Groupe de travail Réseau
Request for Comments : 5085
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

T. Nadeau, éditeur, Cisco Systems, Inc.
C. Pignataro, éditeur, Cisco Systems, Inc.
décembre 2007

Vérification de connexité de circuit virtuel (VCCV) pseudo filaire : un canal de contrôle pour les pseudo filaires

Résumé
Le présent document décrit la vérification de connexité de circuit virtuel (VCCV, *Virtual Circuit Connectivity Verification*) qui fournit un canal de contrôle associé à un pseudo-filaire (PW, *Pseudo-Wire*) ainsi que les opérations et fonctions de gestion correspondantes (comme la vérification de connexité) pour être utilisées sur ce canal de contrôle. VCCV s'applique à tous les types de circuit d'accès et de transport pris en charge actuellement définis pour les PW.

Table des Matières

1. Introduction

Il y a un besoin de mécanismes de détection de fautes et de diagnostic qui puissent être utilisés pour la détection de fautes de bout en bout et les diagnostics pour un pseudo-filaire, comme moyen pour déterminer l'état de fonctionnement réel du PW. Les opérateurs ont indiqué dans les [RFC4377] et [RFC3916] qu'un tel outil est nécessaire pour le fonctionnement et la maintenance de PW. Le présent document définit un protocole appelé vérification de connexité de circuit virtuel (VCCV, *Virtual Circuit Connectivity Verification*) qui satisfait à ces exigenes. VCCV est, dans sa plus simple description, un canal

de contrôle entre les points d'entrée et de sortie d'un pseudo-filaire sur lequel des messages de vérification de connexité peuvent être envoyés.

Le groupe de travail Émulation de pseudo filaire de bord à bord (PWE3) a défini un mécanisme qui émule les attributs essentiels d'un service de télécommunications (comme une liaison louée T1 ou un relais de trame) sur divers types de réseaux de commutation de paquets (PSN, *Packet Switched Network*) [RFC3985]. PWE3 est destiné à fournir seulement la fonction minimum nécessaire pour émuler le service avec le degré requis de confiance pour la définition du service en question. Les fonctions requises des PW incluent d'encapsuler des flux binaires, des cellules, ou des PDU spécifiques du service qui arrivent à un accès d'entrée et de les porter à travers un chemin IP ou un tunnel MPLS. Dans certains cas, il est nécessaire d'effectuer d'autres opérations, comme de gérer leur temporalité et leur ordre, d'émuler le comportement et les caractéristiques du service au degré de confiance requis.

Du point de vue des appareils côté consommateur (CE, *Customer Edge*) le PW est caractérisé comme une liaison ou circuit non partagé du service choisi. Dans certains cas, il peut y avoit des déficiences dans l'émulation de PW qui impactent le trafic porté sur un PW et donc limitent l'applicabilité de cette technologie. Ces limitations doivent être pleinement décrites dans les documents appropriés spécifiques du service.

Pour chaque type de service, il va y avoir un mode de fonctionnement par défaut que tous les PE qui offrent ce type de service doivent prendre en charge. Cependant, des modes facultatifs ont été définis pour améliorer la fiabilité du service émulé, ainsi que pour offrir un moyen pour que les plus anciennes mises en œuvre puissent prendre en charge ces services.

La Figure 1 décrit l'architecture d'un pseudo-filaire comme elle est définie dans la [RFC3985]. Elle décrit de plus où réside le canal de contrôle VCCV au sein de cette architecture, qui va être discutée plus loin en détails.

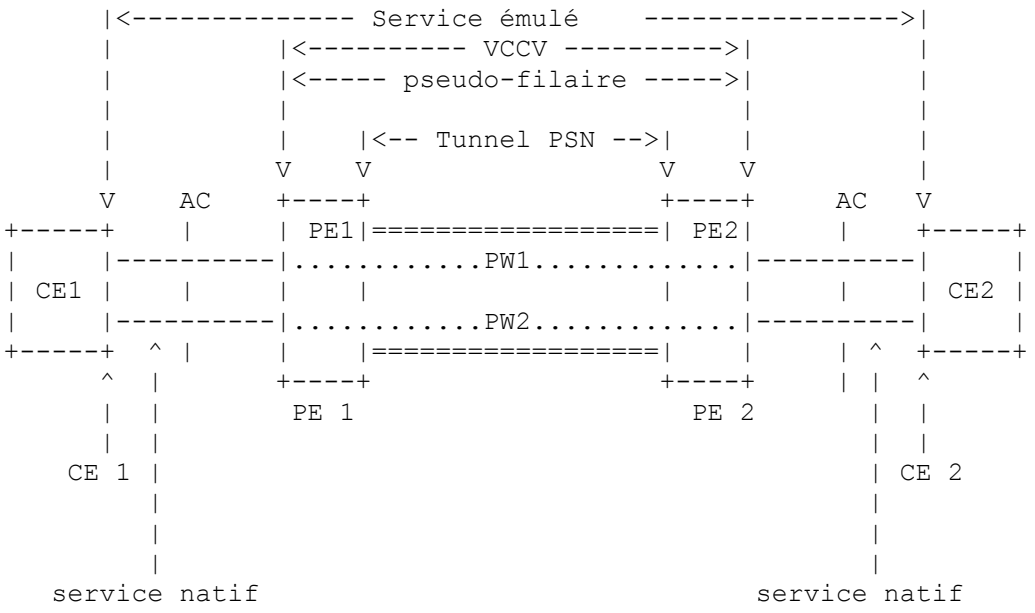


Figure 1 : Modèle de référence du fonctionnement de VCCV PWE3

D'après la Figure 1, les routeurs de côté consommateur (CE, *Customer Edge*) CE1 et CE2 sont rattachés au service émulé via des circuits de rattachement (AC, *Attachment Circuit*) et à chaque routeur de côté fournisseur (PE, *Provider Edge*) (respectivement PE1 et PE2). Un AC peut être un identifiant de connexion de liaison de données (DLCI, *Data Link Connection Identifier*) en relais de trame, un identifiant de chemin virtuel (VPI, *Virtual Path Identifier*) / identifiant de canal virtuel (VCI, *Virtual Channel Identifier*) ATM, un accès Ethernet, etc. Les appareils PE fournissent l'émulation de pseudo-filaire, permettant aux CE de communiquer sur le PSN. Un pseudo-filaire existe entre les PE qui traversent le réseau du fournisseur. VCCV fournit plusieurs moyens de créer un canal de contrôle sur le PW, entre les routeurs PE qui rattachent le PW.

La Figure 2 décrit comment le canal de contrôle VCCV est associé à la pile de protocoles de pseudo-filaire.

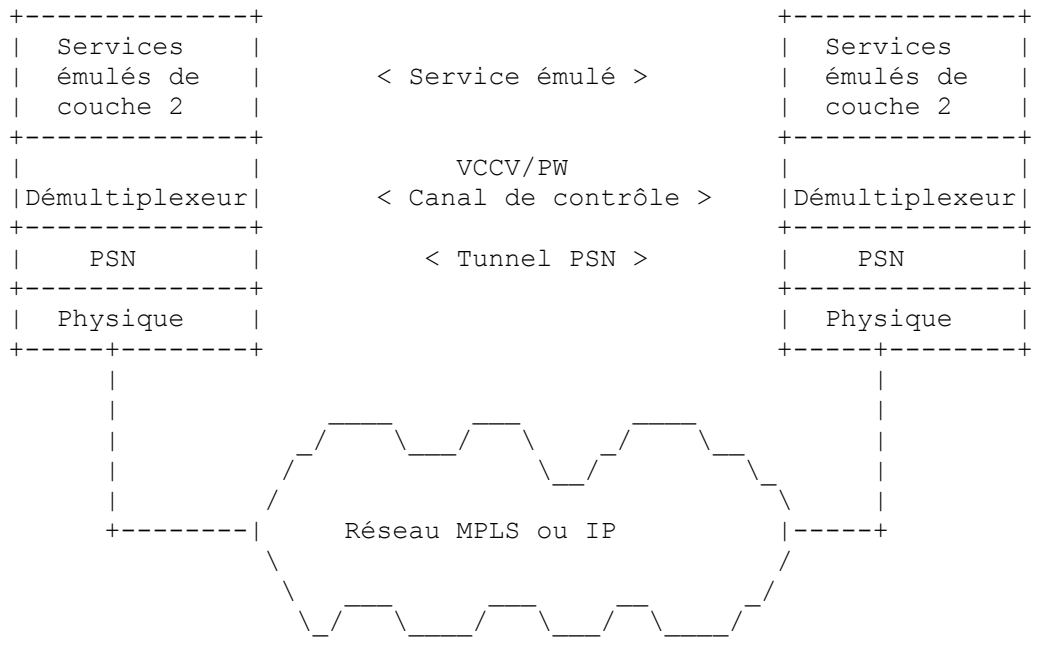


Figure 2 : Modèle de référence de pile de protocole PWE3 incluant le canal de contrôle VCCV

