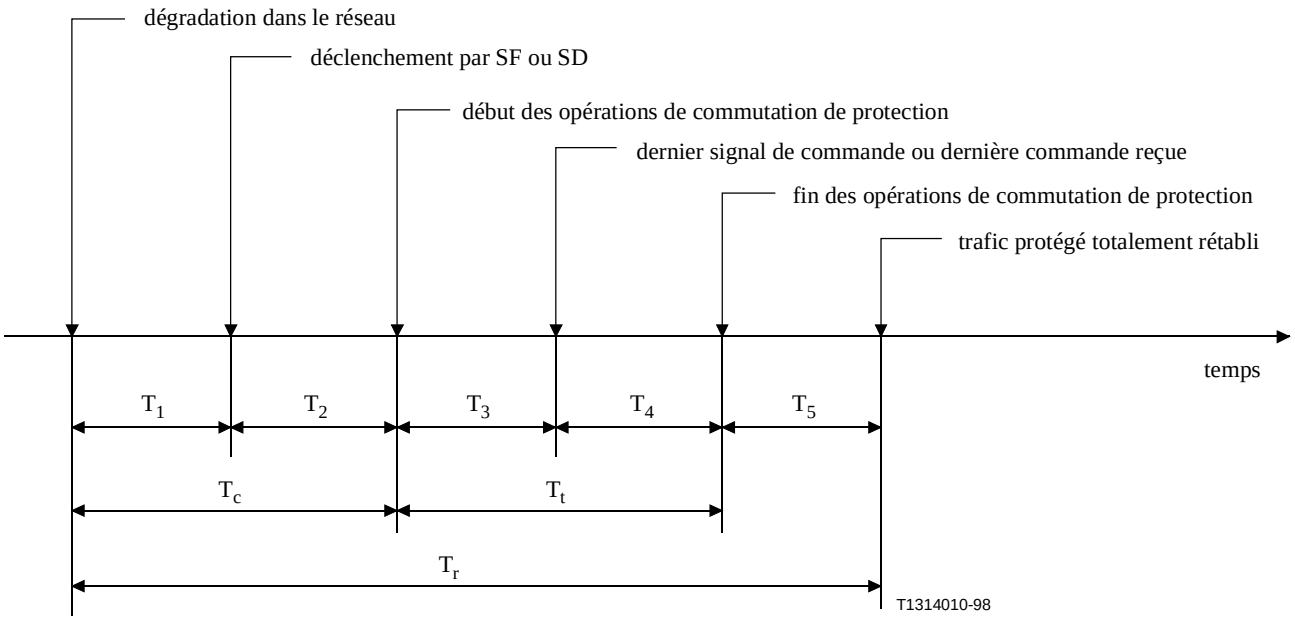
Appelle un complément d'étude.

5.5.4 Configuration (m:n)

Appelle un complément d'étude.

5.6 Qualité de fonctionnement de la commutation de protection

Le modèle temporel de commutation de protection a été établi à partir de la Recommandation M.495 [7] et son chronogramme est représenté à la Figure 8.



T_1: **délai de détection**

T_2: **temps d'attente** [ce temps correspond au temps de rétention (voir 5.7)]

T_3: **délai d'activation de la commutation de protection**

T_4: **temps de transfert de la commutation de protection**

T_5: **délai de rétablissement**

T_c: **délai de confirmation**

T_t: **temps de transfert**

T_r: **temps de rétablissement du trafic protégé**

Figure 8/I.630 – Modèle temporel de commutation de protection

5.7 Blocage par palier des réactions de "survie"

Pour permettre aux fonctions de commutation de protection de couche basse de protéger le trafic actif avant que la commutation de protection de couche ATM ne se produise, ou pour confirmer la persistance du dérangement contre laquelle il faut assurer la protection, ou bien pour retarder la commutation de protection pour d'autres raisons opérationnelles, il faut prévoir un retardement.

Etant donné que les cellules VP/VC-AIS sont transmises pratiquement dès la détection d'un dérangement, la durée du retardement est fixée au niveau du puits du domaine protégé. La commutation de protection commence *x* secondes après qu'un état de bout en bout ou seg_AIS a été observé au puits du domaine protégé.

La valeur de *x* peut être choisie entre 0 et 10 secondes par pas de 500 ms.

5.8 Protocole de commande de la commutation de protection

La commutation de protection bidirectionnelle est réalisée par échange d'informations de coordination entre la source et le puits du domaine protégé. L'information de coordination est transmise sur une cellule VP/VC-APS spéciale. Le format de cette cellule est donné à la Figure 9. Les points de code associés sont donnés dans le Tableau 1. Le mécanisme de coordination de la commutation de protection pour des configurations (1:1) et (1+1) est décrit de manière détaillée dans l'Annexe A.

La commutation de protection (1+1) unidirectionnelle est réalisée sans protocole de coordination. Les détails sont donnés dans l'Annexe B.

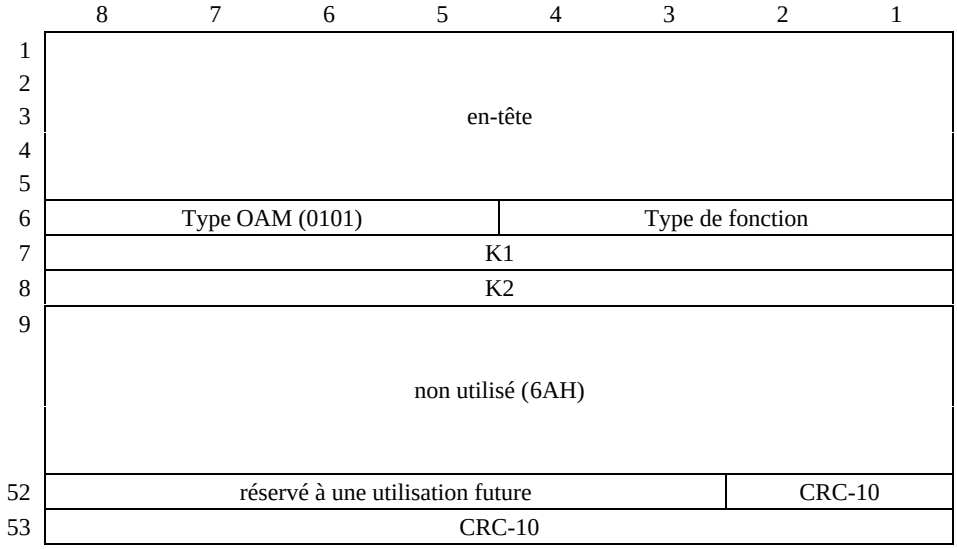


Figure 9/I.630 – Format de la cellule APS

Tableau 1/I.630 – Points de code de la cellule APS

Type OAM	Codage	Type de fonction	Codage
Protocole de coordination	0101	Protection de groupe	0000
		Protection individuelle	0001

6 Commutation de protection de VP /VC ATM

6.1 Spécifications générales et objectifs

Les spécifications générales et les objectifs exposés au 5.1.2 sont applicables à la commutation de protection de VP/VC ATM.

6.2 Mécanisme de déclenchement de la commutation de protection

La commutation de protection doit se produire lorsque:

1) elle est déclenchée par une commande d'opérateur (par exemple, commutation manuelle, commutation forcée et blocage de la protection);

2) une panne de signal est détectée;

3) une dégradation du signal est détectée;

4) la temporisation "attente avant rétablissement" expire.

6.2.1 Commande d'opérateur

La commande par opérateur de la fonction de commutation de protection peut être transférée via les interfaces du RGT (interfaces F ou Q3 [8] et [9]).

6.2.2 Déclenchement par une panne de signal

Pour la commutation de protection de VP/VC individuelle (unidirectionnelle ou bidirectionnelle) lorsque le domaine protégé est associé à un segment OAM, la commutation de protection est déclenchée lorsque la durée de seg_AIS est supérieure au temps de blocage programmé au puits du domaine protégé pour les entités actives et les entités de protection.

Pour la commutation de protection de VP/VC individuelle (unidirectionelle ou bidirectionelle) lorsque le domaine protégé est associé à une connexion de bout en bout, la commutation de protection est déclenchée lorsque la durée de l'état e-t-e_AIS est supérieure au temps de blocage programmé au puits du domaine protégé pour les entités actives et les entités de protection.

Pour une commutation de protection 1+1 unidirectionnelle de VP/VC individuelle dans le cas d'une protection de connexion de sous-réseau supervisée sans intrusion, la commutation de protection est déclenchée lorsque la durée de l'état e-t-e_AIS (déterminée localement au moyen du monitorage sans intrusion) est supérieure au temps de blocage au puits du domaine protégé pour les entités de active et de protection.

Les formats des cellules e-t-e_/seg_VP-AIS et de la cellule e-t-e_/seg_VC-AIS ainsi que la déclaration et les conditions de dépassement de l'état AIS sont spécifiés dans la Recommandation I.610 [5].

6.2.3 Déclenchement par dégradation du signal

La dégradation de la qualité de fonctionnement des entités actives et de protection peut être détectée au moyen des flux OAM de qualité de fonctionnement de bout en bout (e-t-e) ou de segment. Le fonctionnement détaillé appelle un complément d'étude.

7 Commutation de protection de groupe VP/VC ATM

7.1 Spécifications particulières et objectifs

Les spécifications générales et les objectifs indiqués au 5.1.2 sont applicables à la commutation de protection de VPG/VCG ATM.

7.2 Architecture

7.2.1 Introduction

L'entité logique pour le groupement de protection au niveau de la couche ATM est le groupe de conduit virtuel (VPG, *virtual path group*) et le groupe de canal virtuel (VCG, *virtual channel group*).

Un groupe VPG/VCG (VPG/VCG actif [VPG_W/VCG_W] ou un VPG/VCG de protection [VPG_P/VCG_P]) est un faisceau logique d'une ou de plusieurs connexions de réseaux et de sous-réseaux VP/VC ATM partageant le ou les mêmes trajets de transmission à l'intérieur du domaine protégé. Le groupe VPG/VCG est configuré par l'opérateur à la source et également au puits du domaine protégé. En cas de commutation de protection, tous les VP/VC appartenant au groupe

VPG/VCG sauf le VPC/VCC de commutation de protection sont commutés simultanément. Voir la Figure 10 qui présente un exemple concernant des groupes VPG.

