Groupe de travail Réseau
Request for Comments : 35187
RFC rendue obsolète : 2878
Catégorie : En cours de normamisation

M. Higashiyama, Anritsu
F. Baker & T. Liao, Cisco Systems
avril 2003
Traduction Claude Brière de L'Isle

Protocole de contrôle de pontage (BCP) pour le protocole point à point (PPP)

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le protocole point à point (PPP) fournit une méthode standard pour transporter des datagrammes multi-protocole sur des liaisons point à point. PPP définit un protocole de contrôle de liaison (LCP, *Link Control Protocol*) extensible et propose une famille de protocoles de contrôle de réseau (NCP, *Network Control Protocol*) pour établir et configurer différents protocoles de couche réseau.

Le présent document définit le NCP pour établir et configurer le pontage à distance pour les liaisons PPP.

Le présent document rend obsolète la RFC 2878, qui se fondait sur le pont MAC IEEE 802.1D-1993. Le présent document étend cette spécification en améliorant la prise en charge des paquets de contrôle de ponts.

Table des Matières

1. Perspective historique

Deux algorithmes de base sont très répandus dans l'industrie pour le pontage des réseaux de zone locale. L'algorithme le plus courant est appelé "pontage transparent", et a été normalisé pour les configurations de LAN étendus par la norme IEEE 802.1. L'autre est appelé "pontage de route de source", et est dominant sur les LAN à anneau à jetons de la norme IEEE 802.5.

L'IEEE a combiné ces deux méthodes dans un appareil appelé un pont d'acheminement de source transparent (SRT, *Source Routing Transparent*) qui fournit concurremment à la fois le pontage de route de source et le pontage transparent. Les ponts transparents et SRT sont spécifiés dans la norme IEEE 802.1D-1998 [802.1D-98].

Bien que le comité IEEE 802.1G traite du pontage à distance [802.1g], aucun standard ne définit directement les mécanismes de mise en œuvre du pontage à distance. Techniquement, cela irait au-delà du mandat du comité IEEE 802. Cependant, 802.1D et 802.1G le permettent toutes deux. La mise en œuvre peut modéliser la ligne soit comme un composant au sein d'une seule entité de relais de commande d'accès au support physique (couche 3) (MAC, *Media Access Control*) soit comme le support de LAN entre deux ponts distants.

La norme IEEE 802.1D d'origine est augmentée par IEEE 802.1Q [802.1Q] pour fournir la prise en charge de LAN virtuel. Le LAN virtuel est une caractéristique intégrante des réseaux LAN commutés.

1.1 Mots clés des exigences

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

2. Méthodes de pontage

2.1 Pontage transparent

Pour les non initiés, décrivons d'abord le pontage transparent. Essentiellement, dans un réseau, les ponts fonctionnent comme des entités isolées, qui s'ignorent largement les unes les autres. Un pont transparent tient une base de données de transmission consistant en enregistrements de {adresse, interface} ou {adresse, interface, identifiant de VLAN}, en sauvegardant l'adresse de source de chaque transmission de LAN qu'il reçoit, ainsi qu'avec l'identifiant d'interface pour l'interface sur laquelle il l'a reçu. Les ponts qui prennent en charge les LAN virtuels conservent de plus l'identifiant de LAN virtuel dans leur base de données de transmission. Le pont va ensuite vérifier si l'adresse de destination est dans la base de données, et si elle y est, soit éliminer le message lorsque destination et source sont situées à la même interface, soit transmettre le message à l'interface indiquée. Un message dont l'adresse de destination ne se trouve pas dans le tableau est transmis à toutes les interfaces excepté celle où il a été reçu. Ce comportement s'applique aussi aux trames en diffusion/diffusion groupée.

L'erreur évidente est que des chemins redondants dans le réseau causent l'apparition d'un comportement de transmission indéterminé (ou bien, trop déterminé). Pour empêcher cela, un protocole appelé protocole d'arbre d'expansion *(Spanning Tree Protocol)* est exécuté entre les ponts pour détecter et retirer logiquement les chemins redondants du réseau.

Un système est choisi comme "racine", qui émet périodiquement un message appelé une unité de données protocolaires de pont (BPDU, *Bridge Protocol Data Unit*), entendu par tous les ponts du voisinage. Chacun d'eux modifie et passe la BPDU à ses voisins, jusqu'à ce qu'elle arrive aux derniers segments de LAN dans le réseau (où elle meurt, n'ayant plus d'autre

voisin à qui la passer) ou jusqu'à ce que le message soit arrêté par un pont qui a un chemin supérieur à la "racine". Dans ce dernier cas, l'interface sur laquelle est reçue la BPDU est ignorée (elle est placée dans un état d'attente chaude, aucun trafic n'est émis dessus sauf la BPDU, et tout le trafic reçu d'elle est éliminé) jusqu'à ce qu'un changement de topologie force un nouveau calcul du réseau.

Pour établir des LAN virtuels dans un environnement à plusieurs ponts, le protocole d'enregistrement de VLAN GARP (GVRP, *GARP VLAN Registration Protocol*) est exécuté entre les ponts pour échanger les informations de LAN virtuel. GVRP fournit un mécanisme pour établir de façon dynamique et mettre à jour les connaissances sur l'ensemble de LAN virtuels qui ont actuellement des membres actifs.

Pour réduire l'arrosage inutile de diffusions groupées dans le réseau, les ponts échangent les adresses MAC de groupe en utilisant le protocole d'enregistrement de diffusion groupée de GARP. GMRP *(GARP Multicast Registration Protocol)* fournit un mécanisme par lequel les ponts peuvent savoir quelles trames de diffusion groupée devraient être transmises sur chaque accès.

2.2 Pontage transparent à distance

Il existe deux sortes de ponts de base – ceux qui interconnectent directement les LAN, appelés ponts locaux, et ceux qui interconnectent les LAN via un support intermédiaire comme une liaison louée, appelés ponts distants. PPP peut être utilisé pour connecter les ponts distants.

Le comité IEEE 802.1G Pontage MAC distant a proposé un modèle de pont distant dans lequel un ensemble de deux ponts distants ou plus interconnectés via des lignes distantes est appelé un groupe de ponts distants. Au sein d'un groupe, une grappe de ponts distants est formée de façon dynamique par l'exécution d'un arbre d'expansion comme l'ensemble des ponts qui peuvent se passer des trames entre eux.

Ce modèle accorde aux lignes distantes les propriétés de base d'un LAN, mais n'exige pas une transposition bijective des lignes en segments de LAN virtuel. Par exemple, le modèle de trois ponts distants interconnectés, A, B et C, peut être celui d'un segment de LAN virtuel entre A et B et un autre entre B et C. Cependant, si une ligne existe entre les ponts distants B et C, une trame pourrait en fait être envoyée directement de B à C, pour autant qu'elle semble de l'extérieur avoir voyagé à travers A.

IEEE 802.1G permet donc une grande liberté de mise en œuvre pour des caractéristiques comme l'optimisation de chemin et l'équilibrage de charge, pour autant que le modèle soit conservé.

Pour rester simple, on expose le pontage distant dans le présent document dans les termes de deux ponts distants connectés par une seule ligne.

2.3 Acheminement de source

Le comité IEEE 802.1D a normalisé l'acheminement de source pour tous les types MAC qui permettent son utilisation. Actuellement, les types MAC qui prennent en charge l'acheminement de source sont FDDI et l'anneau à jetons IEEE 802.5.