Les messages VCCV sont encapsulés en utilisant l'encapsulation PWE3 comme décrit dans les Sections 5 et 6, de sorte qu'ils sont traités de la même manière (ou dans certains cas, de manière similaire) que les PDU de PW pour lesquelles ils fournissent un canal de contrôle. Ces messages VCCV sont échangés seulement après la capacité (exprimée comme deux espaces de type VCCV, à savoir les types VCCV Canal de contrôle et Vérification de connexité) et que le désir d'échanger un tel trafic a été annoncé entre les PE (voir aux paragraphes 5.3 et 6.3) et que les types de VCCV sont choisis.

1.1 Spécification des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Abréviations

AC *(Attachment Circuit)* circuit de rattachement [RFC3985].
AVP *(Attribute Value Pair)* paire attribut/valeur [RFC3931].
CC *(Control Channel)* canal de contrôle (utilisé comme type de CC).
CE *(Customer Edge)* côté consommateur.
CV *(Connectivity Verification)* vérification de connexité (utilisé comme type de CV).
CW *(Control Word)* mot de contrôle [RFC3985].
FEC *(Forwarding Equivalence Class)* classe d'équivalence d'acheminement
L2SS *(L2-Specific Sublayer)* sous couche spécifique de couche 2 [RFC3931].
LCCE *(L2TP Control Connection Endpoint)* point d'extrémité de connexion de contrôle L2TP [RFC3931].
OAM *(Operation and Maintenance)* fonctionnement et maintenance.
PE *(Provider Edge)* côté fournisseur.
PSN *(Packet Switched Network)* réseau de commutation de paquets [RFC3985].
PW *(Pseudowire)* pseudo-filaire [RFC3985].
PW-ACH *(PW Associated Channel Header)* en-tête de canal associé au PW [RFC4385].
VCCV *(Virtual Circuit Connectivity Verification)* vérification de connexité de circuit virtuel.

3. Vue d'ensemble de VCCV

Le but de VCCV est de vérifier et diagnostiquer le chemin de transmission de pseudo-filaire. À cette fin, VCCV est constitué de différents composants :
o un moyen de signaler les capacités VCCV à un PE homologue,

- une encapsulation pour les messages de canal de contrôle VCCV qui permet au PE receveur de les intercepter, les interpréter, et les traiter en local comme des messages d'OAM, et
- des spécifications pour le fonctionnement des divers modes de fonctionnement VCCV transmis au sein des messages VCCV.

Quand un pseudo-filaire est signalé pour la première fois en utilisant le protocole de distibution d'étiquettes (LDP, *Label Distribution Protocol*) [RFC4447] ou la version 3 du protocole de tunnelage de couche deux (L2TPv3, *Layer Two Tunneling Protocol version 3*) [RFC3931], un message est envoyé du PE initiateur au PE receveur, demandant qu'un pseudo-filaire soit établi. Ce message a été étendu pour inclure des informations de capacité VCCV (voir la Section 4). Les informations de capacité VCCV indiquent au PE receveur quelles combinaisons de types de canal de contrôle (CC) et de vérification de connexité (CV) il est capable de recevoir. Si le PE receveur accepte d'établir le PW, il va retourner ses capacités dans le message de signalisation suivant pour indiquer quels types de CC et CV il est capable de traiter. Les règles de préséance pour quel type de CC et CV choisir dans les cas où plus d'un est spécifié dans ce message sont définis à la Section 7 du présent document.

Une fois que le PW est signalé, les données pour le PW vont s'écouler entre les PE qui terminent le PW. À ce moment, les PE peuvent commencer à transmettre les messages VCCV sur la base des combinaisons de type de CC et CV discutées. À cette fin, VCCV définit une encapsulation pour ces messages qui les identifie comme appartenant au canal de contrôle pour le PW. Cette encapsulation est conçue pour permettre au canal de contrôle d'être traité fonctionnellement de la même manière que les données de trafic pour le PW afin de vérifier de façon fiable le plan des données pour le PE, et permettre au PE d'intercepter et traiter ces messages VCCV au lieu de les transmettre hors de l'AC vers le CE comme si c'était du trafic de données. De cette façon, la fonction de base du canal de contrôle VCCV est de vérifier la connexité du pseudo-filaire et du plan des données utilisé pour transporter les données de chemin pour le pseudo-filaire. On devrait noter que à cause du nombre de combinaisons d'encapsulations de plan des données facultatives et obligatoires pour le trafic de données de PW, VCCV définit un certain nombre de types de canal de contrôle (CC) et de vérification de connexité (CV) afin d'en prendre en charge autant que possible. Bien que conçu pour prendre en charge la plupart des combinaisons existantes (obligatoires et facultatives) VCCV ne définit pas de combinaison par défaut de type de CC et CV pour chaque type de démultiplexeur de PW, comme il va être décrit en détail plus loin dans le présent document.

VCCV peut être utilisé à la fois comme outil de détection de fautes et/ou de diagnostic pour les pseudo-filaires. Par exemple, un opérateur peut périodiquement invoquer VCCV de façon régulière, pour une vérification de connexité proactive sur un pseudo-filaire actif, ou de façon ad hoc ou comme nécessaire comme moyen de vérification manuelle de connexité. Quand il invoque VCCV, l'opérateur déclenche une combinaison d'un de ses divers types de CC et d'un de ses divers types de CV. Les types de CV incluent le ping de LSP [RFC4379] pour les PW MPLS, et le ping ICMP [RFC0792], [RFC4443] pour les PW MPLS et L2TPv3. On définit une matrice de combinaisons acceptables de type de CC et de CV plus loin dans cette spécification.

Le canal de contrôle tenu par VCCV peut également porter l'état de détection de fautes entre les points d'extrémité du pseudo-filaire. De plus, ces informations peuvent alors être traduites en les codes d'état d'OAM natif utilisé par les technologies d'accès natives, comme ATM, relais de trame ou Ethernet. Les détails spécifiques de cet inter-fonctionnement d'état sortent du domaine d'application du présent document, et sont seulement notés ici pour illustrer l'utilité de VCCV pour de tels objets. Les détails complets se trouvent dans [MSG-MAP] et la [RFC4447].

4. Types de CC et de CV

Le type de canal de contrôle VCCV définit plusieurs types possibles de canal de contrôle que VCCV peut prendre en charge. Ces canaux de contrôle peuvent à leur tour porter plusieurs types de protocoles définis par le type de vérification de connexité (CV). VCCV prend potentiellement en charge plusieurs types de CV concurremment, mais il prend seulement en charge l'utilisation d'un seul type de CC. Le ou les types spécifiques de paquets VCCV qui peuvent être acceptés et envoyés par un routeur sont indiqués durant l'annonce de capacités comme décrit aux paragraphes 5.3 et 6.3. Les divers types de CV VCCV pris en charge sont utilisés seulement quand ils s'appliquent au contexte du démultiplexeur de PW utilisé. Par exemple, le type de CV ping LSP devrait seulement être utilisé quand des étiquettes MPLS sont utilisées comme démultiplexeur de PW.

Une fois qu'un ensemble de capacités VCCV est reçu et annoncé, un ou des types de CC et CV qui correspondent à la fois aux capacités reçues et transmises peuvent être choisis. C'est-à-dire qu'un routeur PE a seulement besoin de permettre les types qui sont à la fois reçus et annoncés pour être choisis, en effectuant un ET logique entre les champs de fanions binaires reçus et transmis. Le ou les types spécifiques de CC et CV sont alors choisis au sein des contraintes et règles spécifiées à la Section 7. Une fois qu'un type spécifique de CC a été choisi (c'est-à-dire, il correspond aux capacités de CC VCCV transmises et reçues) et transmis, et qu'il a reçu une réponse, ce type de CC DOIT être le seul utilisé jusqu'au moment où le

pseudo-filaire est re-signalé. De plus, sur la base de ces règles et des procédures définies au paragaphe 5.2 de la [RFC4447], le pseudo-filaire DOIT être re-signalé si un ensemble différent de types de capacités est désiré. La portion pertinente du paragraphe 5.2 de la [RFC4447] est : Sous TLV Paramètre d'interface.