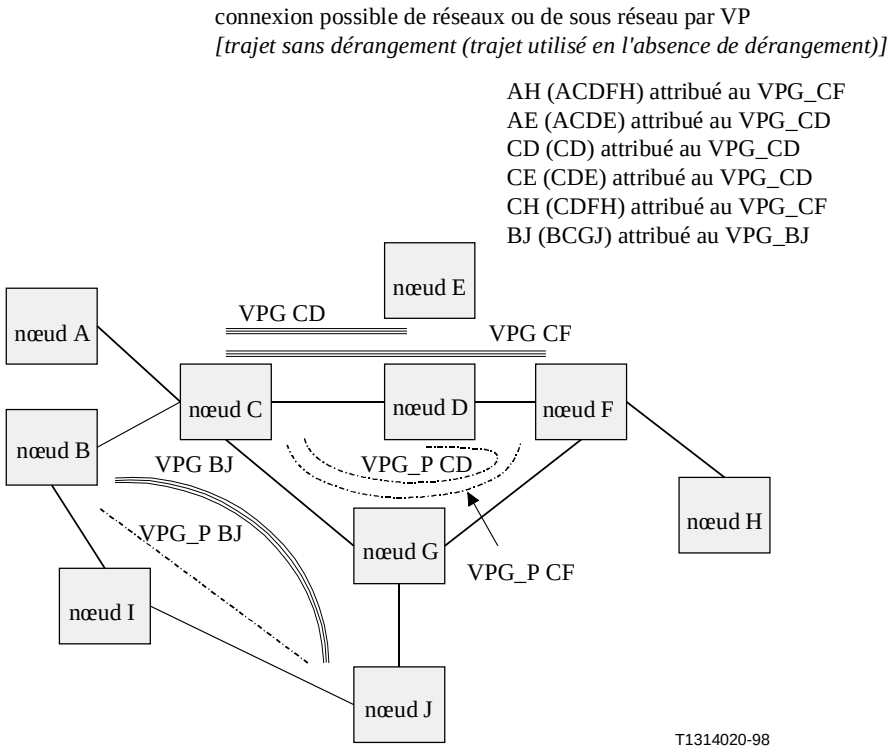


Figure 10/I.630 – Exemple de groupe VPG

7.2.2 Généralités

Le mode de commutation de protection de VPG/VCG défini ci-dessous, présente les caractéristiques architecturales suivantes:

- il utilise un algorithme de commande décentralisée;
- il utilise pour l'entité de protection un trajet et des ressources en largeur de bande spécialement affectés;
- la source et le puits du domaine protégé peuvent être couplés ou découplés des points d'extrémité de la connexion/du segment OAM;
- il n'est défini actuellement que pour les configurations linéaires et ne dépend pas de la topologie de la couche Serveur (c'est-à-dire de la couche Physique);
- le déclenchement de l'action de protection peut être retardé d'une durée réglable (temps de blocage), afin que la protection au niveau de la ou des couches serveur soit exécutée en premier.

7.2.3 Architecture de protection 1+1 de VPG/VCG

La Figure 11 illustre l'architecture d'une configuration 1+1 de VPG/VCG (un seul sens de la transmission est représenté).

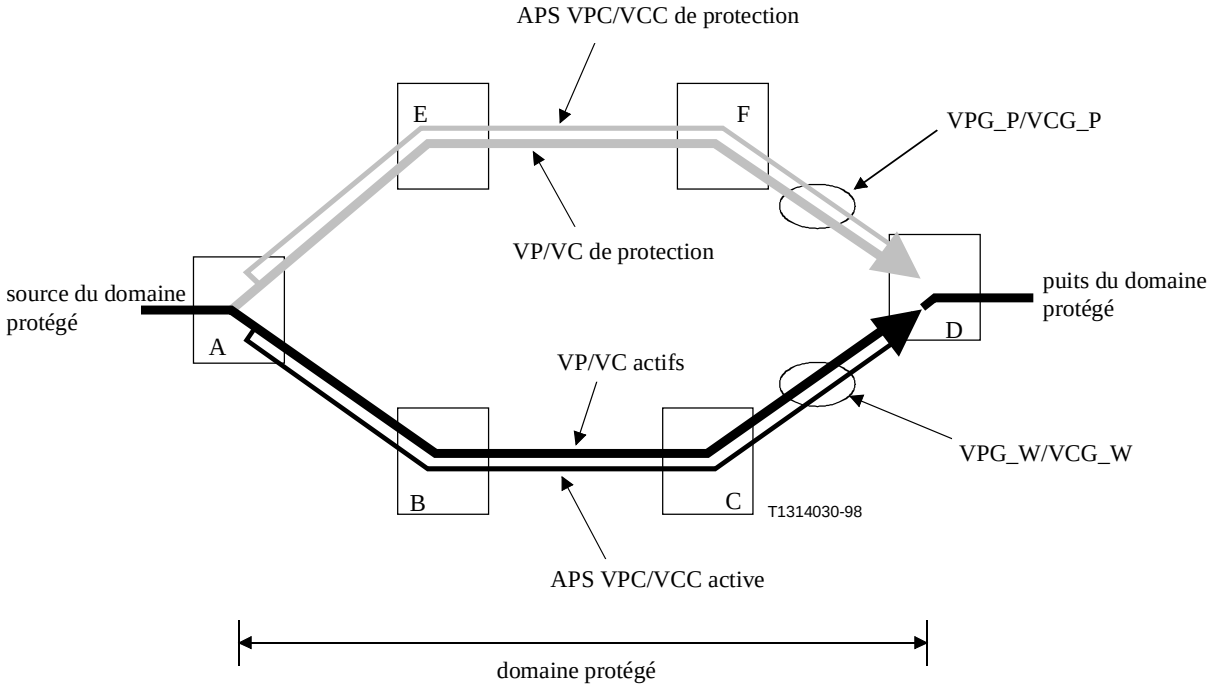


Figure 11/I.630 – Configuration 1+1 de VPG/VCG

Il convient de noter qu'à la source du domaine protégé, le trafic actif est ponté en permanence sur l'entité de protection.

7.2.4 Architecture de protection 1:1 de VPG/VCG

La Figure 12 illustre une architecture 1:1 VPG/VCG (un seul sens de la transmission est représenté).

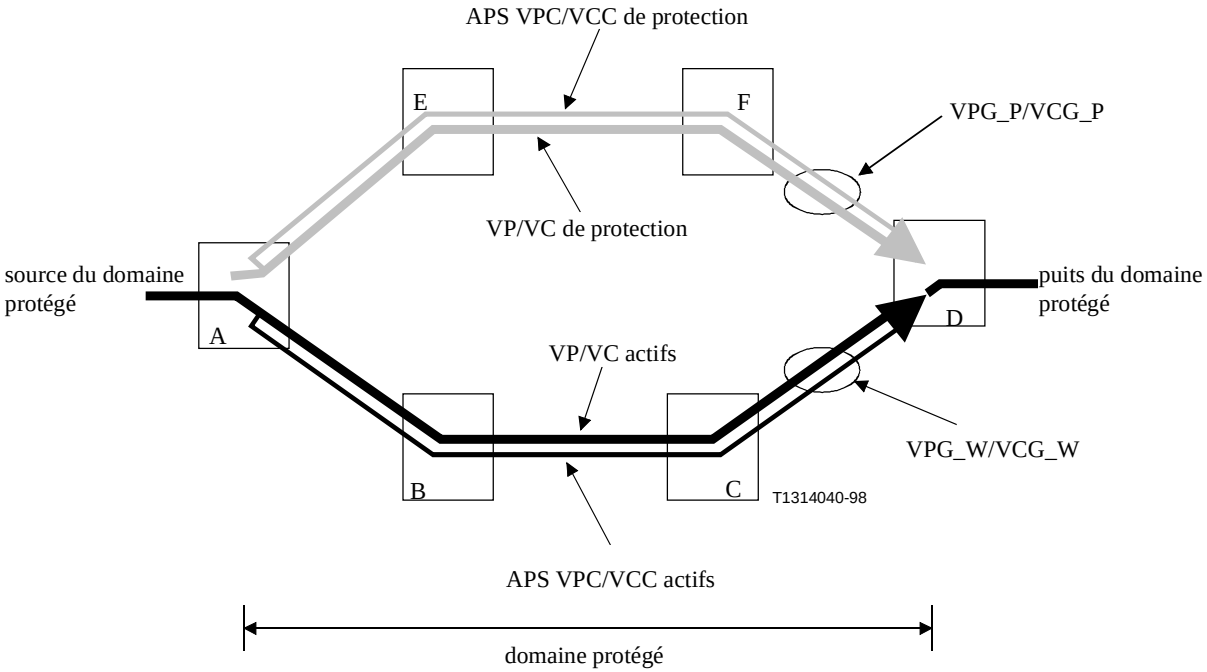


Figure 12/I.630 – Configuration 1:1 de VPG/VCG

Il convient de noter que ce pont est considéré du point de vue fonctionnel comme un simple commutateur (transmettant le trafic alternativement vers les entités actives ou vers les entités de protection), et non pas comme un pont de diffusion comme dans la Figure 11, dans laquelle le trafic est ponté à la fois sur les entités actives et sur les entités de protection.

7.2.5 Architecture de protection 1:N (N>1) de VPG/VCG

Appelle un complément d'étude.

7.2.6 Architecture de protection M:N de VPG/VCG

Appelle un complément d'étude.

7.3 Mécanisme de déclenchement de la commutation de protection

La commutation de protection doit se produire lorsque:

1) elle est déclenché par une commande de l'opérateur (commutation manuelle, commutation forcée, désactivation);
2) une panne de signal est détectée;
3) une dégradation de signal est détectée;
4) la temporisation "attente avant rétablissement" expire.

7.3.1 Commande d'opérateur

La commande d'opérateur de la fonction de commutation de protection peut être transférée via les interfaces du RGT (interfaces F ou Q3 [8] et [9]).