La norme IEEE définit l'acheminement de source seulement comme un composant d'un pont SRT. Cependant, de nombreux ponts ont été mis en œuvre avec la capacité d'effectuer seuls l'acheminement de source. Ils sont le plus souvent mis en œuvre en conformité soit avec l'architecture de référence de réseau en anneau à jeton d'IBM [IBM] soit avec l'appendice d'acheminement de source de IEEE 802.1D-1998 [802.1D-98].

Dans l'approche de l'acheminement de source, le système d'origine a la responsabilité d'indiquer le chemin que le message devrait suivre. Il le fait, si le message est dirigé hors du segment local, en incluant une extension d'en-tête MAC de longueur variable appelée champ d'informations d'acheminement (RIF, *Routing Information Field*). Le RIF consiste en un mot de 16 bits de fanions et paramètres, suivi par zéro, un ou plusieurs identifiants de segment et de pont. Chaque pont en route détermine à partir de la liste d'acheminements de source si il devrait accepter le message et comment le transmettre.

Afin de découvrir le chemin vers une destination, le système d'origine transmet une trame Explorer. Une trame Explorer tous chemins (ARE, *All-Routes Explorer*) suit tous les chemins possibles vers une destination. Une trame Explorer l'arbre d'expansion (STE, *Spanning Tree Explorer*) ne suit que les chemins définis par les accès de pont que l'algorithme d'arbre d'expansion a mis dans l'état Transmission. Les états d'accès ne s'appliquent pas aux trames ARE ou aux trames à acheminement spécifique. Le système de destination répond à chaque copie d'une trame ARE par une trame à

acheminement spécifique, et à une trame STE par une trame ARE. Dans l'un et l'autre cas, la station d'origine peut recevoir plusieurs réponses, à partir desquelles elle choisit le chemin qu'elle va utiliser pour les futures trames à acheminement spécifique.

L'algorithme pour l'acheminement de source exige que le pont soit capable d'identifier toute interface par son identifiant de segment et de pont. Lorsque un paquet est reçu qui a le RIF présent, un booléen est inspecté dans le RIF pour déterminer si les identifiants de segment et de pont sont à inspecter dans le sens "avant" ou "inverse". Dans cette recherche, le pont examine l'identifiant de segment et de pont de l'interface sur laquelle le paquet a été reçu, et transmet le paquet vers le segment identifié dans l'identifiant de segment et de pont qui le suit.

GVRP et GMRP sont disponibles et efficaces sur les réseau à acheminement de source.

2.4 Pontage d'acheminement de source à distance

Pour le moment, il n'y a pas de proposition de pont d'acheminement de source distante dans la norme IEEE 802.1, bien que de nombreux fabricants proposent des produits de pont d'acheminement de source distante.

On permet la modélisation de la ligne soit comme une connexion résidant entre deux moitiés d'un pont "partagé" (le modèle du pont partagé) ou comme un segment de LAN entre deux ponts (modèle du pont indépendant). Dans ce dernier cas, la ligne requiert un identifiant de segment de LAN.

Par défaut, les ponts PPP à acheminement de source utilisent le modèle du pont indépendant. Cette exigence assure l'interopérabilité en l'absence de négociation d'option. Afin d'utiliser le modèle du pont partagé, un système DOIT réussir à négocier l'option de configuration Identification de pont.

Bien qu'aucune négociation d'option ne soit requise pour qu'un système utilise le modèle du pont indépendant, il est fortement recommandé que les systèmes qui utilisent ce modèle négocient l'option de configuration Identification de ligne. Le faire permet de vérifier que la configuration de l'identifiant de segment de LAN alloué à la ligne est correcte.

Lorsque deux systèmes PPP utilisent le modèle du pont partagé, le système qui transmet une trame Explorer sur la liaison PPP DOIT mettre à jour le RIF au nom des deux systèmes. L'objet de cette contrainte est de s'assurer de l'interopérabilité et de préserver la simplicité de l'algorithme de pontage. Par exemple, si le système receveur ne sait pas si le système émetteur a mis à jour le RIF, il va devoir examiner le RIF et décider si il le met à jour. Le choix du système émetteur du rôle de mise à jour du RIF permet au système receveur de la trame provenant de la liaison PPP de transmettre la trame sans traiter le RIF.

Étant donné que l'acheminement de source est configuré sur une ligne ou ensemble de lignes, les spécificités de l'état de la liaison par rapport à la trame STE sont définies par le protocole d'arbre d'expansion utilisé. Le choix entre le modèle du pont partagé et celui du pont indépendant n'affecte pas le fonctionnement de l'arbre d'expansion. Dans les deux cas, le protocole d'arbre d'expansion est exécuté indépendamment sur les deux systèmes.

2.5 Pontage de traduction SR-TB

La norme IEEE 802 ne traite pas actuellement les ponts d'adressage qui font la traduction entre pontage transparent et acheminement de source. Pour les besoins de la présente norme, un tel appareil est soit un pont transparent soit un pont d'acheminement de source, et va agir sur la ligne d'une de ces deux façons, comme il le fait sur le LAN.

3. Services de trafic

Plusieurs services sont fournis à différents types de systèmes et configurations d'utilisateurs. Cela inclut la préservation de la somme de contrôle de trame de LAN, la génération de somme de contrôle de trame de LAN, la compression Tinygram, et l'identification d'ensembles clos de LAN.

3.1 Préservation de la somme de contrôle de trame de LAN

La norme IEEE 802.1 stipule que le LAN étendu doit bénéficier de la même probabilité d'erreur non détectée qu'un LAN individuel. Bien qu'il y ait eu un débat considérable sur l'algorithme, aucun autre algorithme n'a été proposé que d'avoir la

somme de contrôle de trame de LAN reçue par le dernier receveur identique à la valeur calculée par l'émetteur d'origine. Le réaliser exige bien sûr que les protocoles de ligne préservent la somme de contrôle de trame de LAN de bout en bout. Le protocole est optimisé pour cette approche.

3.2 Trafic sans somme de contrôle de trame de LAN

Le fait que le protocole soit optimisé à l'égard de la préservation de la somme de contrôle de trame de LAN soulève deux questions jumelles : "quelle est l'approche à utiliser par les systèmes qui, quelle qu'en soit la raison, ne peuvent pas facilement prendre en charge la préservation de la somme de contrôle de trame ?" et "quelle est l'approche à utiliser lorsque le système génère un message, qui n'a donc pas de somme de contrôle de trame précalculée ?"

Il est certain qu'une approche serait d'exiger des stations qu'elles calculent la somme de contrôle de trame dans le logiciel si la prise en charge par le matériel était indisponible ; cela serait parfaitement consternant et soulèverait des questions sérieuses d'interprétation au niveau du pont/routeur.

Cependant, les stations qui mettent en œuvre la préservation de la somme de contrôle de trame doivent déjà résoudre ce problème, car elles génèrent bien du trafic. Donc, la solution adoptée est que les messages qui n'ont pas de somme de contrôle de trame soient étiquetés et portés à travers la ligne.

Lorsque un système qui ne met pas en œuvre la préservation de la somme de contrôle de trame de LAN reçoit une trame qui a une séquence de contrôle de trame (FCS, *Frame Check Sequence*) incorporée, il la convertit pour son propre usage en retirant les quatre octets de queue. Lorsque un système transmet une trame qui ne contient pas de FCS incorporée à un LAN, il la transmet d'une façon qui cause le calcul de la FCS.