Noter que le "sous TLV Paramètre d'interface" fait partie de la classe d'équivalence de transmission (FEC, *Forwarding Equivalence Class*) et les règles de LDP rendent impossible de changer les paramètres d'interface une fois que le pseudo-filaire a été établi.

Les champs d'indicateur de type de CC et CV sont définis comme des gabarits binaires de 8 bits utilisés pour indiquer le ou les types spécifiques de CC ou CV (c'est-à-dire, aucun, un, ou plusieurs) des paquets de canal de contrôle qui peuvent être envoyés sur le canal de contrôle VCCV. Ces valeurs représentent la valeur numérique correspondant au bit réel établi dans le champ binaire. La définition de chaque type de CC et CV dépend du contexte du type de PW, MPLS ou L2TPv3, au sein duquel il est défini.

Types de canal de contrôle (CC) :
Les valeurs définies pour les types de CC pour les PW MPLS sont : Types de canal de contrôle MPLS.

Bit (valeur)	**Description**
Bit 0 (0x01)	Type 1 : Mot de contrôle PWE3 0001b comme premier quartet (PW-ACH, voir la [RFC4385])
Bit 1 (0x02)	Type 2 : Étiquette d'alerte de routeur MPLS
Bit 2 (0x04)	Type 3 : Étiquette de PW MPLS avec TTL == 1
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé
Bit 6 (0x40)	Réservé
Bit 7 (0x80)	Réservé

Les valeurs définies pour les types de CC pour les PW L2TPv3 sont : Types de canal de contrôle L2TPv3.

Bit (valeur)	**Description**
Bit 0 (0x01)	Sous couche spécifique de couche 2 avec le bitV établi
Bit 1 (0x02)	Réservé
Bit 2 (0x04)	Réservé
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé
Bit 6 (0x40)	Réservé
Bit 7 (0x80)	Réservé

Types de vérification de connexité : les valeurs définies pour les types de CV pour les PW MPLS sont :

Types de vérification de connexité MPLS :

Bit (valeur)	**Description**
Bit 0 (0x01)	Ping ICMP
Bit 1 (0x02)	Ping LSP
Bit 2 (0x04)	Réservé
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé
Bit 6 (0x40)	Réservé
Bit 7 (0x80)	Réservé

Les valeurs définies pour les types de CV pour les PW L2TPv3 sont : Types de vérification de connexité L2TPv3.

Bit (valeur)	**Description**
Bit 0 (0x01)	Ping ICMP
Bit 1 (0x02)	Réservé
Bit 2 (0x04)	Réservé
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé

Bit 6 (0x40) Réservé
Bit 7 (0x80) Réservé

Si aucun des types ci-dessus n'est pris en charge, les champs entiers de type de CC et CV DEVRAIENT être transmis à 0x00 (c'est-à-dire, tous les bits dans le champ binaire sont réglés à 0) pour l'indiquer à l'homologue.

Si aucune capacité n'est signalée, l'homologue DOIT alors supposer que l'homologue n'a pas de capacité VCCV et suivre les procédures spécifiées dans le présent document pour ce cas.

5. Canal de contrôle VCCV pour PW MPLS

Quand MPLS est utilisé pour transporter des paquets de PW, les paquets VCCV sont portés sur le LSP MPLS, comme défini dans cette Section. Afin d'appliquer les outils de surveillance IP à un PW, un opérateur peut configurer VCCV comme un canal de contrôle pour le PW entre les points d'extrémité du PE [RFC3985]. Les paquets envoyés à travers ce canal du PE de source vers le PE de destination soit comme du trafic dans la bande avec les données de PW, soit hors bande. Dans tous les cas, le trafic du canal de contrôle n'est pas transmis après les points d'extrémité de PE vers les appareils du côté consommateur (CE) ; les messages VCCV sont plutôt interceptés aux points d'extrémité de PE pour un traitement exceptionnel.

5.1 Types de canaux de contrôle VCCV pour MPLS

Comme déjà décrit à la Section 4, la capacité de quels types de canal de contrôle sont pris en charge est annoncée par un PE. Une fois que le PE receveur a choisi un mode de type de CC à utiliser, il DOIT continuer en utilisant ce mode jusqu'au moment où le PW est re-signalé. Donc, si un nouveau type de CC est désiré, le PW doit être supprimé et rétabli.

Idéalement, un tel canal de contrôle va être complètement dans la bande (c'est-à-dire, suivant la même fiabilité de plan des données que les données de PW). Quand un mot de contrôle est présent sur le PW, il est possible d'indiquer le canal de contrôle en établissant un bit dans l'en-tête du mot de contrôle (voir le paragraphe 5.1.1).

Les paragraphes 5.1.1 à 5.1.3 décrivent chacun des types de canal de contrôle VCCV actuellement définis.

5.1.1 VCCV dans la bande (Type 1)

Le type de CC 1 est aussi appelé "mot de contrôle PWE3 avec 0001b comme premier quartet". Il utilise l'en-tête de canal associé de PW (PW-ACH, *PW Associated Channel Header*) ; voir la Section 5 de la [RFC4385].

Le protocole d'établissement de PW [RFC4447] détermine si un PW utilise un mot de contrôle. Quand un mot de contrôle est utilisé, et que le CW utilise le format de "mot de contrôle générique de PW MPLS" (voir la Section 3 de la [RFC4385]), un canal de contrôle à l'usage des messages VCCV peut être créé en utilisant le format de CW de canal associé de PW (voir la Section 5 de la [RFC4385]).

Le canal associé au PW pour le trafic de canal de contrôle VCCV est défini dans la [RFC4385] comme montré à la Figure 3:

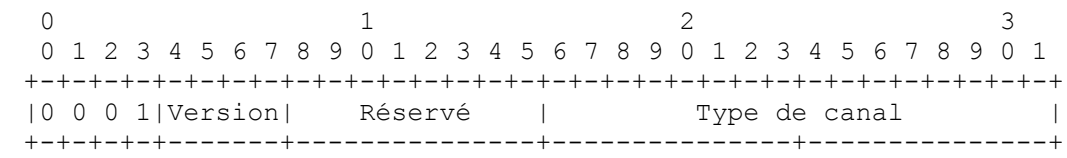


Figure 3 : En-tête de canal associé au PW

Le premier quartet est réglé à 0001b pour indiquer un canal associé à un pseudo-filaire (voir la Section 5 de la [RFC4385] et le paragraphe 3.6 de la [RFC4446]). Les champs Version et Réservé sont réglés à 0, et le type de canal est réglé à 0x0021 pour les charges utiles IPv4 et à 0x0057 pour les charges utiles IPv6.

Par exemple, la Figure 4 montre comment serait reçu le PW-ACH Ethernet [RFC4448] contenant une charge utile de ping LSP correspondant à un choix de type de CC de 0x01 et de type de CV de 0x02 :

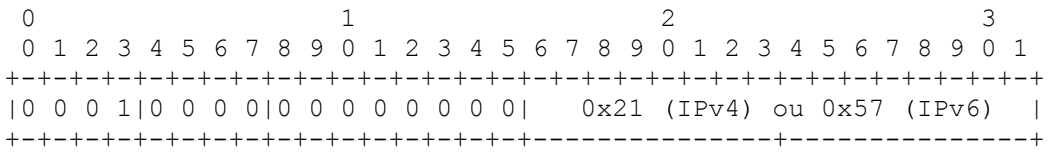


Figure 4 : En-tête de canal associé au PW pour VCCV

On devrait noter que bien que certains types de PW ne soient pas obligés de porter de mot de contrôle, ce type de VCCV peut seulement être utilisé pour les types de PW qui emploient bien un mot de contrôle quand il est en usage. De plus, ce type de CC peut seulement être utilisé si le CW PW suit le format de "mot de contrôle générique de PW MPLS". Ce mode de fontionnement de VCCV DOIT être pris en charge quand le mot de contrôle est présent.