7.3.2 Déclenchement après panne de signal

Pour la protection d'un groupe (unidirectionnel ou bidirectionnel) qui utilise la commutation de protection automatique de VPC/VCC, la commutation de protection est déclenchée lorsque la durée de l'état AIS de bout en bout dépasse le temps de blocage programmé au puits du domaine protégé pour les VPC/VCC APS associés.

7.3.3 Déclenchement après dégradation du signal

Appelle un complément d'étude.

ANNEXE A

Protocole de coordination de la commutation de protection pour les configurations 1+1/1:1

A.1 Introduction

Le protocole de coordination de la commutation de protection décrit dans la présente annexe peut être appliqué aux configurations linéaires 1+1 et 1:1.

A.1.1 Architecture d'application

Le protocole de commutation de protection ATM linéaire 1+1/1:1 décrit dans les sous-paragraphes qui suivent peut être appliqué aux architectures de protection ATM linéaire (point à point) de la classe de commutation de protection (PS, *protection switching*), avec des ressources de protection affectées (trajet et largeur de bande attribués à l'avance) et commande décentralisée (l'algorithme de protection opère dans des éléments de réseau ATM situés aux deux extrémités du domaine de protection).

Le domaine protégé peut être une connexion par VP (ou par VC) de bout en bout, ou un segment de connexion par VP (ou par VC) pour la protection individuelle. Le cas où le domaine protégé n'est pas associé à une connexion de bout en bout ou à un segment OAM appelle un complément d'étude.

Outre la protection individuelle, le présent protocole s'applique aussi à la protection de groupe. L'information de coordination APS est acheminée à travers une connexion spécialisée (canal APS) pour la protection de groupe. Le domaine protégé peut être aligné avec ou indépendant d'une connexion de bout en bout ou d'un segment OAM.

Le protocole s'applique aux architectures 1+1. Il s'applique également aux architectures 1:1 avec ou sans trafic supplémentaire. Le trafic supplémentaire est un trafic de priorité faible qui peut être transmis via l'entité de protection lorsque celle-ci n'est pas utilisée pour transmettre le trafic actif.

Un système de protection 1:1 est intrinsèquement plus long en commutation qu'un système 1+1, car il nécessite une communication entre les deux extrémités du domaine protégé pour exécuter même les opérations de commutation unidirectionnelle, mais il présente l'avantage d'accepter facultativement du trafic supplémentaire. De même, dans les configurations 1:1 sans trafic supplémentaire, la largeur de bande de l'entité de protection est attribuée à l'avance mais en réalité elle n'est pas utilisée lorsqu'il n'y a pas d'anomalie.

A.1.1.1 Architecture 1+1

La Figure A.1 illustre l'architecture de commutation de protection linéaire 1+1. Le trafic est ponté en permanence simultanément sur l'entité active (#1) et sur l'entité de protection (#0). Dans cette Figure, le trafic est représenté comme étant reçu via le sélecteur depuis l'entité active (#1). Il convient de noter que la fonction de sélecteur utilise la fonctionnalité d'acheminement VPI/VCI et peut être mise en œuvre de deux manières différentes:

– par modification des tables d'acheminement VPI/VCI qui est faite dans le cas d'un commutateur de protection; ou tout simplement

– par blocage du trafic depuis l'entité active ou depuis l'entité de protection, avec des tableaux d'acheminement VPI/VCI configurés pour une fonction "OU" logique pour tout le trafic depuis l'entité active et depuis l'entité de protection.

La Figure A.2 illustre une situation dans laquelle une commutation de protection (bidirectionnelle) s'est produite, due à une panne de signal sur l'entité active (#1).

A.1.1.2 Architecture 1:1

La Figure A.3 illustre l'architecture de commutation de protection linéaire 1:1, dans laquelle le trafic actif est transmis via l'entité active (#1). La transmission de trafic supplémentaire sur l'entité de protection est facultative. La fonction sélecteur pour le trafic actif est la même que dans le cas de l'architecture 1+1. Le sélecteur pour le trafic supplémentaire utilise également la fonctionnalité d'acheminement VPI/VCI de sorte que le trafic est acheminé selon la valeur VPI/VCI donnée à la sortie du trafic supplémentaire.

La Figure A.4 illustre une situation dans laquelle une commutation de protection (bidirectionnelle) s'est produite, due à une panne de signal sur l'entité active (#1). Du côté émission, le trafic actif est ponté vers l'entité de protection et le trafic supplémentaire est éliminé. Il convient de noter que ce pont est considéré fonctionnellement comme un simple commutateur (transmettant le trafic vers les entités actives ou les entités de protection), et non pas comme un pont de diffusion comme c'était le cas dans la Figure A.1, dans laquelle le trafic est ponté à la fois vers l'entité active et l'entité de protection. Du côté réception, le sélecteur est activé de sorte que le trafic est reçu depuis l'entité de protection. Dans le même temps, la réception du trafic supplémentaire est bloquée et un signal AIS est inséré en aval de la sortie du trafic supplémentaire. Durant l'opération de commutation de protection, il peut y avoir défaut de correspondance transitoire entre les positions pont/sélecteur aux sites OUEST et EST. Toutefois, toute erreur d'aiguillage entre le trafic actif et le trafic supplémentaire est impossible car la fonction sélecteur achemine toujours correctement le trafic, sur la base de la valeur VPI/VCI, soit vers la sortie trafic actif, soit vers la sortie trafic supplémentaire. Il convient de noter que pour cet acheminement par VPI/VCI, différentes valeurs VPI/VCI doivent être configurées sur l'entité de protection pour le trafic actif et le trafic supplémentaire. Ce qui peut être réalisé automatiquement en configurant un trajet individuel VPI/VCI pour le trafic actif via l'entité de protection; le trafic n'est alors ponté sur ce trajet qu'en cas de commutation de protection. A noter que dans le cas d'une protection VP/VC individuelle, si des valeurs VPI/VCI différentes sont configurées sur l'entité de protection pour le trafic actif et le trafic supplémentaire, la surveillance de la panne SF et de la dégradation SD et la communication du protocole de protection ne s'applique qu'à la valeur VPI/VCI configurée pour le trafic actif.

L'acheminement du trafic en fonction de la valeur VPI/VCI incluse dans la fonction sélecteur, implique que, pour des architectures 1:1, une incompatibilité d'aiguillage du trafic est impossible. Cela simplifie fortement la fonctionnalité du protocole de commutation de protection et permet d'utiliser un protocole à une phase, un seul échange d'informations étant nécessaire entre les deux extrémités pour exécuter une commutation bidirectionnelle. En revanche, pour la protection d'une section multiplex des réseaux SDH, l'acheminement par VPI/VCI n'est pas possible. Ainsi, un protocole de protection à deux ou trois phases est nécessaire dans le cas d'architectures 1:n, afin d'éviter des situations où un sélecteur peut être activé avant un pont, ce qui crée des erreurs d'aiguillage temporaires entre le trafic actif et le trafic supplémentaire.

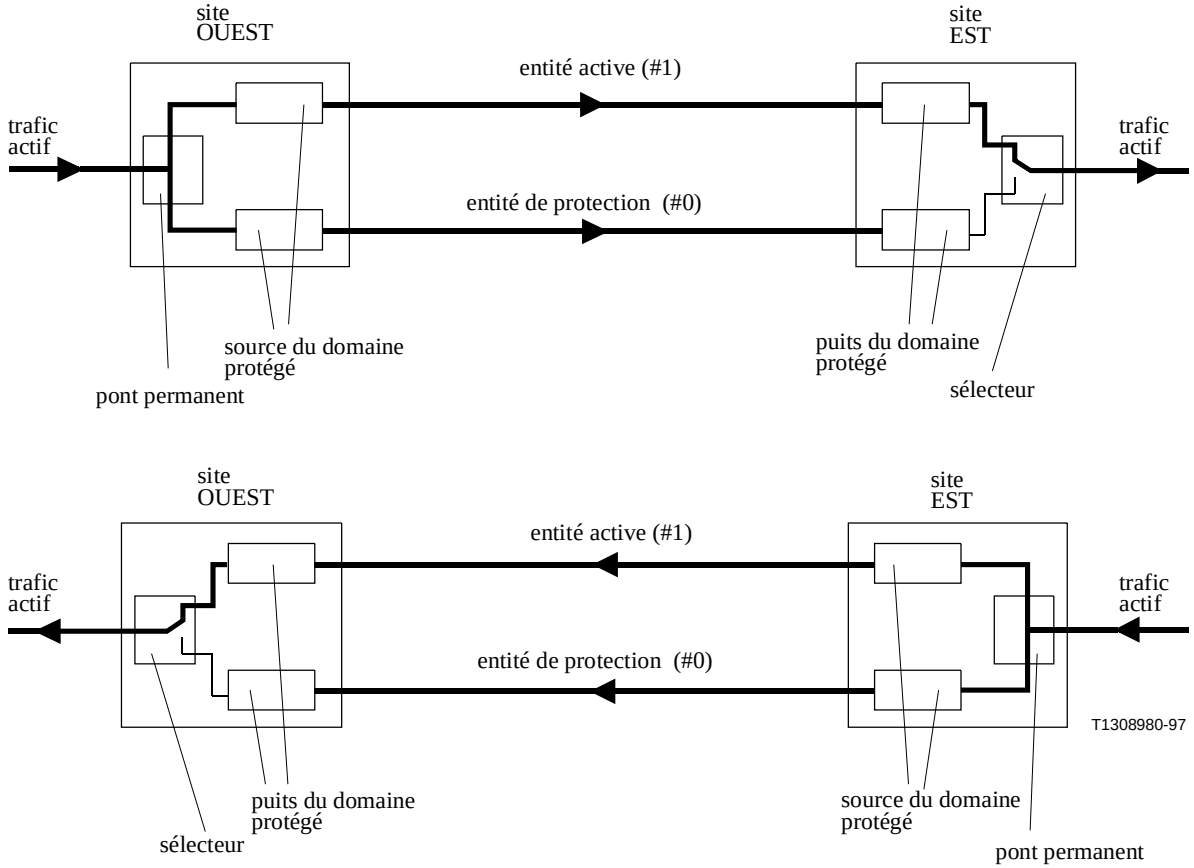


Figure A.1/I.630 – Architecture de commutation de protection linéaire 1+1 – Le sélecteur est positionné pour recevoir le trafic depuis l'entité active (#1)