3.3 Compression des petits datagrammes

Un problème du pontage Ethernet distant est que les protocoles qui sont les plus intéressants pour le pont sont enclins à avoir des problèmes sur les lignes à bas débit (64 kbit/s et en dessous). Cela peut être partiellement compensé en observant que les fabricants qui définissent ces protocoles remplissent souvent la PDU avec des octets à zéro. Donc, une PDU Ethernet ou IEEE 802.3 reçue d'une ligne qui est (1) inférieure à la taille minimum de PDU, et (2) a une somme de contrôle de trame de LAN présente, doit être bourrée en insérant des zéros entre les quatre derniers octets et le reste de la PDU avant de la transmettre sur un LAN. Ces protocoles sont fréquemment utilisés pour des sessions interactives, et qui donc sont souvent aussi petites.

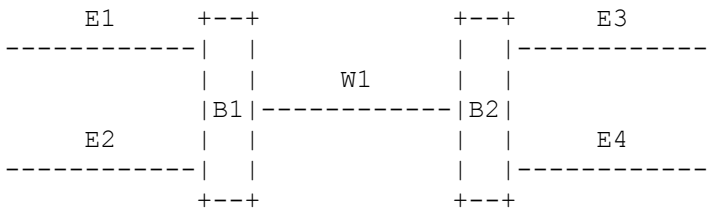
Pour prévenir toute ambiguïté, les PDU qui exigent un bourrage sont explicitement étiquetées. La compression est une option de la station émettrice, et n'est probablement effectuée que sur les lignes à bas débit, peut-être sous le contrôle de la configuration.

Le pseudocode de l'Appendice B décrit ces algorithmes.

3.4 LAN virtuels

La norme IEEE 802.1Q définit les LAN virtuels et leur format échangeable de trame étiquetée de VLAN. Les LAN virtuels permettent aux usagers que plusieurs groupes de communautés coexistent au sein d'un pont. Une communauté de pontage est identifiée par son identifiant de VLAN. Si un système qui prend en charge les LAN virtuels reçoit une trame du LAN, cette trame ne sera émise que vers un LAN qui appartient à la même communauté. Afin de traiter plusieurs communautés sur une seule ligne, la norme IEEE 802.1Q définit une trame étiquetée de VLAN.

Par exemple, supposons qu'on ait la configuration suivante :



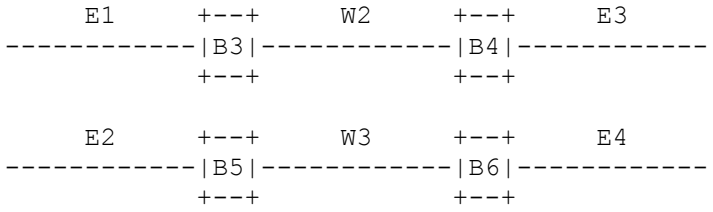
E1, E2, E3, et E4 sont des LAN Ethernet (ou des anneaux à jetons, FDDI, etc.). W1 est un WAN (PPP sur T1). B1 et B2

sont des ponts de niveau MAC.

On veut faire communiquer les stations terminales E1 et E3, et on veut que les stations terminales E2 et E4 communiquent, mais on ne veut pas que les stations terminales E1 et E3 communiquent avec les stations E2 et E4.

Ceci est vrai pour les trafic en envoi individuel, en diffusion groupée, et en diffusion. Si un datagramme en diffusion est généré en E1, on veut qu'il ne soit propagé qu'à E3, et pas à E2 ou E4.

Une autre façon de regarder cela est que E1 et E3 forment un LAN virtuel, et que E2 et E4 forment un LAN virtuel, comme si la configuration suivante était en fait utilisée :



3.5 Indicateur de paquet de contrôle de pont

L'option Indicateur de paquet de contrôle de pont est utilisée pour classer les paquets de contrôle de pont comme des BPDU d'arbre d'expansion, des PDU GARP, etc. Les protocoles comme STP et GARP sont au monde du pontage ce que OSPF ou BGP sont au monde de l'acheminement. Tout comme les paquets de mise à jour de chemin IP sont marqués avec une valeur de préséance IP de 6 ou 7 et reçoivent un certain traitement préférentiel de transmission [RFC2474], les paquets de contrôle de pont sont marqués d'une façon similaire avec le bit Indicateur de paquet de contrôle de pont.

Si l'option Indicateur de paquet de contrôle de pont est activée, un système DOIT régler le bit Indicateur de paquet de contrôle de pont d'un paquet dans le champ Fanions à 1 si et seulement si il est une trame sortante de contrôle de pont. De plus, un système DOIT éviter d'éliminer ou de retarder de façon significative les paquets de contrôle de ponts.

Si l'option Indicateur de paquet de contrôle de pont est désactivée, un système DOIT régler le bit Indicateur de paquet de contrôle de pont à 0 pour toutes les trames. Cela préserve la rétro compatibilité avec la [RFC2878]. Cependant, même si cette option est désactivée, un système DEVRAIT quand même éviter d'éliminer ou de retarder de façon significative les paquets de contrôle de pont. Cela peut être réalisé par l'analyse du champ Adresse MAC de destination.

4. Protocole de contrôle de réseau PPP pour le pontage

Le protocole de contrôle de pontage (BCP, *Bridging Control Protocol*) est chargé de configurer, activer et désactiver les modules de protocole de pont des deux extrémités de la liaison point à point. BCP utilise le même mécanisme d'échange de paquets que le protocole de contrôle de liaison. Les paquets BCP ne peuvent pas être échangés tant que PPP n'a pas atteint la phase Protocole de couche réseau. Les paquets BCP reçus avant cette phase DEVRAIENT être éliminés en silence.

Le protocole de contrôle de pontage est exactement le même que le protocole de contrôle de liaison [RFC1661] avec les exceptions suivantes :

Modifications de trame
Le paquet peut utiliser toutes modifications au format de trame de base qui ont été négociées durant la phase d'établissement de la liaison
Les mises en œuvre NE DEVRAIENT PAS négocier la compression de champ d'adresse et de contrôle ou la compression du champ Protocole sur d'autres liaisons qu'à basse vitesse.

Champ Protocole de couche liaison des données
Exactement un paquet BCP est encapsulé dans le champ Informations PPP, où le champ Protocole PPP indique le type hexadécimal 8031 (BCP).

Champ Code
Seuls les codes 1 à 7 (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack et Code-Reject) sont utilisés. Les autres codes DEVRAIENT être traités comme non reconnus et DEVRAIENT résulter en un Code-Reject.

Fin de temporisation
Les paquets BCP ne peuvent pas être échangés avant que PPP ait atteint la phase Protocole de couche réseau. Une mise en œuvre DEVRAIT être prête à attendre que l'authentification et la détermination de la qualité de la liaison se finissent avant de mettre fin à la temporisation de l'attente d'un Configure-Ack ou d'une autre réponse. Il est suggéré qu'une mise en œuvre n'abandonne qu'après une intervention de l'utilisateur ou un délai configurable.

Types d'options de configuration
BCP a un ensemble distinct d'options de configuration, qui sont définies dans le présent document.