5.1.2 VCCV hors bande (Type 2)

Le type de CC 2 est aussi appelé une "étiquette d'alerte de routeur MPLS".

Un canal de contrôle VCCV peut aussi être créé en utilisant l'étiquette d'alerte de routeur MPLS [RFC3032] immédiatement au dessus de l'étiquette de PW. On devrait noter que cette approche pourrait résulter en un comportement de hachage de chemins multiples de coût égal (ECMP, *Equal Cost Multi-Path*) différent de celui des PDU de pseudo-filaire, et donc résulte en ce que le trafic de canal de contrôle VCCV prenne un chemin qui diffère de celui du trafic réel de données soumis à l'essai. Voir la Section 2 de la [RFC4928].

Le type de CC 2 peut être utilisé que le PW soit établi ou non avec un mot de contrôle présent.

C'est le mode préféré de fonctionnement de VCCV quand le mot de contrôle est absent.

Si le mot de contrôle est utilisé sur ce PW, il DOIT aussi être inclus avant le message VCCV. C'est pour éviter des comportements différents de hachage d'ECMP. Dans ce cas, le CW utilise le format PW-ACH décrit au paragraphe 5.1.1 (voir les Figures 3 et 4). Si le mot de contrôle n'est pas utilisé sur ce PW, le message VCCV suit directement l'étiquette de PW.

5.1.3 Expiration de TTL de VCCV (Type 3)

Le type de CC 3 est aussi appelé une "étiquette de PW MPLS avec TTL == 1".

Le TTL de l'étiquette de PW peut être réglé à 1 pour forcer le paquet à être traité au sein du plan de contrôle du routeur de destination. Cette approche pourrait aussi résulter en un comportement différent de hachage ECMP et en ce que les messages VCCV prennent un chemin différent de celui du trafic de données de PW.

Le type de CC 3 peut être utilisé que le PW soit établi ou non avec un mot de contrôle présent.

Si le mot de contrôle est utilisé sur ce PW, il DOIT aussi être inclus avant le message VCCV. Ceci est pour éviter un comportement différent de hachage ECMP. Dans ce cas, le CW utilise le format de PW-ACH décrit au paragraphe 5.1.1 (voir les Figures 3 et 4). Si le mot de contrôle n'est pas utilisé sur ce PW, le message VCCV suit directement l'étiquette de PW.

5.2 Types de vérification de connexité de VCCV pour MPLS

5.2.1 Ping ICMP

Quand ce mode facultatif de vérification de connexité est utilisé, un paquet Écho ICMP utilisant le codage spécifié dans la [RFC0792] (ICMPv4) ou dans la [RFC4443] (ICMPv6) réalise la vérification de connexité. Les mises en œuvre DOIVENT utiliser ICMPv4 [RFC0792] si la signalisation pour VCCV utilise des adresses IPv4, ou ICMPv6 [RFC4443] si des adresses IPv6 sont utilisées. Si le pseudo-filaire est établi statiquement, le codage DOIT alors utiliser ce qui a été utilisé pour le pseudo-filaire dans la configuration.

5.2.2 Ping de LSP MPLS

L'en-tête de ping LSP DOIT être utilisé en accord avec la [RFC4379] et DOIT aussi contenir la pile de FEC cible contenant le sous-TLV de sous-type 8 pour le "point d'extrémité de VPN de couche 2", 9 pour le "pseudo-filaire de FEC 128

(déconseillé)", 10 pour le "pseudo-filaire de FEC 128", ou 11 pour le "pseudo-filaire de FEC 129". La valeur du sous-TLV indique le PW à vérifier.

5.3 Annonce de capacité de VCCV pour les PW MPLS

Pour permettre l'indication du ou des types de mode de canal de contrôle et de vérification de connexité de PW sur un PW particulier, un paramètre VCCV est défini au paragraphe 5.3.1 qui est utilisé au titre de la signalisation d'établissement de PW. Quand un PE signale un PW et désire l'OAM de PW pour ce PW, il DOIT l'indiquer durant l'établissement du PW en utilisant les messages définis au paragraphe 5.3.1. Spécifiquement, le PE DOIT inclure le sous-TLV Paramètre d'interface VCCV (0x0C) alloué dans la [RFC4446] dans le message d'établissement du PW [RFC4447].

La décision du type de canal de contrôle VCCV est laissée complètement à l'entité de contrôle receveuse, bien que l'ensemble des choix soit donné par l'envoyeur en ce qu'il indique le ou les types de canaux de contrôle et de vérification de connexité qu'il peut comprendre. Le receveur DEVRAIT choisir un seul type de canal de contrôle dans les choix envoyés et reçus correspondants, sur la base de la sélection d'annonces de capacité spécifiée à la Section 7, et il DOIT continuer d'utiliser ce type pour la durée de la vie du canal de contrôle. Changer les types de canal de contrôle après qu'il en a été établi un pour être utilisé pourrait causer des problèmes potentiels à l'extrémité receveuse et pourrait aussi comduire à des problèmes d'interopérabilité ; donc, ce n'est PAS RECOMMANDÉ.

Quand un PE envoie un message de transposition d'étiquette pour un PW, il utilise le paramètre VCCV pour indiquer le ou les types de canaux de contrôle et de vérification de connexité OAM qu'il veut recevoir et peut envoyer sur ce PW. Un PE distant NE DOIT PAS envoyer de messages VCCV avant que soit signalée la capacité de prendre en charge le type de canal de contrôle (et le ou les types de vérification de connexité à utiliser sur eux). Ensuite, il peut le faire seulement sur un canal de contrôle et en utilisant le ou les types de vérification de connexité à partir de ceux indiqués.

Si un PE reçoit des messages VCCV avant l'annonce de capacité pour ce message, il DOIT éliminer ces messages et ne pas y répondre. Dans ce cas, le PE DEVRAIT incrémenter un compteur d'erreurs et facultativement produire une notification au système et/ou SNMP pour indiquer à l'administrateur du système que cette condition existe.

Quand LDP est utilisé comme protocole de signalisation de PW, le PE demandeur indique sa ou ses capacités VCCV configurées au PE distant en incluant le paramètre VCCV avec les options appropriées dans le champ Sous-TLV Paramètre d'interface VCCV du TLV FEC d'ID de PW (FEC 128) ou dans le sous-TLV paramètre d'interface du TLV FEC d'ID de PW généralisé (FEC 129). Ces options indiquent quels types de canal de contrôle et de vérification de connexité il prend en charge. Le PE demandeur PEUT indiquer qu'il prend en charge plusieurs options de canal de contrôle, et en le faisant, il accepte de prendre en charge tous les types indiqués qui lui sont transmis. Cependant, il DOIT faire cela en accord avec les règles stipulées au paragraphe 5.3.1 (sous-TLV Annonce de capacité VCCV.)

La politique locale peut conduire le PE à prendre en charge une certaine capacité OAM et à l'indiquer. L'absence du paramètre VCCV indique qu'aucune fonction OAM n'est prise en charge par le PE demandeur, et donc le PE receveur NE DOIT PAS lui envoyer de trafic de canal de contrôle VCCV. La réception d'un paramètre VCCV sans ensemble d'options DOIT être ignorée comme si aucune n'était transmise.

Le PE receveur indique de même ses types de canal de contrôle pris en charge dans le message de transposition d'étiquette. Ils peuvent ou non être les mêmes que ceux qui lui ont été envoyés. L'envoyeur devrait examiner l'ensemble qui est retourné pour comprendre quels canaux de contrôle il peut établir avec l'homologue distant, comme spécifié dans les Sections 4 et 7. De même, il NE DOIT PAS envoyer de trafic de canal de contrôle au PE distant pour lequel le PE distant n'a pas indiqué qu'il le prend en charge.