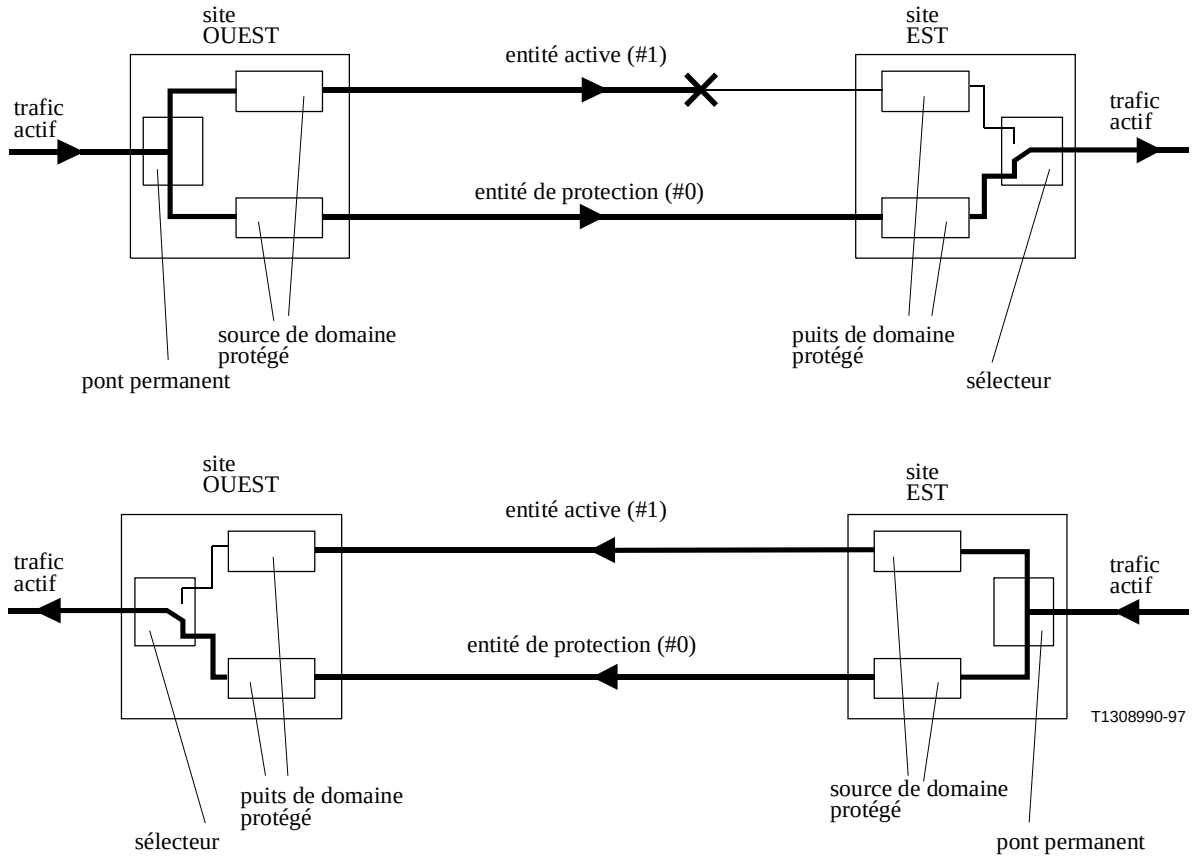


Figure A.2/I.630 – Architecture de commutation de protection linéaire 1+1 – Le sélecteur est positionné pour recevoir le trafic depuis l'entité de protection (#0) due à une panne de signal unidirectionnel pour l'entité (#1)

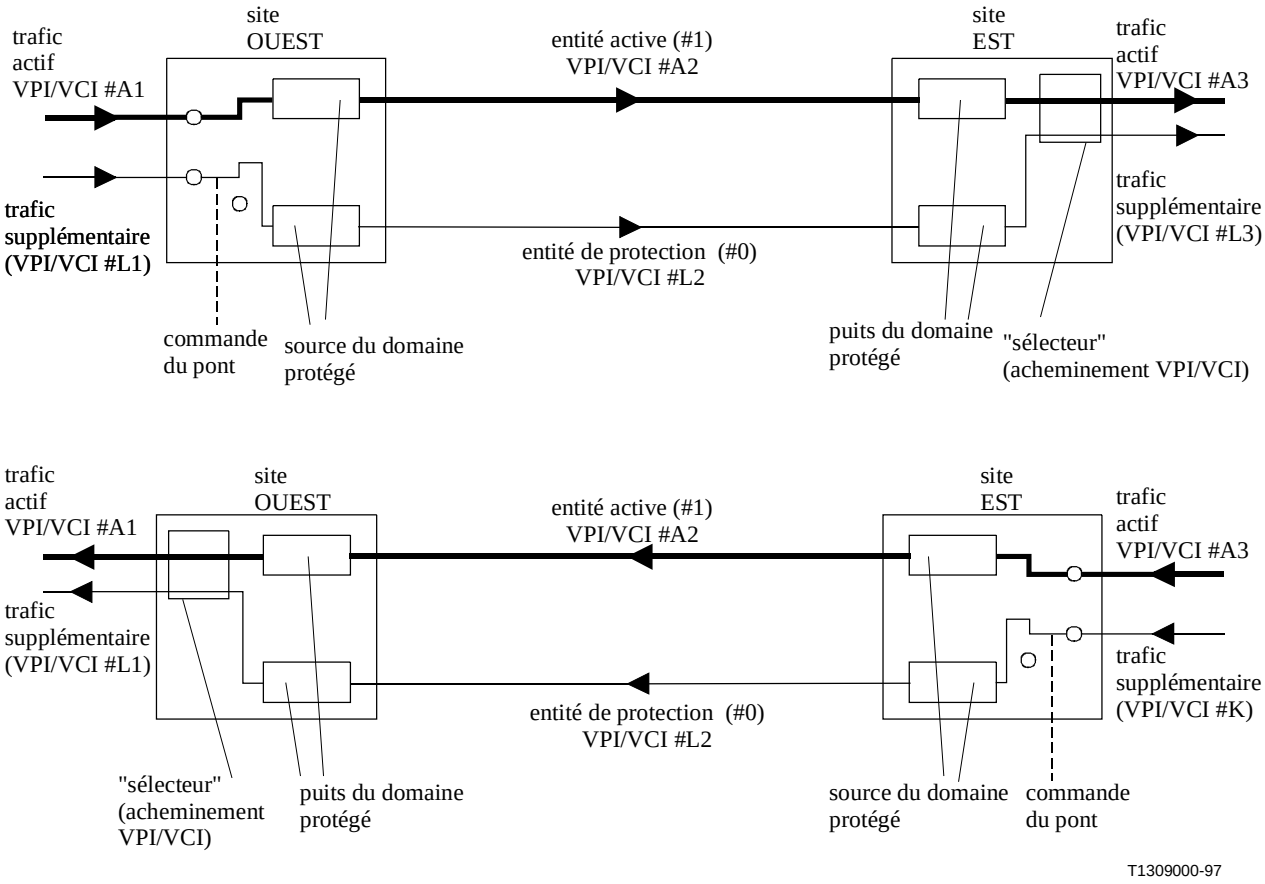


Figure A.3/I.630 – Architecture de commutation de protection linéaire 1:1 – Transmission du trafic actif via l'entité active (#1)