4.1 Envoi des trames de pont

Avant que tout trafic de LAN ponté ou BPDU puissent être communiqués, PPP DOIT atteindre la phase Protocole de couche réseau, et le protocole de contrôle de pontage DOIT atteindre l'état Ouvert.

Exactement un trafic de LAN ponté ou BPDU est encapsulé dans le champ Informations PPP, où le champ Protocole PPP indique en hexadécimal le type 0031 (PDU pontée).

4.1.1 Considérations sur l'unité de réception maximum

La longueur maximum d'un datagramme ponté transmis sur une liaison PPP est la même que la longueur maximum du champ Informations d'un paquet PPP encapsulé. Comme il n'y a pas de méthode standard pour fragmenter et réassembler les PDU pontées, les liaisons PPP qui prennent en charge le pontage DOIVENT négocier une MRU assez grande pour prendre en charge les types de MAC qui sont ensuite négociés pour la prise en charge du pontage. Parce qu'elles incluent les en-têtes MAC, même les trames Ethernet pontées sont plus grandes que la MRU PPP par défaut de 1500 octets.

4.1.2 Surveillance de bouclage et de qualité de liaison

Il est vivement recommandé que les mises en œuvre du protocole de pont PPP utilisent la détection de bouclage de numéro magique et la surveillance de qualité de liaison. Le protocole d'arbre d'expansion 802.1, qui est intégré au pontage transparent et à l'acheminement de source (comme normalisés) est unidirectionnel en fonctionnement normal. Les BPDU de configuration émanent du système racine dans la direction générale des feuilles, sans aucun trafic inverse sauf en réponse aux événements du réseau.

4.1.3 Séquence de messages

Le cas de la liaison multiple exige de prendre en compte la séquence des messages. Le système émetteur peut déterminer si le protocole qui est ponté exige que les transmissions arrivent dans l'ordre de leur transmission d'origine, et met à la file toutes les transmissions sur une certaine conversation sur la même liaison pour forcer la préservation de l'ordre, ou que le protocole N'EXIGE PAS que les transmissions arrivent dans l'ordre de leur transmission originale, et utilise cette connaissance pour optimiser l'utilisation de plusieurs liaisons, mettant en file le trafic sur plusieurs liaisons pour minimiser les délais.

En l'absence d'une telle détermination, le système émetteur DOIT agir comme si tous les protocoles exigeaient la préservation de l'ordre. De nombreux protocoles conçus principalement pour être utilisés sur un seul LAN exigent la préservation de l'ordre.

PPP multi liaison [RFC1990] et son extension multi classes [RFC2686] peut être utilisé pour permettre l'utilisation de plusieurs liaisons PPP entre une paire de systèmes sans perte de la séquentialité des messages. Il traite le groupe de liaisons comme une seule liaison avec une vitesse égale à la somme des vitesses des liaisons dans le groupe.

4.1.4 Séparation des domaines d'arborescence

Il est concevable qu'un gestionnaire de réseau puisse souhaiter inhiber l'échange des BPDU sur une liaison afin de diviser logiquement deux régions en des arbres d'expansion séparés avec des racines différentes (et éventuellement des mises en œuvre ou algorithmes d'arbre d'expansion différents). Pour ce faire, il devrait configurer les deux extrémités à ne pas échanger de BPDU sur une liaison. Une mise en œuvre qui ne prend pas en charge de protocole d'arbre d'expansion DOIT éliminer en silence tout paquet de BPDU IEEE 802.1D reçu.

Si un pont est connecté à un vieux pont BCP [RFC1638], l'autre pont ne peut pas fonctionner selon la présente

spécification. Les options sont donc de décider que :

(a) Si le pont veut terminer la connexion, il envoie une Demande de fin et termine la connexion.

(b) Si le pont veut faire fonctionner la connexion mais pas recevoir de vieilles BPDU, sa seule option est de fonctionner sans arbre d'expansion du tout sur la liaison, ce qui est dangereux. Il devrait faire Configure-Reject sur l'option et aviser l'administration du réseau de ce qu'il a fait.

(c) Si le pont choisit d'être entièrement rétro compatible, il envoie Configure-Ack et opère de la façon décrite à l'Appendice A.

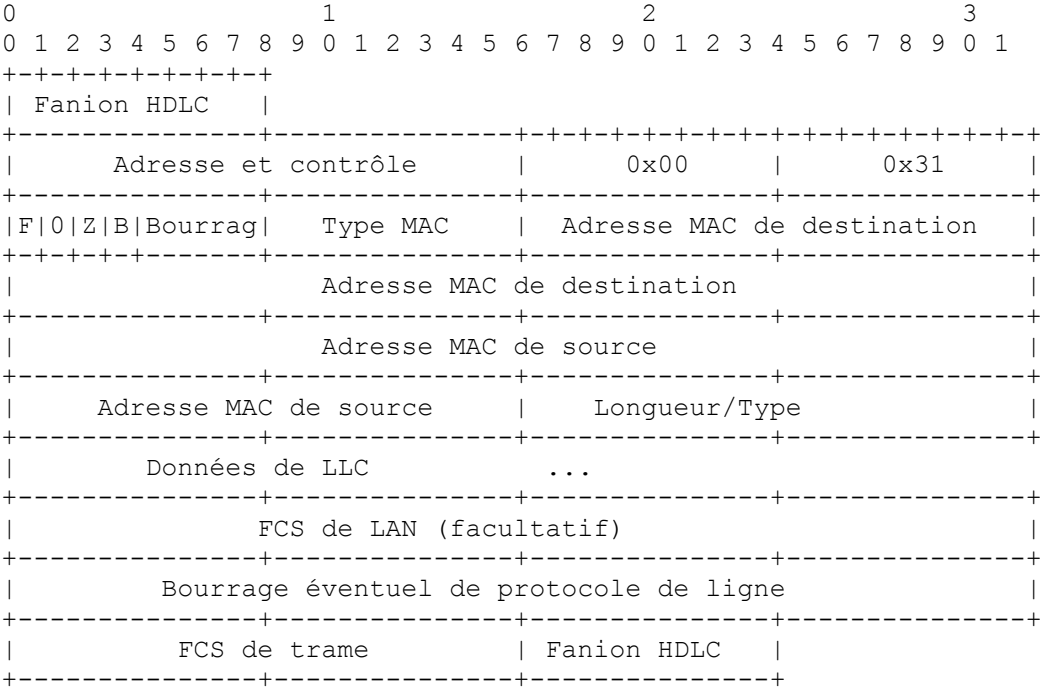
Dans le cas où les deux options nouvelles Management-Inline *(Gestion en ligne)* et Spanning-Tree-Protocol-Configuration *(Configuration de protocole d'arbre d'expansion)* sont en rejet de configuration, ce qui indique que l'homologue ne met en œuvre aucun protocole d'arbre d'expansion et ne comprend pas les options, c'est une mise en œuvre incomplète. Pour des raisons de sécurité, le système devrait cesser de tenter de configurer des ponts, et noter le fait dans le journal. Si l'homologue a rejeté la configuration des options afin de désactiver entièrement l'arbre d'expansion, il comprend l'option mais n'a pas pu se conformer à la configuration. Il aurait du envoyer l'option Spanning-Tree-Protocol-Configuration avec la valeur NUL.

Les mises en œuvre DEVRAIT mettre en œuvre un mode rétro compatibilité.