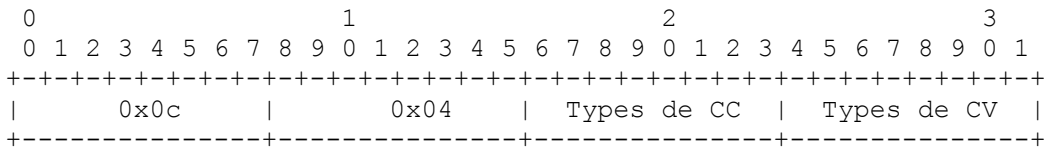
5.3.1 Sous TLV Annonce de capacité VCCV LDP

La [RFC4447] définit un champ Sous-TLV Paramètre d'interface dans la FEC ID de PW LDP (FEC 128) et un TLV Paramètres d'interface dans la FEC ID de PW LDP généralisé (FEC 129) pour signaler les différentes capacités pour des PW spécifiques. Un paramètre sous-TLV facultatif est défini pour indiquer la capacité de prendre en charge aucun, un, ou plusieurs types de canal de contrôle et de vérification de connexité pour VCCV. C'est le champ Paramètre VCCV. Si la FEC 128 est utilisée, le champ Paramètre VCCV est porté dans le champ Sous-TLV Paramètre d'interface. Si la FEC 129 est utilisée, il est porté comme sous-TLV Paramètre d'interface dans le TLV Paramètres d'interface.

L'identifiant de paramètre VCCV est défini comme suit dans la [RFC4446] :

Identifiant de paramètre	Longueur	Description
0x0c	4	VCCV

Le format du champ Paramètre VCCV est comme suit :



Le champ type de CC définit un gabarit binaire utilisé pour indiquer le ou les types de canal de contrôle (c'est-à-dire, aucun, un, ou plusieurs) sur lesquels un routeur est capable de recevoir le trafic de canal de contrôle. Si plus d'un canal de contrôle est spécifié, le routeur accepte le trafic de contrôle sur l'un ou l'autre ; cependant, voir les règles spécifiées aux Sections 4 et 7 pour plus de détails. Si aucun des types n'est pris en charge, un type d'indicateur de CC de 0x00 DEVRAIT être transmis pour l'indiquer à l'homologue. Cependant, si aucune capacité n'est signalée, le PE DOIT alors supposer que son homologue est incapable de recevoir tout type de CC VCCV et NE DOIT PAS lui envoyer de trafic OAM de canal de contrôle. Noter que les définitions de type de CC et CV sont cohérentes sans considération du type de transport ou de circuit d'accès du PW. Les valeurs de type de CC et CV sont définies à la Section 4.

6. Canal de contrôle VCCV pour PW L2TPv3/IP

Quand L2TPv3 est utilisé pour établir un PW sur un PSN IP, les paquets VCCV sont portés sur la session L2TPv3 comme défini dans cette section. L2TPv3 fournit un mécanisme "Hello" de maintien en vie pour le plan de contrôle L2TPv3 qui fonctionne dans la bande sur IP ou UDP (voir le paragraphe 4.4 de la [RFC3931]). Cette facilité de Hello incorporée ne fournit la détection de l'homologue et du chemin morts que pour le groupe de sessions associé à la connexion de contrôle L2TP. VCCV permet cependant aux sessions L2TP individuelles d'être vérifiées. Cela fournit un mécanisme d'une granularité plus fine qui peut être utilisé pour corriger de potentiels problèmes au sein du plan des données des points d'extrémité L2TP eux-mêmes, ou pour fournir de l'état de connexion supplémentaire des pseudo-filaires individuels.

La capacité de quel type de canal de contrôle utiliser est annoncée par un PE pour indiquer lesquels de divers types potentiels de canal de contrôle sont pris en charge. Une fois que le PE receveur a choisi un mode à utiliser, il DOIT continuer d'utiliser ce mode jusqu'au moment où le PW est re-signalé. Donc, si un nouveau type de CC est désiré, le PW doit être supprimé et rétabli.

Un LCCE envoie des messages VCCV sur un pseudo-filaire signalé par L2TPv3 pour la détection de fautes et le diagnostic de la session L2TPv3. Le message VCCV voyage dans la bande avec la session et suit exactement le même chemin que les données d'utilisateur pour la session, parce que l'en-tête IP et l'en-tête de session L2TPv3 sont identiques. Le LCCE de sortie de la session L2TPv3 intercepte et traite le message VCCV, et vérifie la signalisation et l'état de transmission du pseudo-filaire à réception du message VCCV. On notera que le mécanisme VCCV pour L2TPv3 est principalement ciblé sur la vérification de l'état de signalisation et de transmission du pseudo-filaire au LCCE de sortie. Il aide aussi quand les chemins de connexion de contrôle L2TPv3 et de session ne sont pas identiques.

6.1 Type de canal de contrôle VCCV pour L2TPv3

Afin de porter les messages VCCV au sein d'un paquet de données de session L2TPv3, le PW DOIT être établi de façon à ce qu'une sous-couche spécifique de couche 2 (L2SS, *L2-Specific Sublayer*) qui définit le bit V soit présente. Le présent document définit le bit V pour la sous couche spécifique de couche 2 par défaut [RFC3931] et la sous couche spécifique de ATM [RFC4454] en utilisant la position de bit 0 (voir les paragraphes 8.3.2 et 8.3.3). La présence de la sous couche spécifique de couche 2 et du type (défaut ou L2SS spécifique du PW) est signalée via l'AVP Sous-couche spécifique de couche, type d'attribut 69, comme défini dans la [RFC3931]. Le bit V au sein de la L2SS est utilisé pour identifier qu'un message VCCV suit, et quand le bit V est établi, la L2SS a le format montré à la Figure 5:

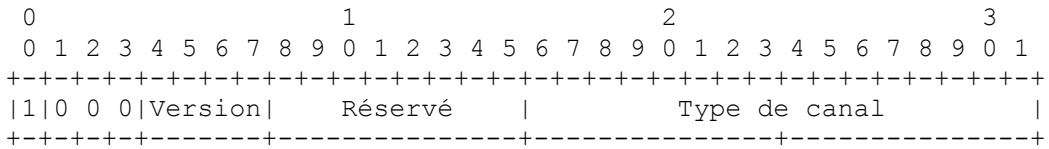


Figure 5 : Format de sous couche spécifique de couche 2 quand le bit V (bit 0) est établi

Les messages VCCV sont distingués des données d'utilisateur par le bit V. Le bit V est établi à 1, pour indiquer qu'un message de session VCCV suit. Les trois bits suivants DOIVENT être réglés à 0 à l'envoi et ignorés à réception. Les champs restants comportent 28 bits (c'est-à-dire, Version, Réservé, et Type de canal) et suivent la même définition, format, et numéro de registre qu'à la Section 5 de la [RFC4385].

Les champs Version et Réservé sont réglés à 0. Pour le type de CV actuellement défini de ping ICMP (0x01) le type de canal peut indique IPv4 (0x0021) ou IPv6 (0x0057) (voir la [RFC4385]) comme charge utile VCCV suivant directement le L2SS.

6.2 Type de vérification de connexité de VCCV pour L2TPv3

Le message VCCV sur L2TPv3 suit directement la sous couche spécifique de L2 avec le bit V établi. Il DOIT contenir un paquet Écho ICMP comme décrit au paragraphe 6.2.1.

6.2.1 VCCV L2TPv3 utilisant le Ping ICMP

Quand ce mode de vérification de connexité est utilisé, un paquet Écho ICMP utilisant le codage spécifié dans la [RFC0792] pour (ICMPv4) ou dans la [RFC4443] (pour ICMPv6) réalise la vérification de connexité. Les mises en œuvre DOIVENT utiliser ICMPv4 [RFC0792] si la signalisation pour le PW L2TPv3 utilise des adresses IPv4, ou ICMPv6 [RFC4443] si des adresses IPv6 sont utilisées. Si le pseudo-filaire est établi de façon statique, le codage DOIT alors utiliser celui qui a été utilisé pour le pseudo-filaire dans la configuration.

Le paquet Ping ICMP suit directement le L2SS avec le bit V établi. Dans la demande d'écho ICMP, les champs d'en-tête IP DOIVENT avoir les valeurs suivantes : l'adresse IP de destination est réglée à l'adresse IP du LCCE distant pour le point d'extrémité de tunnel, l'adresse de source IP est réglée à l'adresse IP du LCCE local pour le point d'extrémité de tunnel, et le TTL ou limite de bonds est réglé à 1.