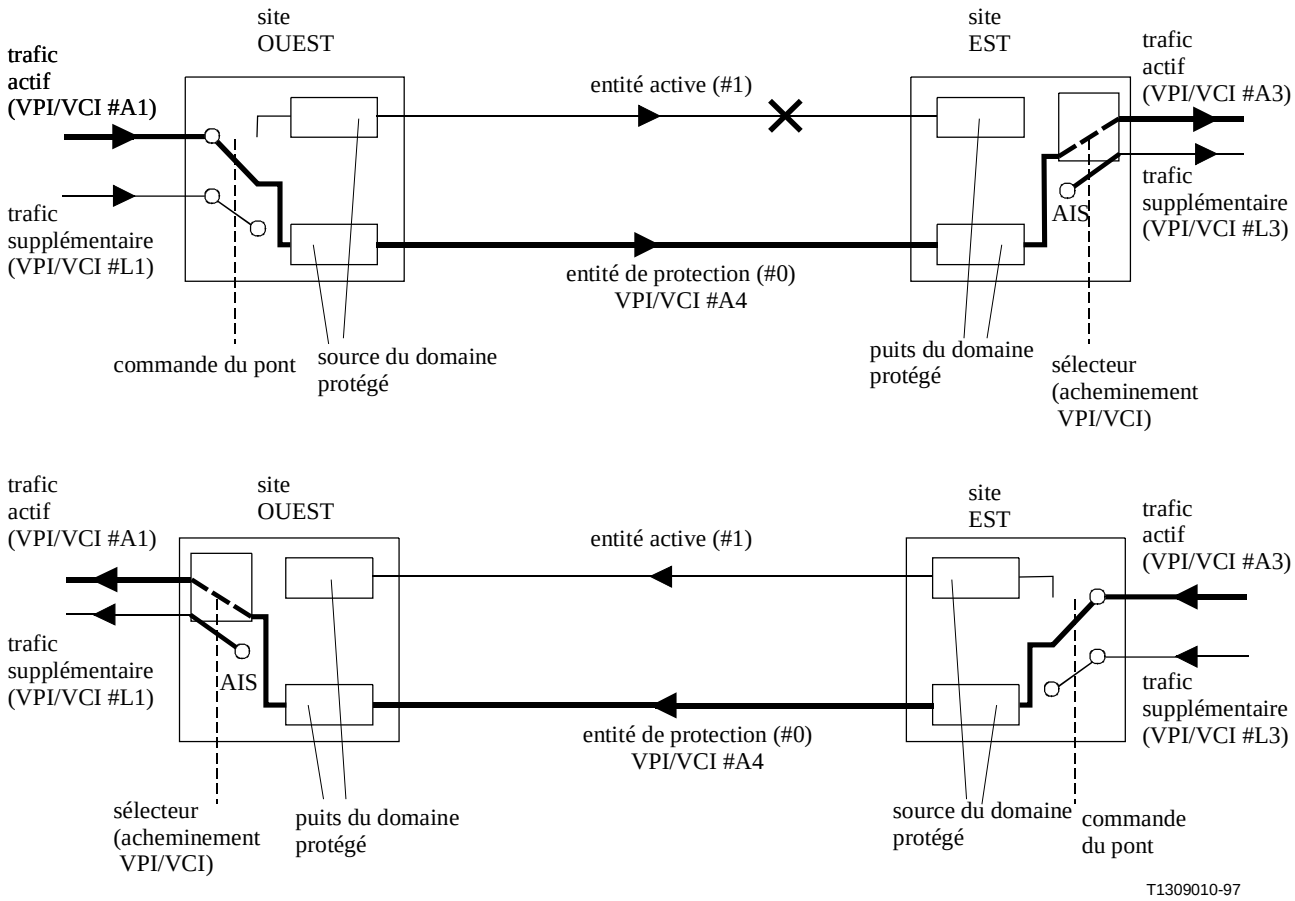


Figure A.4/I.630 – Architecture de commutation de protection linéaire 1:1 – Transmission du trafic actif via l'entité de protection (#0) due à une panne de signal unidirectionnel pour l'entité (#1)

A.1.2 Compatibilité avec les objectifs de réseau

La compatibilité entre les objectifs de réseau importants et le protocole de commutation de protection linéaire ATM est analysée dans le A.2.

1) *Étendue de la protection*

   Pour une panne affectant un point unique, tout le trafic qui aurait dû passer par ce point s'il n'y avait pas eu de panne, est rétabli. Dans le cas de plusieurs pannes, la panne présentant le plus haut niveau de priorité est prioritaire. Par exemple, une panne de type SF a priorité sur une panne de type SD.

2) *Types de commutation*

   La commutation bidirectionnelle est prise en charge dans la présente annexe.

3) *Protocole de commutation de protection*

   Le protocole de commutation de protection est simple, rapide et fiable. La simplicité facilite la mise en œuvre et assure la transparence des opérations. Un protocole rapide (ou "à prise de contact optimisée") permet de respecter plus facilement le temps d'exécution de la commutation exigé. Le protocole est fiable grâce à sa simplicité intrinsèque, ce qui rend un mauvais fonctionnement peu probable (dû à des erreurs de mise en œuvre résiduelles).

4) *Modes opératoires*

La commutation réversible est assurée. Pour des architectures 1:1 sans trafic supplémentaire et pour des architectures 1+1, la commutation non réversible est également possible.

5) *Commande manuelle*

Les commandes d'opérateur (gel de la fonction de protection locale, la désactivation de la protection, la commutation forcée et la commutation manuelle) sont acceptées. Le protocole étant particulièrement simple, il n'exige de la part de l'opérateur aucun entraînement préalable.

6) *Autres critères de déclenchement de la commutation*

Outre les commandes manuelles précitées, les commandes panne de signal, dégradation de signal, attente avant rétablissement, ne pas retourner et pas de requête sont prises en charge en tant que critères de déclenchement (ou d'empêchement) d'une commutation de protection.

A.2 Protocole de commutation de protection linéaire 1+1/1: 1

A.2.1 Critères de déclenchement de la commutation

Les critères de déclenchement de la commutation de protection sont les suivants:

1) une commande à déclenchement externe (annulation, gel de la fonction locale de commutation de protection, blocage de la protection, commutation forcée, commutation manuelle);
2) une commande à déclenchement automatique (panne ou dégradation de signal) associée à un domaine de protection;
3) un état ("attente avant rétablissement", "non-retour à l'état initial", "pas de requête") de la fonction commutation de protection.

A.2.1.1 Commandes à déclenchement externe

Les commandes à déclenchement externe sont indiquées ci-dessous par ordre décroissant de priorité. Chaque commande peut être appliquée à l'élément OUEST ou à l'élément EST de réseau d'un système de commutation de protection automatique linéaire (comme par exemple, celui de la Figure A.1).

Annulation: annule toutes les commandes citées ci-dessous pour l'élément de réseau associé. Il convient de noter que la commande Annulation n'est utilisée que pour réinitialiser la fonction de gel de la commutation de protection locale, désactivation de la protection, les commandes commutation forcée ou manuelle. Cette commande n'est pas signalée via le protocole de commutation de protection.

Gel de la fonction de commutation de protection locale: cette commande gèle (maintient) la position du moment du pont/sélecteur et les valeurs des octets K1/K2 du moment transmis pour la fonction de commutation de protection locale. Sa priorité est la plus élevée de toutes les commandes à déclenchement externe autres que l'annulation. Ainsi, les requêtes locales autres que l'annulation sont ignorées lorsque cette commande est en cours. Il convient de noter que les octets K1/K2 reçus depuis l'extrémité distante continuent d'être évalués de sorte que la détection locale de non concordance de pont/sélecteur reste possible. Cette commande n'est pas signalée via le protocole de commutation de protection.

NOTE – Cette commande est principalement destinée à la maintenance. Lorsque les tâches de maintenance sont effectuées sur l'entité active, on peut demander à ce que l'entité active ne soit pas utilisée même si l'entité de protection a une panne. A cette fin, la commande FS ne peut être utilisée car cette commande ne serait pas

prioritaire pour une panne de signal dans l'entité de protection. Voici un exemple possible de scénario de maintenance:

1) confirmation que l'entité de protection n'est pas en panne;

2) émission d'une commande FS pour passer sur l'entité de protection;

3) émission d'une commande "gel de la fonction de commutation de protection locale";

4) exécution des travaux de maintenance sur l'entité active;

5) annulation de la commande "gel de la fonction de commutation de protection locale".

Désactivation de la protection (LoP, *lockout of protection*): interdit à tout le trafic actif (mais pas au trafic supplémentaire) l'accès à l'entité de protection.

Commutation forcée (FS, *forced switch*) pour l'entité active (#1): ponte/commute le trafic actif (#1) sur l'entité de protection, à moins qu'il existe une condition de panne de signal pour l'entité de protection. Il convient de noter que la commutation forcée pour l'entité de protection (#0) n'est pas définie, étant donné que cette fonctionnalité est accomplie par une commande désactivation de la protection.

Commutation manuelle (MS, *manual switch*) pour l'entité de protection (#0): interdit au trafic actif l'accès à l'entité de protection à moins qu'une requête de priorité plus élevée (telle une panne de signal ou une dégradation de signal pour une entité active) soit en cours de traitement.

Commutation manuelle (MS) pour l'entité active (#1): ponte/commute le trafic actif (#1) sur l'entité de protection, à moins qu'une requête de priorité plus élevée soit en cours de traitement.

Il convient de noter que des commandes destinées à l'entraînement, telles que définies pour des protocoles de protection plus complète, ne sont pas nécessaires et par conséquent ne sont pas définies.

A.2.1.2 Commandes à déclenchement automatique

Pour empêcher des transitions fréquentes, la transition de panne de signal de la condition active à la condition inactive ne doit se produire que si l'état AIS dure au moins 5 secondes.

A.2.1.3 Etats

L'état "attente avant rétablissement" (WTR, *wait to restore*) ne s'applique qu'en mode réversible à une entité active (#1). On passe à cet état au moyen de la fonction de commutation de protection locale lorsque le trafic actif (#1) est reçu via l'entité de protection et que les requêtes de commutation de protection locale (voir Figure A.5) précédemment actives sont devenues inactives. On empêche ainsi le retour sur la position du pont/sélecteur libérée jusqu'à ce que le délai "attente avant rétablissement" ait expiré. Le délai d'attente avant rétablissement est configuré par l'opérateur par pas de 1 minute et est compris entre 1 et 30 minutes; la valeur par défaut est de 12 minutes.

L'état "non-retour à l'état initial" (DNR, *do not revert*) est seulement applicable au mode non réversible (qui est possible dans les architectures 1:1 sans trafic supplémentaire ou dans les architectures 1+1) et est seulement défini pour l'entité active (#1). Le passage à cet état par la fonction de commutation de protection locale s'effectue dans les conditions dans lesquelles le trafic (#1) se trouve transmis via l'entité de protection, si les requêtes de commutation de protection locale (voir Figure A.5) précédemment actives sont devenues inactives. Cet état empêche le retour sur la position initiale du pont/sélecteur dans le mode non réversible en l'absence de requête.

L'état "pas de requête" [(NR, *no request*) qui est seulement défini pour l'entité de protection (#0)] est l'état commandé par la fonction de commutation de protection locale (voir Figure A.5) où toutes les conditions où aucune requête de commutation de protection locale (y compris attendre avant de rétablir et ne pas inverser) n'est active; il convient de noter qu'une telle situation peut apparaître lorsque le pont/sélecteur est activé ou lorsqu'il est désactivé.

A.2.2 Règles de formation des octets K1/K2

NOTE – Dans la présente annexe, le bit 1 est le bit de plus fort poids (MSB) et le bit 8 est le bit de plus faible poids (LSB).

Dans le cas d'un protocole linéaire 1+1/1:1, l'information protocolaire est acheminée entre les éléments de réseau aux sites OUEST et EST via 2 octets d'information appelés K1 et K2. Ces 2 octets sont véhiculés par des cellules APS via l'entité de protection (voir par exemple Figure A.1), ils sont insérés par la fonction source du domaine de protection et extraits par la fonction puits du domaine de protection. Tous les bits de l'octet K1 sont définis; en revanche, seuls les 4 premiers bits de l'octet K2 sont définis.

Les règles de formation dans le cas d'un protocole linéaire 1+1/1:1 sont les suivantes:

les bits 1 à 8 de l'octet K1 indiquent une requête d'action de commutation de la logique de priorité locale de la commutation de protection (voir Figure A.5).