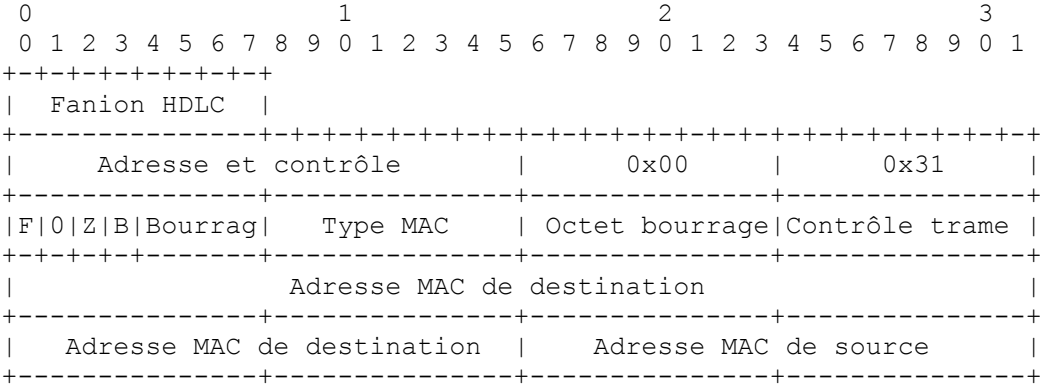
4.2 Trafic de LAN ponté (trame IEEE 802 non étiquetée)

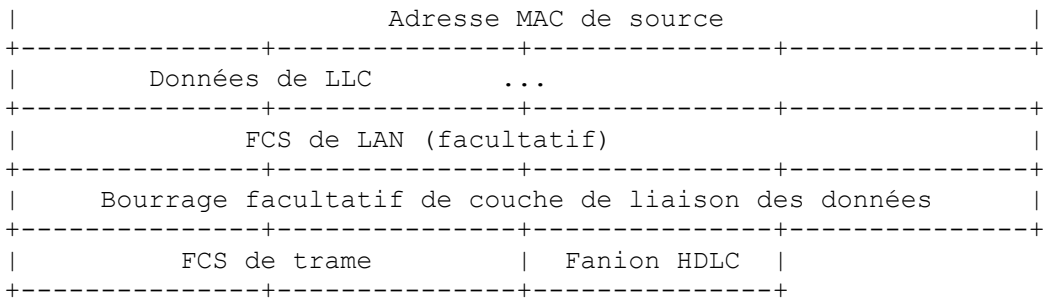
Pour le trafic de LAN ponté, le format de la trame sur la ligne est montré ci-dessous. Ce format est utilisé si le trafic ne comporte pas d'identifiant de VLAN et de priorité. Les champs sont transmis de gauche à droite.

Format de trame 802.3 (trame IEEE 802 non étiquetée)



Format de trame 802.4/802.5/FDDI (trame IEEE 802 non étiquetée)





Adresse et contrôle : comme défini par le tramage utilisé.

Protocole PPP : 0x0031 pour le pontage PPP.

Fanions
bit F : à 1 si le champ FCS de LAN est présent.
bit 0 : réservé, doit être zéro.
bit Z : à 1 si le bourrage IEEE 802.3 doit être rempli de zéros jusqu'à la taille minimum.
bit B : à 1 si la trame est un paquet de contrôle de pont. Voir les détails au paragraphe 3.5.

Bourrages : toute trame PPP peut avoir un bourrage inséré dans le champ "Bourrage facultatif de couche de liaison des données". Ce nombre dit au système receveur combien d'octets de bourrage supprimer.

Type MAC : les valeurs actuelles du champ Type MAC sont spécifiés dans la plus récente RFC "Numéros alloués" [RFC3232]. Les valeurs actuelles sont allouées comme suit :

0 : réservé
1 : IEEE 802.3/Ethernet avec adresses canoniques
2 : IEEE 802.4 avec adresses canoniques
3 : IEEE 802.5 avec adresses non canoniques
4 : FDDI avec adresses non canoniques
5 à 10 : réservé
11 : IEEE 802.5 avec adresses canoniques
12 : FDDI avec adresses canoniques

"Canonique" est le format d'adresse défini comme représentation d'adresse standard par l'IEEE. Dans ce format, le bit au sein de chaque octet qui est à transmettre en premier sur un LAN est représenté comme le bit de moindre poids. À l'opposé, dans une forme non canonique, le bit au sein de chaque octet qui est à transmettre en premier est représenté comme le bit de poids fort. De nombreuses mises en œuvre d'interface de LAN utilisent la forme non canonique. Dans les deux formats, les octets sont représentés dans l'ordre de transmission.
Si une mise en œuvre prend en charge un type MAC qui est le format du numéro le plus élevé de ce type MAC, il DOIT alors aussi prendre en charge le format de numéro inférieur de ce type MAC. Par exemple, si une mise en œuvre prend en charge FDDI avec le format d'adresse canonique, il DOIT alors aussi prendre en charge FDDI avec le format d'adresse non canonique. L'objet de cette exigence est d'assurer la rétro compatibilité avec les versions antérieures de la présente spécification.
Un système NE DOIT PAS transmettre un type MAC d'un numéro supérieur à 4 sauf si il a reçu de son homologue une option de configuration MAC-Support qui indique que l'homologue veut recevoir des trames de ce type MAC.

Contrôle trame
Sur les LAN 802.4, 802.5, et FDDI, il y a quelques octets qui précèdent l'adresse MAC de destination, dont l'un est protégé par la FCS. Le type MAC de la trame détermine le contenu du champ Contrôle de trame. Un octet de bourrage est présent pour assurer l'alignement sur 32 bits.

Adresse MAC de destination : Comme défini par l'IEEE. Le champ Type MAC définit l'ordre des bits.

Adresse MAC de source : Comme défini par l'IEEE. Le champ Type MAC définit l'ordre des bits.

Données de LLC
C'est le reste de la trame MAC qui est (ou serait s'il était présent) protégé par la FCS de LAN. Par exemple, le champ Contrôle d'accès 802.5, et l'en-queue d'état ne sont pas significatifs pour être transmis à un autre anneau, et sont omis.

FCS de LAN
Si présent, c'est la FCS de LAN qui a été calculée par (ou qui paraît avoir été calculée par) la station d'origine. Si le fanion FCS de LAN n'est pas établi, ce champ n'est alors pas présent, et la PDU fait quatre octets de moins.

Bourrage facultatif de couche de liaison des données
Toute trame PPP peut avoir un bourrage inséré entre le champ Informations et la FCS de trame. Le champ Bourrage contient la longueur de ce bourrage, qui ne peut pas excéder 15 octets.
Les extensions LCP à PPP [RFC1570] spécifient un bourrage auto descriptif. Les mises en œuvre sont invitées à régler le champ Bourrage à zéro, et à utiliser à la place le bourrage auto descriptif.