6.3 Annonce de capacité de VCCV L2TPv3 pour L2TPv3

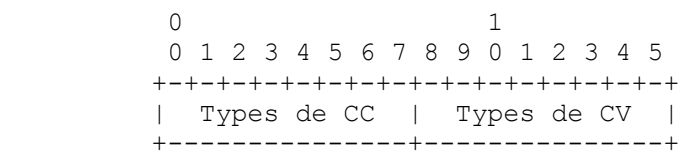
Une nouvelle AVP facultative VP est définie au paragraphe 6.3.1 pour indiquer les capacités VCCV durant l'établissement de session. Un LCCE DOIT signaler son désir d'utiliser la vérification de connexité pour une session L2TPv3 particulière et ses capacités VCCV en utilisant l'AVP Capacité de VCCV.

Un LCCE NE DOIT PAS envoyer de paquets VCCV sur une session L2TPv3 sauf si il a reçu de l'extrémité distante la capacité VCCV au moyen de l'AVP Capacité de VCCV. Si un LCCE reçoit des paquets VCCV et qu'il n'a pas la capacité VCCV ou si il n'a pas envoyé d'indication de capacité à l'extrémité distante, il DOIT éliminer ces messages. Il devrait aussi incrémenter un compteur d'erreurs. Dans ce cas le LCCE PEUT facultativement produire une notification au système et/ou à SNMP.

6.3.1 AVP Capacité de VCCV L2TPv3

Le type 96 d'attribut "AVC de capacité VCCV", spécifie les capacités VCCV comme une paire de fanions binaires pour les types de canal de contrôle (CC) et vérification de connexité (CV). Cette AVP est échangée durant l'établissement de session (dans les messages ICRQ (demande d'appel entrant), ICRP (réponse d'appel entrant), OCRQ (demande d'appel sortant), ou OCRP (réponse d'appel sortant)). Le champ Valeur a le format suivant :

AVP Capacité VCCV (ICRQ, ICRP, OCRQ, OCRP)



Types de CC : le champ Types de CC définit un gabarit binaire utilisé pour indiquer le ou les types des canaux de contrôle qui peuvent être utilisés pour recevoir le trafic d'OAM sur la session concernée. Le routeur accepte le trafic VCCV à tout moment sur tous les types de canal de contrôle VCCV signalés. Les valeurs de type de CC sont définies à la Section 4. Bien qu'il y ait seulement une valeur définie dans le présent document, le champ Types de CC est inclus pour la rétro compatibilité si d'autres types de CC devaient être définis à l'avenir. Un type de CC de 0x01 peut seulement être demandé quand il y a une sous couche spécifique de couche 2 qui définit le bit V comme présent. Si un type de CC de

0x01 est demandé sans demander une AVP Sous couche spécifique de couche 2 avec un type de L2SS qui définit le bit V, la session DOIT être déconnectée avec un message Notification d'appel déconnecté (CDN, *Call-Disconnect-Notify*). Si aucun type de CC n'est pris en charge, un indicateur de type de CC de 0x00 DEVRAIT être envoyé.

Types de CV : le champ Types de vérification de connexité (CV) définit un gabarit binaire utilisé pour indiquer le ou les types spécifiques (c'est-à-dire, aucun, un, ou plusieurs) des paquets de contrôle qui peuvent être envoyés sur le canal de contrôle VCCV spécifié. Les valeurs de type de CV sont définies à la Section 4. Si aucune AVP Capacité VCCV n'est signalée, le LCCE DOIT alors supposer que l'homologue est incapable de recevoir VCCV et NE DOIT PAS lui envoyer de trafic OAM de canal de contrôle.

Toutes les AVP L2TP ont un bit M (obligatoire) un bit H (caché) une Longueur, et un Identifiant de fabricant. L'identifiant de fabricant pour l'AVP Capacité de VCCV DOIT être 0, indiquant que c'est une AVP définie par l'IETF. Cette AVP PEUT être cachée (le bit H PEUT être 0 ou 1). Le bit M pour cette AVP DEVRAIT être réglé à 0. La Longueur (avant de cacher) de cette AVP est 8.

7. Choix d'annonce de capacité

Quand un PE reçoit une annonce de capacité VCCV, l'annonce peut contenir plus d'un type de CC ou CV. Seules des capacités correspondantes peuvent être choisies. Quand plusieurs capacités correspondent, seul un type de CC DOIT être utilisé.

En particulier, comme déjà spécifié, une fois qu'un type de CC valide est utilisé par un PE (trafic envoyé en utilisant cette encapsulation) le PE NE DOIT PAS envoyer de trafic sur un autre type de CC de canal de contrôle.

Pour les cas où plusieurs types de CC sont annoncés, les régles de préséance suivantes s'appliquent lors du choix du seul type de CC à utiliser :
1. Type 1 : mot de contrôle PWE3 avec 0001b comme premier quartet
2. Type 2 : étiquette d'alerte de routeur MPLS
3. Type 3 : étiquette de PW MPLS avec TTL == 1

Pour les PW MPLS, le type de CV ping LSP (0x02) est le type par défaut, et le type de CV ping ICMP (0x01) est facultatif.

8. Considérations relatives à l'IANA

8.1 Sous TLV Interface de VCCV

Le codet de sous TLV Paramètres d'interface VCCV est défini dans la [RFC4446]. L'IANA a créé et va tenir des registres pour les types de CC et de CV (gabarits binaires dans l'identifiant de paramètre VCCV). Les nouveaux registres de type de CC et de type de CV (voir respectivement les paragraphes 8.1.1 et 8.1.2) ont été créés dans les espaces de noms de pseudo-filaires, accessibles dans [IANA.pwe3]. Les allocations doivent être faites en utilisant la politique de "consensus de l'IETF" définie dans la [RFC2434].

8.1.1 Types de canal de contrôle de VCCV MPLS

L'IANA a établi un registre des "Types de canal de contrôle VCCV MPLS". Ce sont des champs de 8 bits. Les valeurs de type de CC 0x01, 0x02, et 0x04 sont spécifiées à la Section 4 du présent document. Les valeurs des champs binaires restants (0x08, 0x10, 0x20, 0x40, et 0x80) sont à allouer par l'IANA en utilisant la politique de "consensus de l'IETF" définie dans la [RFC2434]. Une description de type de canal de contrôle VCCV et une référence à une RFC approuvée par l'IESG sont exigées pour toute allocation dans ce registre.

Types de canal de contrôle MPLS :

Bit (valeur)	**Description**
Bit 0 (0x01)	Type 1 : Mot de contrôle PWE3 0001b comme premier quartet (PW-ACH, voir la [RFC4385])
Bit 1 (0x02)	Type 2 : Étiquette d'alerte de routeur MPLS
Bit 2 (0x04)	Type 3 : Étiquette de PW MPLS avec TTL == 1
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé

Bit 6 (0x40) Réservé
Bit 7 (0x80) Réservé

Le bit de poids fort (d'ordre supérieur) est marqué bit 7, et le bit de moindre poids (d'ordre inférieur) est marqué bit 0, voir la "valeur" entre parenthèses.

8.1.2 Types de vérification de connexité de VCCV MPLS

L'IANA a établi un registre des "Types de vérification de connexité de VCCV MPLS". Ce sont des champs de 8 bits. Les valeurs de type de CV 0x01 et 0x02 sont spécifiées à la Section 4 du présent document. Les valeurs de champ binaire restantes (0x04, 0x08, 0x10, 0x20, 0x40, et 0x80) sont à allouer par l'IANA en utilisant la politique de "consensus de l'IETF" définie dans la [RFC2434]. Une description de type de vérification de connexité de VCCV et une référence à une RFC approuvée par l'IESG sont exigées pour toute allocation dans ce registre.

Types de vérification de connexité MPLS :

Bit (valeur)	Description
Bit 0 (0x01)	Ping ICMP
Bit 1 (0x02)	Ping LSP
Bit 2 (0x04)	Réservé
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé
Bit 6 (0x40)	Réservé
Bit 7 (0x80)	Réservé

Le bit de poids fort (d'ordre supérieur) est marqué bit 7, et le bit de moindre poids (d'ordre inférieur) est marqué bit 0, voir la "valeur" entre parenthèses.

8.2 Type de canal associé au PW

Les types de canal associé au PW utilisés par VCCV comme définis dans les paragraphes 5.1.1 et 6.1 s'appuient sur les numéros précédemment alloués dans le registre des types de canal associé au pseudo-filaire [RFC4385] dans l'espace de noms de pseudo-filaires accessible dans [IANA.pwe3]. En particulier, 0x21 (Protocole Internet version 4) DOIT être utilisé chaque fois que une charge utile IPv4 suit l'en-tête de canal associé au pseudo-filaire, ou 0x57 DOIT être utilisé quand une charge utile IPv6 suit l'en-tête de canal associé au pseudo-filaire.