Les bits 1 à 4 indiquent le type de requête (voir Tableau A.1).

Les bits 5 à 8 de l'octet K1 indiquent le numéro de l'entité associée, à savoir si la requête s'applique à l'entité active (#1 à #n, n étant inférieur ou égal à 15) ou à l'entité de protection (#0), comme suit:

bits 5678	
0000	la requête s'applique à l'entité de protection.
0001	la requête s'applique à l'entité active (# 1).

Les bits 1 à 4 du demi-octet K2 indiquent l'état du pont/sélecteur local de la logique de priorité global de la commutation de protection (voir Figure A.5), comme suit:

Pour le mode opératoire 1+1, la position du sélecteur de l'élément de réseau local est indiquée de la manière suivante:

bits 1234	
0000	le sélecteur est activé pour recevoir le trafic depuis l'entité de protection (voir Figure A.2).
0001	le sélecteur est désactivé pour recevoir le trafic depuis l'entité active (#1) (voir Figure A.1).

Pour le mode opératoire 1:1, la position du pont/sélecteur de l'élément de réseau local est indiquée comme suit:

bits 1234	
0000	le pont/sélecteur est désactivé de sorte que le trafic est transmis via les entités actives associées et le trafic supplémentaire (s'il est configuré) est transmis via l'entité de protection.
0001	le pont/sélecteur est activé pour transmettre le trafic actif (#1) via l'entité de protection.

Il convient de noter que la stratégie qui est différente pour le codage du bit de l'octet K2 pour le mode 1+1 et pour le mode 1:1, permet le déclenchement automatique d'une alarme de défaut de correspondance si l'élément de réseau à une extrémité du domaine de protection est configuré pour le mode 1+1 et que l'autre extrémité est (involontairement) configurée pour le mode 1:1.

Les bits 5 à 8 de l'octet K2 ne sont pas utilisés dans le protocole 1+1/1:1 linéaire.

Tableau A.1/I.630 – Code de l'octet K1 pour les requêtes

Codage de l'octet K1: bits 1234	Requête (c'est-à-dire commande à déclenchement automatique, état ou commande à déclenchement externe)	Ordre de priorité
1111	Désactivation de la protection (Note 1)	La plus élevée
1110	Panne de signal pour l'entité de protection (Note 1)	|
1101	Commutation forcée pour l'entité active (#1) (Note 5)	|
1100	Réservé à une utilisation future (Note 2)	|
1011	Panne de signal pour l'entité active (#1)	|
1010	Réservé à une utilisation future (Note 2)	|
1001	Dégradation de signal pour l'entité de protection	|
1000	Dégradation de signal pour l'entité active (#1)	|
0111	Réservé à une utilisation future (Note 2)	|
0110	Commutation manuelle de l'entité de protection	|
0101	Commutation manuelle de l'entité active (#1)	|
0100	Réservé à une utilisation future (Note 2)	|
0011	Attendre avant de rétablir pour l'entité active (#1) (Note 3)	|
0010	Réservé à une utilisation future (Note 2)	|
0001	Ne pas inverser pour l'entité active #1 (Note 4)	|
0000	Pas de requête (Note 1)	La plus faible

Il convient de noter que dans le cas où plusieurs requêtes de même priorité, énumérées dans le présent tableau sont simultanément actives, la requête associée au numéro d'entité le plus faible a la priorité. Par conséquent, une requête (par exemple dégradation de signal) pour une entité de protection (#0) a priorité sur la même requête concernant l'entité active (#1).

NOTE 1 – Seul le codage des bits 5 à 8 de l'octet K1 "0000" est autorisé avec les requêtes suivantes: pas de requête, désactivation de la protection, panne de signal pour l'entité de protection, dégradation du signal pour l'entité de protection et commutation manuelle pour l'entité de protection.

NOTE 2 – Ces codes sont ignorés par le récepteur.

NOTE 3 – Attendre avant de rétablir pour l'entité active (#1) n'est applicable que pour le mode avec inversion.

NOTE 4 – "Non retour à l'état initial" pour l'entité active (#1) n'est applicable que pour le mode non réversible: seule la valeur "0001" pour le codage des bits 5 à 8 de l'octet K1 est autorisée.

NOTE 5 – La commutation forcée pour l'entité de protection (#0) n'est pas définie car cette fonction peut être réalisée par le blocage de la commande de protection.

A.2.3 Algorithme de commutation de protection linéaire 1+1/1:1

A.2.3.1 Principe de fonctionnement

La Figure A.5 illustre le principe de l'algorithme de commutation de protection linéaire 1+1/1:1. Cet algorithme est exécuté dans les éléments de réseau aux deux extrémités du domaine de protection (sites OUEST et EST). La commutation bidirectionnelle est réalisée en transmettant des requêtes de commutation locale à l'extrémité distance via l'octet K1. L'octet K2 transmis contient l'information d'état concernant le pont/sélecteur local; un défaut de correspondance persistant entre les deux extrémités peut ainsi être détecté et déclencher une alarme.

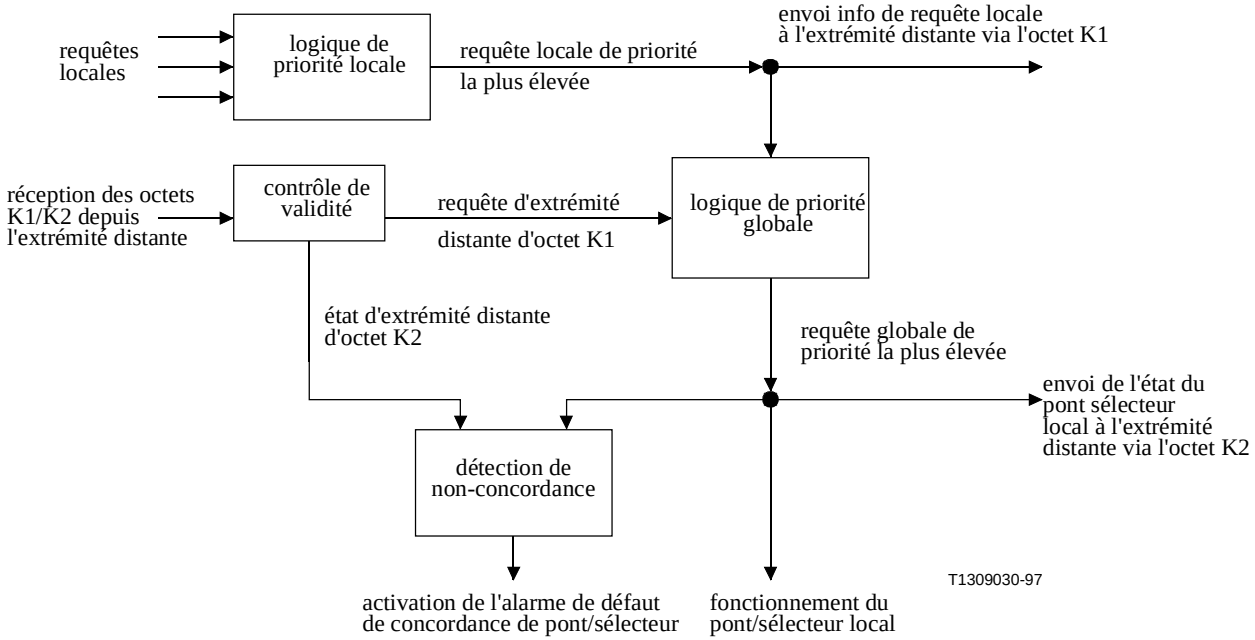


Figure A.5/I.630 – Principe de l'algorithme de commutation de protection linéaire 1+1/1:1

Cet algorithme fonctionne de manière détaillée comme suit (voir Figure A.5):

au niveau de l'élément de réseau une ou plusieurs requêtes de commutation de protection locale (telles qu'énumérées au A.2.1) peuvent être actives. La "logique de priorité locale" détermine laquelle de ces requêtes a la priorité la plus élevée sur la base de la hiérarchie des priorités du Tableau A.1. Cette information de requête locale de priorité la plus élevée est transmise à l'extrémité distante sur l'octet K1 (selon le codage décrit au A.2.2). Elle est également transmise à la "logique de priorité globale".

L'élément de réseau local reçoit l'information de l'élément de réseau de l'extrémité distante par l'intermédiaire des octets K1 et K2. Ces octets sont soumis à une vérification de validité (voir A.2.3.4). Les informations contenues dans l'octet K1 reçu (qui indique la requête locale de priorité la plus élevée à l'extrémité distante) sont ensuite transmises à la "logique de priorité globale". Cette logique compare la requête locale de priorité la plus élevée avec la requête de l'octet K1 reçu (selon l'ordre de priorité donné dans le Tableau A.1) afin de déterminer la requête de priorité globale la plus élevée. Cette requête ensuite détermine la position (ou l'état) du pont/sélecteur de l'élément de réseau local comme suit:

– pour les architectures 1+1 (voir les Figures A.1 et A.2), seule la position du sélecteur est commandée. Pour les architectures 1:1 (voir Figures A.3 à A.5) les positions du pont et du sélecteur sont commandées simultanément, c'est-à-dire à chaque fois que le pont d'un

élément de réseau est activé (ou désactivé), le sélecteur du même élément de réseau est activé (ou désactivé) en même temps;

– si la requête globale de priorité la plus élevée est une requête pour une entité active (voir le Tableau A.1), le trafic actif associé est ponté/commuté vers/à partir de l'entité de protection, c'est-à-dire que le pont/sélecteur associé de l'élément de réseau local est activé;

– si la requête globale de priorité la plus élevée est une requête pour une entité de protection (voir Tableau A.1), aucun trafic actif n'est ponté/commuté vers/depuis l'entité de protection, c'est-à-dire que le pont/sélecteur associé de l'élément de réseau local est désactivé.