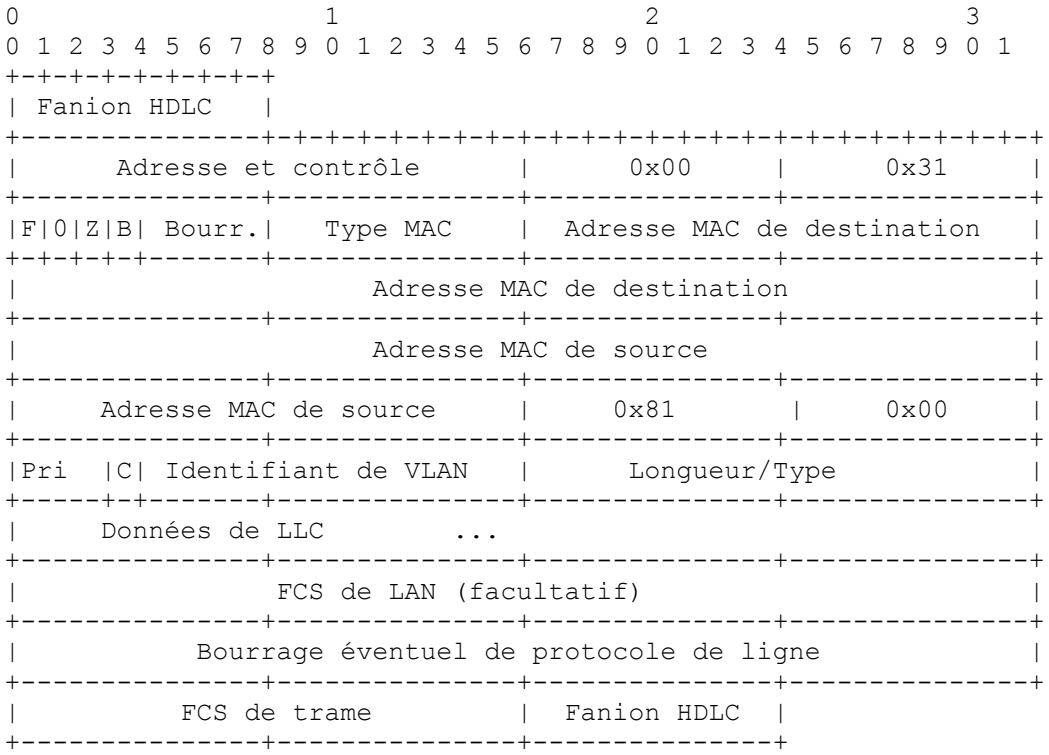
FCS de trame
Mentionné surtout à des fins de clarté. La FCS utilisée sur la liaison PPP est différente de la FCS de LAN et sans relation avec elle.

4.3 Trafic de LAN ponté dans une trame IEEE 802 étiquetée

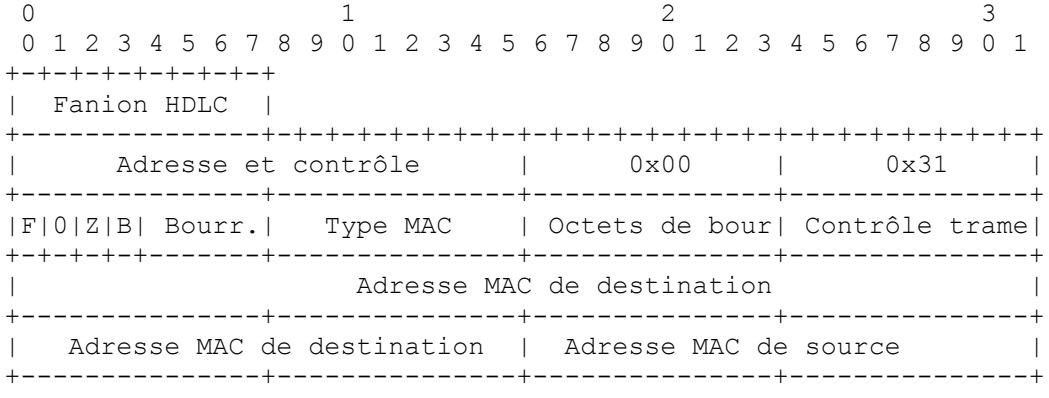
Pour connecter deux segments de LAN virtuel ou plus, la trame DOIT inclure son identifiant de VLAN et sa priorité. Une trame étiquetée IEEE 802 peut être utilisée si l'option IEEE-802-Tagged-Frame est acceptée par l'homologue. Le format de la trame sur la ligne est montré ci-dessous.

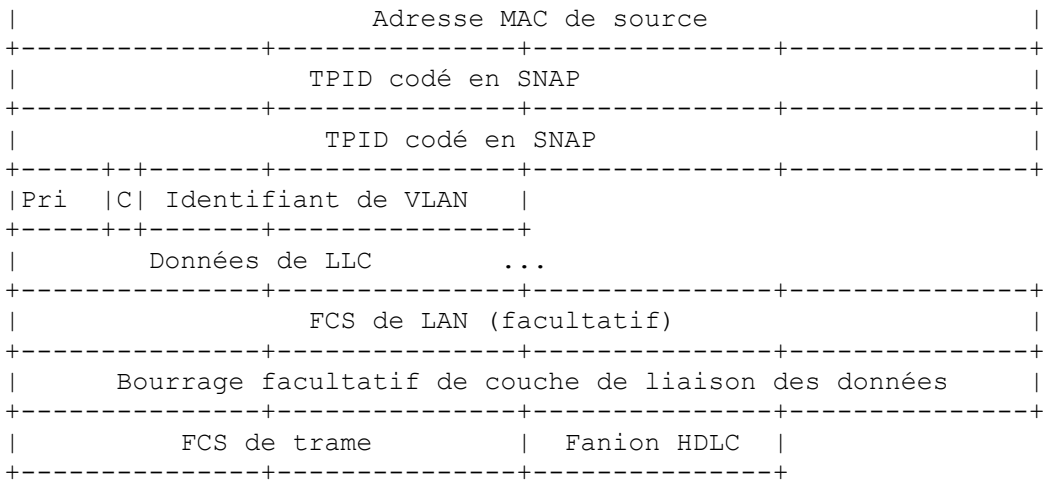
Les champs sont transmis de gauche à droite.

Format de trame 802.3 (trame IEEE 802 étiquetée)



Format de trame 802.4/802.5/FDDI (trame IEEE 802 étiquetée)





Adresse et contrôle : comme défini par le tramage utilisé.

Protocole PPP : 0x0031 pour le pontage PPP

Fanions
bit F : établi si le champ FCS de LAN est présent
bit 0 : réservé, doit être zéro
bit Z : établi si le bourrage IEEE 802.3 doit être rempli de zéro à la taille minimum
bit B : établi si la trame est un paquet de contrôle de pont. Voir les détails au paragraphe 3.5.

Bourrages
Toute trame PPP peut avoir un bourrage inséré dans le champ "Bourrage facultatif de couche de liaison des données". Ce nombre dit au système receveur combien d'octets de bourrage supprimer.