8.3 Allocations L2TPv3

Les paragraphes 8.3.1 à 8.3.3 sont les enregistrements des nouvelles valeurs de L2TP pour les registres déjà gérés par l'IANA. Le paragraphe 8.3.4 est un nouveau registre qui a été ajouté aux espaces de noms L2TP existants, et sera tenu par l'IANA en conséquence. Les espaces de nom de protocole de tunnelage de couche 2 "L2TP" sont accessibles à [IANA.l2tp].

8.3.1 Paires d'attribut/valeur (AVP) de message de contrôle

Un attribut d'AVP supplémentaire est spécifié au paragraphe 6.3.1. Il a été défini par l'IANA comme décrit au paragraphe 2.2 de la [RFC3438].

Type d'attribut	Description
96	AVP Capacité VCCV

8.3.2 Bits de la sous couche par défaut spécifique de couche 2

La sous couche par défaut spécifique de couche 2 contient 8 bits dans la portion d'ordre inférieur de l'en-tête. Le présent document définit un bit réservé dans la sous couche par défaut spécifique de couche 2 au paragraphe 6.1, qui a été alloué par IANA suivant le consensus de l'IETF [RFC2434].

Bits de sous couche par défaut spécifique de couche 2 - selon la [RFC3931]
Bit 0 - bit V (VCCV)

8.3.3 Bits de sous couche spécifique de ATM

La sous couche spécifique de ATM contient 8 bits dans la portion d'ordre inférieur de l'en-tête. Le présent document définit un bit réservé dans la sous couche spécifique de ATM au paragraphe 6.1, qui a été alloué par l'IANA suivant le consensus de l'IETF [RFC2434].

Bits de sous couche spécifique de ATM - selon la [RFC4454]
Bit 0 - bit V (VCCV)

8.3.4 Valeurs d'AVP de capacité VCCV

Ceci est un nouveau registre que tient l'IANA dans l'espace de noms L2TP. L'IANA a créé et tient un registre pour les gabarits binaires de types de CC et de types de CV dans l'AVP Capacité de VCCV, définie au paragraphe 6.3.1. Les allocations doivent être faites en utilisant la politique de "consensus de l'IETF" définie dans la [RFC2434]. Une description de type de CC ou type de CV VCCV et une référence à une RFC approuvée par l'IESG sont exigées pour toute allocation dans ce registre.

L'IANA a réservé les bits suivants dans ce registre :

Valeurs d'AVP Capacité VCCV (type d'attribut 96)

Types de canal de contrôle L2TPv3 :

Bit (valeur)	**Description**
Bit 0 (0x01)	Sous couche spécifique de couche 2 avec le bitV établi
Bit 1 (0x02)	Réservé
Bit 2 (0x04)	Réservé
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé
Bit 6 (0x40)	Réservé
Bit 7 (0x80)	Réservé

Types de vérification de connexité L2TPv3 :

Bit (valeur)	**Description**
Bit 0 (0x01)	Ping ICMP
Bit 1 (0x02)	Réservé
Bit 2 (0x04)	Réservé
Bit 3 (0x08)	Réservé
Bit 4 (0x10)	Réservé
Bit 5 (0x20)	Réservé
Bit 6 (0x40)	Réservé
Bit 7 (0x80)	Réservé

Le bit de poids fort (d'ordre supérieur) est marqué bit 7, et le bit de moindre poids (d'ordre inférieur) est marqué bit 0, voir la "valeur" entre parenthèses.

9. Considérations d'encombrement

Il est recommandé que les ressources de bande passante utilisées par VCCV soient minimales comparées à celles du PW associé. La bande passante requise pour le canal de VCCV est prise en dehors de toute allocation au trafic de données de PW, et peut être configurable. Quand on fait une réservation de ressource ou une programmation de réseau, les exigences de bande passante pour les données de PW et le trafic de VCCV doivent être prises en compte.

Les applications VCCV (c'est-à-dire, les types Vérification de connexité) DOIVENT considérer les implications d'encombrement et d'usage de bande passante et fournir des détails sur la gestion de bande passante ou la fréquence des paquets. Les applications VCCV peuvent avoir une gestion incorporée de bande passante dans leurs protocoles. D'autres

applications VCCV peuvent avoir leur bande passante limitée par configuration, et les limiter en débit peut être dommageable car cela pourrait se traduire en une déclaration incorrecte des défaillances de connexité. Pour toutes les autres applications VCCV, les messages VCCV sortants DEVRAIENT être limités en débit pour empêcher qu'une vérification de connexité agressive consomme une bande passante excessive, causant de l'encombrement, devenant des attaques de déni de service, ou générant un taux excessif de paquet au PE lié au CE.

Si ces conditions ne peuvent pas être respcetées, un schéma adaptatif fondé sur la perte DEVRAIT être appliqué au trafic VCCV sortant de contrôle d'encombrement, afin qu'il soit en compétition équitable avec TCP au sein d'un ordre de grandeur. Une méthode pour déterminer une bande passante acceptable pour VCCV (TFRC) est décrite dans la [RFC3448] ; d'autres méthodes existent. Par exemple, la gestion de la bande passante ou de la fréquence de paquet peut inclure tout ce qui suit : une négociation de l'intervalle/débit de transmission, un étranglement du taux de transmission dans les situations "d'encombrement détecté", un démarrage lent après une fermeture due à l'encombrement et jusqu'à ce que la connexité de base soit vérifiée, et autres mécanismes.

Les applications de ping ICMP et de LSP MPLS DEVRAIENT être limitées en débit en dessous de 5 % du débit binaire du PW associé. À cette fin, le débit binaire considéré d'un pseudo-filaire dépend du type de PW. Pour les pseudo-filaires qui portent un trafic à débit constant (par exemple, les PW en multiplexage temporel) le débit binaire complet du PW est utilisé. Pour les pseudo-filaires qui portent du trafic à débit variable (par exemple, des PW Ethernet) le débit moyen ou soutenu du PW est utilisé.

Comme décrit à la Section 10, les messages VCCV entrants peuvent être limités en débit pour la protection contre les attaques de déni de service. Cet étranglement ou régulation des messages VCCV entrants ne devrait pas être plus contraignant que la bande passante allouée au canal de VCCV pour empêcher des fausses indications de défaillance de connexité.

10. Considérations sur la sécurité

Les routeurs qui mettent en œuvre VCCV créent un canal de contrôle (CC) associé à un pseudo-filaire. Ce canal de contrôle peut être signalé (par exemple, en utilisant LDP ou L2TPv3 selon le PWE3) ou configuré de façon statique. Sur ce canal de contrôle sont envoyés les messages de vérification de connexité VCCV. Donc, trois zones différentes sont concernées du point de vue de la sécurité.

La première zone de problèmes se rapporte aux attaques du paramètre de plan de contrôle et du message d'état, c'est-à-dire, les attaques qui concernent la signalisation des capacités VCCV. La sécurité du plan de contrôle de PW MPLS est discutée au paragraphe 8.2 de la [RFC4447]. La sécurité du plan de contrôle de PW L2TPv3 est discutée au paragraphe 8.1 de la [RFC3931]. L'ajout des extensions de négociation de vérification de connexité ne change pas les aspects de sécurité du paragraphe 8.2 de la [RFC4447], ou du paragraphe 8.1 de la [RFC3931]. La mise en œuvre de filtres d'adresse de source IP peut aussi aider à supprimer ces types d'attaques.

Une seconde zone de soucis concerne les attaques sur le plan des données, c'est-à-dire, des attaques sur le canal associé lui-même. Les routeurs qui mettent en œuvre les mécanismes de VCCV sont de plus soumis à des attaques de déni de service sur le plan des données comme suit :

Un intrus pourrait intercepter ou injecter des paquets VCCV fournissant effectivement des faux positifs ou négatifs.

Un intrus pourrait délibérément inonder un routeur homologue avec des messages VCCV pour dénier le service aux autres.