L'état du pont/sélecteur est transmis à l'extrémité distante via l'octet K2 (avec le codage décrit au A.2.2). Il est également comparé avec l'état du pont/sélecteur de l'extrémité distante tel qu'indiqué par l'octet K2 reçu: si une incompatibilité entre les positions de l'extrémité proche et de l'extrémité distante persiste pendant plus de *m* secondes, une alarme d'incompatibilité de pont/sélecteur est déclenchée pour l'élément de réseau local. La durée *m* est suffisamment longue pour tolérer la perte de 3 cellules de protocole APS avant de déclencher l'alarme.

Il convient de noter que l'algorithme de commutation de protection linéaire commence à être exécuté immédiatement chaque fois qu'un des signaux d'entrée est modifié (voir Figure A.5), c'est-à-dire lorsque l'état d'une requête locale change, ou lorsqu'un octet K1/K2 différent est reçu depuis l'extrémité distante. Des actions consécutives de l'algorithme sont également déclenchées immédiatement, c'est-à-dire la modification de la position du pont/sélecteur local (si nécessaire), la transmission d'un nouvel octet K1/K2 (si nécessaire), ou le déclenchement d'une alarme d'incompatibilité de position pont/sélecteur (si le délai autorisé a expiré).

A.2.3.2 Mode réversible

Dans le mode de fonctionnement réversible, lorsque le trafic actif (#1) est reçu via l'entité de protection et que les requêtes de commutation de protection locale (voir Figure A.5) précédemment actives sont devenues inactives, on passe à un état local "attente avant rétablissement". Etant donné que cet état représente maintenant la requête locale de priorité la plus élevée, il est indiqué sur l'octet K1 transmis et l'état du commutateur reste inchangé.

La temporisation associée à cet état "attente avant rétablissement" (voir A.2.1.3) normalement expire et cet état devient un état de non-requête. Ce temporisateur est désactivé avant expiration si une requête de priorité plus élevée préempte cet état.

Il convient de noter que seules les requêtes locales sont prises en considération pour décider de passer ou non à l'état "attente avant rétablissement". Une commutation sur l'entité de protection peut être maintenue par un état "attente avant rétablissement" ou par une requête distante ("attente avant rétablissement" ou autre) reçue via l'octet K1. Par conséquent, lorsqu'une panne bidirectionnelle sur une entité active s'est produite et que les réparations ont été effectuées, le retour bidirectionnel vers l'entité active ne se produit pas jusqu'à ce que les temporisations "attente avant rétablissement" aux deux extrémités aient expiré.

A.2.3.3 Mode non réversible

Le mode non réversible n'est applicable (comme option au mode réversible) qu'aux architectures 1+1 ou 1:1 dans des configurations sans trafic supplémentaire.

Dans le mode non réversible, lorsque le trafic (#1) est transmis via l'entité de protection, et que les requêtes de commutation de protection locale (voir Figure A.5) précédemment actives sont devenues inactives, on passe à un état local pas de retour à l'état initial. Etant donné que cet état représente maintenant la requête locale de priorité la plus élevée, il est indiqué sur l'octet K1 transmis et maintient le commutateur, empêchant ainsi le retour sur la position initiale du pont/sélecteur libérée dans un mode non réversible en l'absence de requête.

A.2.3.4 Transmission et acceptation des octets de protocole de protection

Les octets K1/K2 du protocole de protection sont transportés par des cellules APS via l'entité de protection (voir par exemple Figure A.1), et sont insérés par la fonction source du domaine de protection et extraits par la fonction puits du domaine de protection.

Une nouvelle cellule APS doit être transmise immédiatement dès qu'une modification d'état des octets K1 ou K2 transmis (voir Figure A.5) a lieu.

Pour éviter une production excessive de cellules APS dans des cas où le détecteur de panne de signal oscille rapidement, lors du traitement des requêtes locales (voir Figure A.5) le passage de la panne de signal de la condition active à la condition inactive doit uniquement se produire si l'état AIS persiste pendant 5 secondes.

Pour permettre le bon fonctionnement du protocole dans des situations où des cellules APS sont perdues ou ne sont pas valides, une cellule APS donnant l'état de transmission de l'octet K1/K2 courant sera transmise par l'élément de réseau dans des conditions de régime permanent toutes les 5 secondes (mécanisme de "survie"). Ceci permet de ne pas prévoir de scénarios de protocole complexes de retransmission lorsque des cellules APS sont perdues ou ne sont pas valides. Pour les architectures 1:1, cela conduit à l'exécution d'une commutation de protection différée de 5 secondes lorsqu'une cellule APS sera perdue ou non valide.

En cas de réception d'octets K1/K2 non valides, les derniers octets valides reçus restent applicables. Pendant une panne de signal au niveau de l'entité de protection (prolongée de 5 secondes, telle que décrite précédemment), les octets K1/K2 ne sont pas évalués.

A.2.3.5 Exemple de protocole dans le cas d'une architecture 1+1 en mode non réversible

Le Tableau A.2 illustre une action de commutation de protection (en mode non réversible) pour ce système.

Lorsque le trafic est reçu en provenance de l'entité active (#1) en l'absence de panne, les octets K1 transmis aux deux extrémités indiquent l'absence de requête avec le numéro d'entité "0". Les bits 1 à 4 des octets K2 transmis aux deux extrémités sont positionnés à "0001" pour indiquer que le sélecteur est désactivé et qu'il reçoit le trafic en provenance de l'entité active (#1). Voir Figure A.1 qui illustre ce cas.

La logique de priorité globale de chaque extrémité détermine la requête globale active de priorité la plus élevée. Il peut s'agir d'une requête de l'extrémité distante (reçue via l'octet K1) ou une requête locale. La logique de priorité globale positionnera le sélecteur local conformément à la requête globale de priorité la plus élevée. La position résultante du sélecteur sera indiquée dans les bits 1 à 4 de l'octet K2. Pour la formation de l'octet K1 transmis, seule la requête locale de priorité la plus élevée sera prise en considération; les requêtes extrémité distante ne sont jamais prises en considération.

Dans l'exemple, une panne de signal est détectée à l'emplacement EST sur l'entité active (#1). En conséquence, la logique de priorité globale à l'EST active le sélecteur pour recevoir le trafic en provenance de l'entité de protection (#0). La logique de priorité globale à l'OUEST détecte la panne via l'octet K1 reçu et active également son sélecteur, en maintenant l'indication "pas de requête" pour l'octet K1 transmis, étant donné qu'aucune requête locale n'est active. Voir Figure A.2 qui illustre cette situation.

Après réparation de l'entité active (#1), l'état "non-retour à l'état initial" est indiqué à l'EST et les sélecteurs à l'EST et à l'OUEST restent activés. Le système ne revient pas sur une entité préférée comme dans le cas d'un fonctionnement réversible. Il convient de noter que l'état "non-retour à l'état initial " est effacé s'il est préempté par une requête locale. Par conséquent, si une panne de type SD de l'entité de protection (#0) est ensuite détectée à l'EST, cela sera indiqué dans l'octet K1 transmis à

l'EST et le sélecteur à l'EST sera libéré. La logique de priorité globale à l'OUEST détecte la panne via l'octet K1 reçu et désactive aussi son sélecteur.

Après que l'entité de protection (#0) ait été réparée, l'état "pas de requête" est de nouveau indiqué aux deux extrémités.

Il convient de noter que pour le même exemple et avec un fonctionnement mode réversible, le message "non-retour à l'état initial" ne sera jamais indiqué. Après réparation de l'entité active (#1), le message "attente avant rétablissement" est indiqué à l'EST au lieu du message "non-retour à l'état initial". Il convient de noter que le message "attente avant rétablissement" est effacé et que le temporisateur est réinitialisé s'il est préempté par une requête locale. A la fin de la temporisation "attente avant rétablissement", les deux sélecteurs sont désactivés pour recevoir le trafic depuis l'entité active (#1) et le message "pas de requête" est indiqué aux deux extrémités.

Tableau A.2/I.630 – Exemple de protocole pour architecture 1+1 dans le cas d'un mode opératoire non inversible

Conditions de panne	**Codage des octets de protocole**				**Action**	
	EST → OUEST		**OUEST → EST**			
Bits	**Octet K1 12345678**	**Octet K2 1234**	**Octet K1 12345678**	**Octet K2 1234**	**A l'EST**	**A l'OUEST**
Pas de panne. Le trafic reçu provient de l'entité active (#1)	00000000	0001	00000000	0001	Sélecteur désactivé	Désactivation du sélecteur
L'entité active (#1) est en panne dans le sens OUEST → EST	10110001	0000	00000000	0001	Détection d'une requête locale. Activation du sélecteur; actualisation de K1/K2.	
	10110001	0000	00000000	0000		Détection de la requête de l'extrémité distante Activation du sélecteur; actualisation de K1/K2.
L'entité active (#1) est réparée	00010001	0000	00000000	0000	Détection de l'effacement de la requête locale; Passage à l'état ne pas inverser: Actualisation de K1.	
L'entité de protection (#0) subit une dégradation dans le sens OUEST → EST	10010000	0001	00000000	0000	Détection de la requête locale; libération du sélecteur; actualisation de K1/K2.	

Tableau A.2/I.630 – Exemple de protocole pour architecture 1+1 dans le cas d'un mode opératoire non inversible *(fin)*

Conditions de panne / Bits	Codage des octets de protocole				Action	
	EST → OUEST		OUEST → EST			
	Octet K1 12345678	Octet K2 1234	Octet K1 12345678	Octet K2 1234	A l'EST	A l'OUEST
	10010000	0001	00000000	0001		Détection de la requête extrémité distante. Désactivation du sélecteur; actualisation K1/K2.
L'entité de protection (#0) est réparée	00000000	0001	00000000	0001	Etat "pas de requête". Actualisation K1.	

A.2.3.6 Exemple de protocole dans le cas d'une architecture 1:n sans retour à l'état initial

Le Tableau A.3 illustre une action de commutation de protection (dans le mode sans retour) pour ce système.

Dans des conditions normales de fonctionnement, tout le trafic actif est transmis via les entités actives associées et le trafic supplémentaire est transmis le cas échéant via l'entité de protection (#0). Les ponts/commutateurs OUEST et EST sont désactivés. Les octets K1 transmis aux deux extrémités comportent l'indication "pas de requête" avec un numéro d'entité "0", l'octet K2 transmis aux deux extrémités contiennent l'indication "0000".