Type MAC
Les valeurs à jour du champ Type MAC sont spécifiées dans la plus récente RFC "Numéros alloués" [RFC3232]. Les valeurs actuellement allouées sont les suivantes :

0 : réservé
1 : IEEE 802.3/Ethernet avec adresses canoniques
2 : IEEE 802.4 avec adresses canoniques
3 : IEEE 802.5 avec adresses non canoniques
4 : FDDI avec adresses non canoniques
5 à 10 : réservé
11 : IEEE 802.5 avec adresses canoniques
12 : FDDI avec adresses canoniques

"Canonique" est le format d'adresse défini comme représentation d'adresse standard par l'IEEE. Dans ce format, le bit au sein de chaque octet qui est à transmettre en premier sur un LAN est représenté comme le bit de moindre poids. À l'opposé, dans une forme non canonique, le bit au sein de chaque octet qui est à transmettre en premier est représenté comme le bit de poids fort. De nombreuses mises en œuvre d'interface de LAN utilisent la forme non canonique. Dans les deux formats, les octets sont représentés dans l'ordre de transmission.
Si une mise en œuvre prend en charge un type MAC qui est le format du numéro le plus élevé de ce type MAC, il DOIT alors aussi prendre en charge le format de numéro inférieur de ce type MAC. Par exemple, si une mise en œuvre prend en charge FDDI avec le format d'adresse canonique, il DOIT alors aussi prendre en charge FDDI avec le format d'adresse non canonique. L'objet de cette exigence est d'assurer la rétro compatibilité avec les versions antérieures de la présente spécification.
Un système NE DOIT PAS transmettre un type MAC d'un numéro supérieur à 4 sauf si il a reçu de son homologue une option de configuration MAC-Support qui indique que l'homologue veut recevoir des trames de ce type MAC.

Contrôle trame
Sur les LAN 802.4, 802.5, et FDDI, il y a quelques octets qui précèdent l'adresse MAC de destination, dont l'un est protégé par la FCS. Le type MAC de la trame détermine le contenu du champ Contrôle de trame. Un octet de bourrage est présent pour assurer l'alignement sur 32 bits.

Adresse MAC de destination : Comme défini par l'IEEE. Le champ Type MAC définit l'ordre des bits.

Adresse MAC de source : Comme défini par l'IEEE. Le champ Type MAC définit l'ordre des bits.

Données de LLC
C'est le reste de la trame MAC qui est (ou serait s'elle était présente) protégé par la FCS de LAN. Par exemple, le champ Contrôle d'accès 802.5, et l'en-queue d'état ne sont pas significatifs pour être transmis à un autre anneau, et sont omis.

FCS de LAN
Si présent, c'est la FCS de LAN qui a été calculée par (ou qui paraît avoir été calculée par) la station d'origine. Si le fanion FCS de LAN n'est pas établi, ce champ n'est alors pas présent, et la PDU fait quatre octets de moins.

Pri : valeur de priorité sur trois bits comme défini par IEEE 802.1D.

C : fanion canonique comme défini par IEEE 802.1Q. Il doit être établi si les données de RIF sont présentes dans les données de LLC.

Identifiant de VLAN : identifiant de VLAN de 12 bits comme défini par IEEE 802.1Q.

Données de LLC
C'est le reste de la trame MAC qui est (ou le serait si elle était présente) protégée par la FCS de LAN. Par exemple, le champ Contrôle d'accès 802.5, et l'en-queue d'état n'ont pas de signification pour une transmission à un autre anneau, et sont omis.

FCS de LAN
Si elle est présente, c'est la FCS du LAN qui a été calculée par (ou qui paraît avoir été calculée par) la station d'origine. Si la FCS de LAN n'est pas établie, ce champ n'est alors pas présent, et la PDU est plus courte de quatre octets.

Bourrage facultatif de couche de liaison des données
Toute trame PPP peut avoir un bourrage inséré entre le champ Information et la FCS de trame. Le champ Bourrage contient la longueur de ce bourrage, qui ne doit pas excéder 15 octets.
Les extensions LCP à PPP [RFC1570] spécifient un bourrage auto descriptif. Les mises en œuvre sont invitées à régler le champ Bourrage à zéro, et à utiliser à la place le bourrage auto descriptif.

FCS de trame
Mentionné surtout à des fins de clarté. La FCS utilisée sur la liaison PPP est différente de la FCS de LAN et sans relation avec elle.

4.4 Protocole de pont et protocoles GARP

Pour éviter des boucles de réseau et améliorer la redondance, les ponts échangent une unité de données de protocole d'arbre d'expansion appelée une BPDU. Les ponts échangent aussi une unité de données de protocole d'enregistrement d'attributs génériques pour porter les données du protocole d'enregistrement de VLAN GARP (GVRP, *GARP VLAN Registration Protocol*) et du protocole d'enregistrement de diffusion groupée GARP (GMRP, *GARP Multicast Registration Protocol*). GVRP permet aux ponts de créer des groupes de VLAN de façon dynamique. GMRP permet aux ponts de filtrer les données en diffusion groupée si le receveur est absent du réseau. Ces protocoles de pont incluent le protocole d'arbre d'expansion et les unités de données des protocoles GARP sont portées avec une adresse de destination spéciale assignée par l'IEEE.

Ces unités de données de protocoles de pont et les unités de données de protocole GARP doivent être portées dans le format de trame indiqué aux paragraphes 4.2 ou 4.3. Le pont qui reçoit ces unités de données identifie ces protocoles sur la base de l'adresse de destination dans le format de trame, tout comme le fonctionnement de la réception de trames d'un segment de LAN.

Les unités de données de protocoles de pont et de protocoles GARP DOIVENT être reconnues en vérifiant les adresses de destination, qui sont assignées par l'IEEE.

01-80-c2-00-00-00	adresse de groupe de ponts (utilisé par STP)
01-80-c2-00-00-01	norme IEEE 802.3x fonctionnement de PAUSE en bidirectionnel
01-80-c2-00-00-10	adresse de groupe de gestion de pont
01-80-c2-00-00-20	protocole d'enregistrement de diffusion groupée GARP (GMRP)
01-80-c2-00-00-21	protocole d'enregistrement de VLAN GARP (GVRP)

Mais il y a une exception à cette règle : si le pont est connecté à un ancien pont BCP [RFC1638] et peut prendre en charge la rétro compatibilité, il DOIT envoyer la BPDU dans l'ancien format décrit en Appendice A.

5. Options de configuration de BCP

Les options de configuration de BCP permettent des modifications aux caractéristiques standard du protocole de couche réseau à négocier. Si une option Configuration n'est pas incluse dans un paquet Demande de configuration, la valeur par défaut pour cette option de configuration est supposée.

BCP utilise le même format d'option de configuration que défini pour LCP [RFC1661], avec un ensemble séparé d'options.

Les valeurs à jour du champ Type d'option BCP sont spécifiées dans la plus récente RFC "Numéros alloués" [RFC3232]. Les valeurs allouées actuellement sont les suivantes :

1 Identification de pont
2 Identification de ligne
3 Prise en charge de MAC
4 Compression Tinygram
5 Identification de LAN (obsolète)
6 Adresse MAC
7 Protocole d'arbre d'expansion (ancien format)
8 Trame IEEE 802 étiquetée
9 Gestion en ligne
10 Indicateur de paquet de contrôle de pont

5.1 Identification de pont

Description
L'option de configuration Identification de pont est conçue pour être utilisée lorsque la ligne est une interface entre des demi ponts qui connectent des segments de LAN virtuel ou physique. Comme ces ponts distants sont modélisés comme un seul pont avec une interface interne étrange, chaque pont distant a besoin de savoir les numéros de segment de LAN et de pont du pont distant adjacent. Cette option NE DOIT PAS être incluse dans la même demande de configuration que l'option Identification de ligne.

Le descripteur de chemin d'acheminement de source et son utilisation sont spécifiés par l'Appendice IEEE 802.1D sur l'acheminement de source. Il identifie le segment auquel l'interface est rattachée par son numéro de segment configuré, et lui-même par le numéro de pont sur le segment.