Un appareil mal configuré ou au mauvais comportement pourrait par inadvertence inonder un routeur homologue avec des messages VCCV qui pourraient résulter en un déni de services. En particulier, si un routeur a implicitement ou explicitement indiqué qu'il ne peut pas prendre en charge un ou tous les types de VCCV, mais a envoyé ces messages en quantité suffisante, il pourrait en résulter un déni de service.

Pour se protéger contre ces attaques potentielles (délibérées ou involontaines) plusieurs techniques d'atténuation peuvent être employées :

Des mécanismes d'étranglement de message VCCV peuvent être utilisés, en particulier dans les mises en œuvre réparties qui ont un processus centralisé de plan de contrôle avec diverses cartes de ligne rattachées par un chemin de données du plan de contrôle. Dans ces architectures, les messages VCCV peuvent être traités sur le processeur central après y avoir été transmis par la carte de ligne receveuse. Dans ce cas, le chemin entre la carte de ligne et le processeur de contrôle peut être saturé si un étranglement approprié du trafic de VCCV n'est pas employé, ce qui pourrait conduire à un déni de service complet pour les utilisateurs de cette carte de ligne. Un tel filtrage est aussi utile pour prévenir le traitement de messages VCCV non désirés, comme ceux envoyés sur des types de canal de contrôle ou types de VCCV non voulus (et peut-être non annoncés).

Le paragraphe 8.1 de la [RFC4447] discute des méthodes pour protéger le plan des données des PW MPLS contre les attaques sur le plan des données. Cependant la mise en œuvre du protocole de vérification de connexité étend la gamme des attaques possible du plan des données. Pour cette raison, les mises en œuvre DOIVENT fournir une méthode pour sécuriser le plan des données. Ce peut être sous la forme d'un chiffrement des données avec IPsec sur les paquets MPLS encapsulés conformément à la [RFC4023], ou en fournissant la capacité d'organiser le réseau MPLS d'une façon telle qu'aucun paquet MPLS externe ne puisse être injecté (réseau MPLS privé).

Pour L2TPv3, les considérations de falsification de paquet de données sont examinées au paragraphe 8.2 de la [RFC3931]. Bien que l'identifiant de session L2TPv3 assure la séparation du trafic, le champ facultatif Cookie fournit une protection supplémentaire pour déjouer les attaques de falsification. Pour maximiser la protection contre diverses attaques du plan des données, un mouchard de 64 bits peut être utilisé. L2TPv3 peut aussi fonctionner avec IPsec comme précisé au paragraphe 4.1.3 de la [RFC3931].

Une troisième et dernière zone de soucis se rapporte au traitement du contenu réel des messages VCCV, c'est-à-dire, les messages Ping LSP ICMP. Donc, les considérations de sécurité correspondantes pour ces protocoles (Ping LSP [RFC4379], Ping ICMPv4 [RFC0792], et Ping ICMPv6 [RFC4443]) s'appliquent aussi.

11. Remerciements

Les auteurs tiennent à remercier Hari Rakotoranto, Michel Khouderchah, Bertrand Duvivier, Vanson Lim, Chris Metz, W. Mark Townsley, Eric Rosen, Dan Tappan, Danny McPherson, Luca Martini, Don O'Connor, Neil Harrison, Danny Prairie, Mustapha Aissaoui et Vasile Radoaca pour leurs précieux commentaires et suggestions.

12. Références

12.1 Références normatives

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. *(MàJ par la* RFC6633)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3032] E. Rosen et autres, "Codage de pile d'étiquettes MPLS", janvier 2001. *(Info. ; MàJ par* RFC9017)

[RFC3931] J. Lau et autres, "Protocole de tunnelage de couche deux - version 3 (L2TPv3)", mars 2005. *(P.S.)*

[RFC4379] K. Kompella et G. Swallow, "Détection des défaillances de plan des données en commutation d'étiquettes multi protocole (MPLS)", février 2006. (*MàJ par la* RFC6424 *; Rendue obsolète par* RFC8029) *(P.S.)*

[RFC4385] S. Bryant et autres, "Mot de contrôle d'émulation bord à bord pseudo filaire (PWE3) à utiliser sur un PSN MPLS", février 2006. *(P.S.)*

[RFC4443] A. Conta et autres, "Spécification du protocole de message de contrôle Internet (ICMPv6) pour la version 6 du protocole Internet (IPv6)", mars 2006. (*Remplace* RFC2463) (*MàJ* RFC2780) (*MàJ par* RFC4884) *(D.S.)*

[RFC4446] L. Martini, "Allocations de l'IANA pour l'émulation de bord à bord pseudo filaire (PWE3)", avril 2006. (BCP0116)

[RFC4447] L. Martini et autres, "Établissement et maintenance de pseudo filaires avec le protocole de distribution d'étiquettes", avril 2006. (*MàJ par la* RFC6723) *(P.S. ; Remplacé par* RFC8077 STD 84)

12.2 Références pour information

[IANA.l2tp] Internet Assigned Numbers Authority, "Layer Two Tunneling Protocol "L2TP"", avril 2007, <http://www.iana.org/assignments/l2tp-parameters>.

[IANA.pwe3] Internet Assigned Numbers Authority, "Pseudo Wires Name Spaces", juin 2007, <http://www.iana.org/assignments/pwe3-parameters>.

[MSG-MAP] Nadeau, T., "Pseudo Wire (PW) OAM Message Mapping", Travail en cours, mars 2007.

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC3438] W. Townsley, "Mise à jour des considérations de l'IANA sur le protocole de tunnelage de couche deux (L2TP)", décembre 2002. (BCP0068)

[RFC3448] M. Handley, S. Floyd, J. Padhye, J. Widmer, "Contrôle de débit convivial sur TCP (TFRC) : Spécification du protocole", janvier 2003. (*Obsolète, voir* RFC5348) *(P.S.)*

[RFC3916] X. Xiao, D. McPherson et P. Pate, éd., "Exigences pour l'émulation bord à bord pseudo filaire (PWE3)", septembre 2004. *(Information)*

[RFC3985] S. Bryant et autres, "Architecture d'émulation bord à bord de pseudo-filaire (PWE3)", mars 2005. *(Information)*

[RFC4023] T. Worster et autres, "Encapsulation de MPLS dans IP ou encapsulation d'acheminement générique (GRE)", mars 2005. (*MàJ par* RFC5332) *(P.S.)*

[RFC4377] T. Nadeau et autres, "Exigences de fonctionnement et de gestion (OAM) pour les réseaux en commutation d'étiquettes multiprotocoles (MPLS)", février 2006. *(Information)*

[RFC4448] L. Martini et autres, "Méthodes d'encapsulation pour le transport d'Ethernet sur des réseaux MPLS", avril 2006. *(P.S. ; MàJ par* RFC8469)

[RFC4454] S. Singh et autres, "Mode de transfert asynchrone (ATM) sur la version 3 du protocole de tunnelage de couche 2 (L2TPv3)", mai 2006. *(P.S.)*

[RFC4928] G. Swallow et autres, "Éviter le traitement de chemins multiples à coût égal dans les réseaux MPLS", juin 2007. (BCP0128)

Appendice A Adresse des contributeurs

George Swallow
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA
mél : swallow@cisco.com

Monique Morrow
Cisco Systems, Inc.
Glatt-com
CH-8301 Glattzentrum
Switzerland
mél : mmorrow@cisco.com

Yuichi Ikejiri
NTT Communication Corp.
1-1-6, Uchisaiwai-cho,
Tokyo 100-8019
Shinjuku-ku JAPAN
mél : y.ikejiri@ntt.com

Luca Martini
Cisco Systems, Inc.
9155 East Nichols Avenue, S 400
Englewood, CO, 80112
USA
mél : lmartini@cisco.com

Kenji Kumaki
KDDI Corporation
KDDI Bldg. 2-3-2
Nishishinjuku
Tokyo 163-8003 JAPAN
mél : ke-kumaki@kddi.com

Peter B. Busschbach
Alcatel-Lucent
67 Whippany Road
Whippany, NJ, 07981
USA
mél : busschbach@alcatel-lucent.com

Rahul Aggarwal
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089
USA
mél : rahul@juniper.net

Adresse des auteurs

Thomas D. Nadeau (editor)
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA

Carlos Pignataro (editor)
Cisco Systems, Inc.
7200 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709

mél : tnadeau@lucidvision.com

USA
mél : cpignata@cisco.com

Déclaration complète de droits de reproduction