La logique de priorité globale de chaque extrémité détermine la requête de priorité globale plus élevée qui est active. Il peut s'agir d'une requête d'extrémité distante (reçue via l'octet K1) ou d'une requête locale. La logique de priorité globale positionnera le pont/sélecteur local conformément à la requête globale de priorité la plus élevée. La position résultante du pont/sélecteur sera indiquée dans les bits 1 à 4 de l'octet K2. Pour la formation de l'octet K1 transmis, seule la requête locale de priorité la plus élevée est prise en considération; les requêtes d'extrémités distantes ne sont jamais prises en considération.

Dans l'exemple, une panne de signal est détectée à l'emplacement EST de l'entité active (#1). En conséquence, la logique de priorité globale à l'EST activera le pont/sélecteur de manière à transmettre le trafic actif (#1) vers l'entité de protection (#0). La logique de priorité globale à l'OUEST détecte la panne via l'octet K1 reçu et également active le son pont/sélecteur, conservant l'indication "pas de requête" pour l'octet K1 transmis, étant donné qu'aucune requête locale n'est active. La Figure A.5 illustre cet exemple.

Après réparation de l'entité active (#1), le message "attente avant rétablissement" est indiqué à l'EST et les ponts/commutateurs EST et OUEST restent activés. Il convient de noter de l'indication "attente avant rétablissement" est effacée et le temporisateur réinitialisé s'il y a préemption par une requête locale. Lorsque la temporisation "attente avant rétablissement" expire à l'EST, il y a à l'EST passage à l'état pas de requête, le pont/sélecteur est désactivé et les octets K1/K2 transmis sont actualisés. Ainsi, le système reprend une nouvelle fois encore un mode de fonctionnement normal dans un l'état où il n'y a pas de panne.

Tableau A.3/I.630 – Exemple de protocole pour une architecture 1:n dans le mode opératoire avec retour

Conditions de panne	Codage des octets de protocole				Action	
	EST → OUEST		OUEST → EST			
Bits	Octet K1 12345678	Octet K2 1234	Octet K1 12345678	Octet K2 1234	A l'EST	A L'OUEST
Pas de panne. Tout le trafic actif est transmis via les entités actives associées.	00000000	0000	00000000	0000	Désactivation du pont/sélecteur	Désactivation du pont/sélecteur
L'entité active (#1) tombe en panne dans le sens OUEST → EST	10110001	0001	00000000	0000	Détection d'une requête locale. Activation du pont/sélecteur pour le trafic actif (#1); actualisation K1/K2.	
	10110001	00001	00000000	00001		Détection d'une requête d'extrémité distante. Activation du pont/sélecteur pour le trafic actif (#1); actualisation K2.
Entité active (#1) réparée	00110001	00001	00000000	00001	Détection suppression de requête locale. Passage à l'état attendre pour rétablir pour le trafic actif (#1); actualisation de K1.	
Expiration du délai attendre pour rétablir à l'EST	00000000	0000	00000000	00001	Etat pas de requête. Désactivation pont/sélecteur; actualisation K1/K2.	
	00000000	0000	00000000	0000		Pas de requête (locale ou depuis l'extrémité distante). Désactivation du pont/sélecteur; actualisation K2.

ANNEXE B

Commutation de protection 1+1 unidirectionnelle connexion de sous-réseau (SNC) et de chemin

B.1 Architecture d'application

L'architecture de commutation de protection linéaire 1+1 est représentée à la Figure A.1. Dans le cas d'une commutation de protection unidirectionnelle telle que décrite dans l'Annexe B, celle-ci est exécutée par le sélecteur au niveau du puits de domaine de protection sur la base d'informations exclusivement locales.

Par exemple, si une panne unidirectionnelle (dans le sens OUEST-EST) se produit pour l'entité active de la Figure A.1, cette panne sera détectée au niveau du puits du domaine de protection au site EST et le sélecteur au site EST commutera sur l'entité de protection. Il convient de noter que l'état du sélecteur à la position OUEST n'est pas modifié.

B.2 Conformité avec les objectifs de réseau

Les objectifs de réseau suivants s'appliquent:

1) *Types de commutation*

   La commutation de protection unidirectionnelle 1+1 est prise en charge dans la présente annexe;

2) *Protocole de commutation de protection*

   Il n'y a pas de protocole APS pour la protection 1+1 unidirectionnelle de connexion SNC et de chemin;

3) *Modes opératoires*

   Les modes opératoires pris en charge sont les modes de commutation avec retour et sans retour;

4) *Commande manuelle*

   Les commandes manuelles à savoir les commandes de désactivation de la protection, de commutation forcée et de commutation manuelle sont prises en charge;

5) *Autre critère de déclenchement de la commutation*

   Les états panne ou de dégradation de signal, "attente avant rétablissement" et "pas de requête" sont pris en charge outre les commandes manuelles précitées, en tant que critères de déclencher ou de blocage de la commutation de protection.

B.3 Critère de déclenchement de la commutation

Les critères de déclenchement de la commutation suivants sont pris en charge:

1) commande externe (libération, désactivation de la protection, commutation forcée, commutation manuelle);
2) commande automatique (panne ou dégradation de signal) associée à un domaine protégé;
3) un état ("attente avant rétablissement", "pas de requête") de la fonction commutation de protection.

Pour l'architecture 1+1, toutes les requêtes sont locales. L'ordre de priorité des requêtes locales est donné dans le Tableau B.1.

Tableau B.1/I.630 – Priorité des requêtes locales

Requête locale (c'est-à-dire commande ou état déclenché automatiquement ou bien commande à déclenchement externe)	Ordre de priorité
Annulation	La plus élevée
Désactivation de la protection	|
Commutation forcée	|
Panne de signal	|
Dégradation de signal	|
Commutation manuelle	|
"attente avant rétablissement"	|
Pas de requête	La plus faible

NOTE 1 – Une panne de signal sur l'entité de protection n'a pas priorité sur une commutation forcée concernant l'entité active. Etant donné que la commutation de protection unidirectionnelle est en cours d'exécution et qu'aucun protocole APS n'est pris en charge sur l'entité de protection, la panne de signal sur l'entité de protection n'interfère pas avec la capacité à exécuter une commutation forcée concernant l'entité active.

NOTE 2 – La commutation forcée concernant une entité de protection n'est pas définie car cette fonction peut être obtenue par désactivation de la commande de protection.

B.3.1 Commandes à déclenchement externe

La liste des commandes à déclenchement externe est donnée ci-après par ordre de priorité décroissante. La fonction de chaque commande est indiquée.

annulation: annule toutes les commandes de commutation déclenchées extérieurement et indiquées ci-dessous.

désactivation de la protection (LoP, *lockout of protection*): empêche le sélecteur de se positionner sur l'entité de protection, ou commute le sélecteur de l'entité de protection sur l'entité active.

commutation forcée (FS, *forced switch*) concernant l'entité active: commute le sélecteur de l'entité active sur l'entité de protection (à moins qu'une requête de commutation de priorité plus élevée ne soit en cours de traitement).

commutation manuelle (MS, *manual switch*) concernant l'entité active: commute le sélecteur de l'entité active sur l'entité de protection (à moins qu'une requête de commutation de priorité plus élevée ne soit en cours de traitement).

commutation manuelle concernant l'entité de protection: commute le sélecteur de l'entité de protection sur l'entité active (à moins qu'une requête de commutation de priorité plus élevées ne soit en cours de traitement).

B.3.2 Commandes automatiques

Pour éviter les transitions intempestives, la transition condition active – condition inactive de panne de signal ne doit avoir lieu que si l'état AIS persiste pendant 5 secondes consécutives au moins.

B.3.3 Etats

L'état "attente avant rétablissement" n'est applicable qu'au mode réversible et s'applique à une entité active. La fonction commutation de protection locale passe à cet état lorsque le trafic actif est reçu via l'entité de protection et que les requêtes de commutation de protection précédemment actives sont devenues inactives. Il empêche le retour à la position initiale du sélecteur jusqu'à expiration de la temporisation "attente avant rétablissement". Cette temporisation peut être configurée par l'opérateur par pas de 1 minute entre 1 et 30 minutes, la valeur par défaut étant de 12 minutes.

La fonction commutation de protection locale passe à l'état "pas de requête" lorsque toutes les conditions où il n'y a pas de demande de commutation de protection locale (y compris l'état "attente avant rétablissement") active, il convient de noter qu'une telle situation peut se produire lorsque le sélecteur est activé où lorsqu'il est désactivé.

B.4 Protocole de commutation de protection

Dans le cas d'une architecture 1+1 unidirectionnelle, il n'existe a pas de protocole APS

B.5 Algorithme de commutation de protection unidirectionnelle 1+1

B.5.1 Commande du pont

Dans une architecture 1+1, le trafic actif est dirigé en permanence sur l'entité active et sur l'entité de protection.

B.5.2 Commande du sélecteur

Dans les architectures 1+1 en mode commutation de protection unidirectionnelle, le sélecteur est commandé par la demande locale de priorité la plus élevée (commande ou état déclenché automatiquement ou commande à déclenchement externe). Par conséquent, chaque extrémité fonctionne indépendamment de l'autre. S'il y a priorité égale sur les deux entités (par exemple SF, SD), la commutation ne sera pas exécutée.

B.5.3 Mode réversible

Dans ce mode, lorsque le trafic actif est reçu via l'entité de protection et que les demandes de commutation de protection locale précédemment actives sont devenues inactives, on passe à l'état local état "attente avant rétablissement".

La temporisation associée à cet état normalement expire et devient un état "pas de requête" après expiration de la temporisation état "attente avant rétablissement". Le temporisateur état "attente avant rétablissement" est désactivé plus tôt si une demande locale de priorité plus élevée préempte cet état.

B.5.4 Mode non réversible

Lorsque l'entité en panne ne se trouve plus dans une condition SD ou SF, et qu'il n'y a pas de commandes déclenchées extérieurement, on passe à l'état "pas de requête". Pendant cet état, il n'y a pas de commutation.

SERIES DES RECOMMANDATIONS UIT-T

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