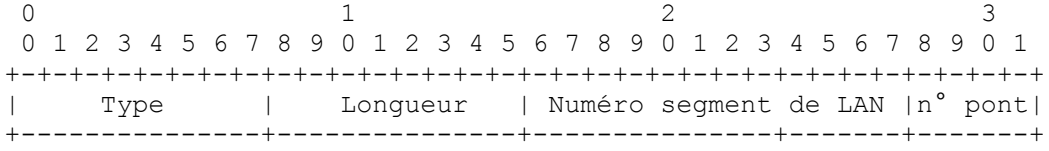
Les deux demi ponts DOIVENT se mettre d'accord sur le numéro de pont. Si un numéro de pont n'a pas fait l'objet d'un accord, le protocole de contrôle de pont NE DOIT PAS entrer dans l'état Ouvert.

Comme des numéros de pont discordants indiquent une erreur de configuration, une configuration correcte exige que le pont soit déclare la discordance de configuration, soit choisisse une des options. Pour permettre à deux systèmes de passer à l'état Ouvert en dépit d'une discordance, un système PEUT changer son numéro de pont en faveur du plus élevé des deux numéros. Un système avec un numéro plus élevé NE DOIT PAS changer son numéro de pont pour un numéro moins élevé. Il devrait, cependant, informer dans tous les cas l'administration du réseau de la malformation.

Par défaut, un système qui ne négocie pas cette option est supposé être configuré à ne pas utiliser le modèle des deux systèmes comme deux moitiés d'un seul pont de route de source. Il est plutôt supposé être configuré à utiliser le modèle des deux systèmes comme ponts indépendants.

ExempleSi le système A annonce le segment de LAN AAA, le pont n° 1, et si le système B annonce le segment de LAN BBB, le pont n° 1, la configuration d'acheminement de source résultante (lue dans la direction appropriée) est alors AAA,1,BBB.

Un sommaire du format de l'option Identification de pont est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 1

Longueur : 4

Numéro de segment de LAN
Numéro de 12 bits identifiant le segment de LAN, comme défini dans la spécification IEEE 802.1D d'acheminement de source.

n° de pont
Numéro de 4 bits identifiant le pont sur le segment de LAN, comme défini dans la spécification IEEE 802.1D d'acheminement de source.

5.2 Identification de ligne

Description
L'option de configuration Identification de ligne est conçue pour être utilisée lorsque la ligne a reçu un numéro de segment de LAN bien que ce soit un segment de LAN à deux systèmes conformément à l'algorithme d'acheminement de source.

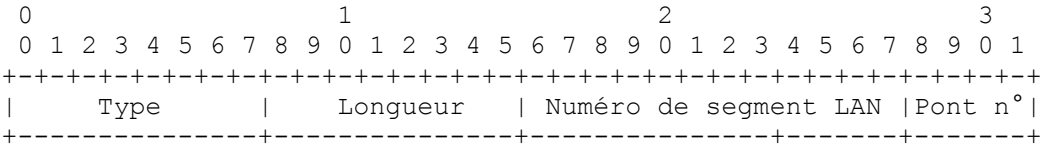
Le descripteur de chemin d'acheminement de source et son utilisation sont spécifiés par l'Appendice sur l'acheminement de source de la norme IEEE 802.1D. Elle identifie le segment auquel est rattachée l'interface par son numéro de segment configuré, et lui-même par le numéro de pont sur le segment.

Les deux ponts DOIVENT s'accorder sur le numéro de segment de LAN. Si il n'y a pas d'accord sur un numéro de segment de LAN, le protocole de contrôle de pontage NE DOIT PAS entrer dans l'état Ouvert.

Comme des numéros de segment de LAN discordants indiquent une erreur de configuration, une configuration correcte exige soit que le pont déclare la mauvaise configuration, soit choisisse une des options. Pour permettre que deux systèmes passent à l'état Ouvert en dépit d'une discordance, un système PEUT changer son numéro de segment de LAN pour prendre le plus élevé des deux numéros. Un système de numéro plus élevé NE DOIT PAS changer son numéro de segment de LAN pour un numéro inférieur. Il devrait cependant, informer dans tous les cas l'administration du réseau de la mauvaise configuration.

Par défaut, un système qui ne négocie pas cette option est supposé avoir son numéro de segment de LAN correctement configuré par l'utilisateur.

Un sommaire du format de l'option Identification de ligne est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 2

Longueur : 4

Numéro de segment de LAN
Numéro de 12 bits qui identifie le segment de LAN, comme défini dans la spécification IEEE 802.1D.

Pont n°
Numéro de 4 bits qui identifie le pont sur le segment de LAN, comme défini dans la spécification IEEE 802.1D.

5.3 Prise en charge de MAC

Description
L'option de configuration Prise en charge de MAC est fournie pour permettre aux mises en œuvre d'indiquer la sorte de trafic qu'elles sont prêtes à recevoir. La négociation de cette option est fortement recommandée.

Par défaut, lorsque une mise en œuvre n'annonce pas les types de MAC qu'elle prend en charge, l'homologue envoie tous les types de MAC qu'il est capable de transporter étant donnés les autres paramètres de configuration. Le receveur va éliminer les types de MAC qu'il ne prend pas en charge.

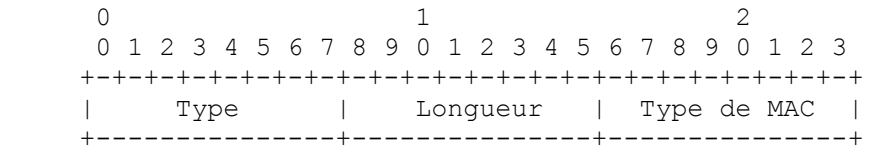
Un appareil qui prend en charge une MRU de 1600 octets peut ne pas vouloir prendre en charge 802.5, 802.4 ou FDDI, qui prennent chacun en charge des trames de plus de 1600 octets.

En annonçant les types de MAC qu'elle prend en charge, une mise en œuvre avise son homologue que tous les types de MAC non spécifiés seront éliminés. L'homologue PEUT alors réduire l'utilisation de la bande passante en n'envoyant pas les types de MAC non pris en charge.

L'annonce de la prise en charge de plusieurs types de MAC est réalisée en plaçant plusieurs options dans la demande de configuration.

La nature de cette option est seulement indicative. Cette option NE DOIT PAS être incluse dans un Configure-Nak.

Un sommaire du format de l'option Prise en charge de MAC est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 3

Longueur : 3

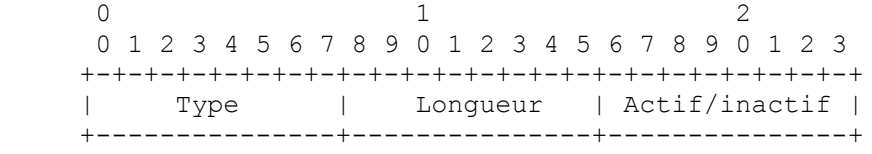
Type de MAC
Une des valeurs du champ Type MAC (décrit précédemment au paragraphe 4.3) que ce système est prêt à recevoir et à servir.

5.4 Compression Tinygram

Description
Cette option de configuration permet à la mise en œuvre d'indiquer la prise en charge de la compression Tinygram.
Tous les systèmes ne sont pas prêts à faire des modifications aux messages en transit. Sur les lignes à haut débit, cela n'en vaut probablement pas la peine.

Cette option NE DOIT PAS être incluse dans un Configure-Nak si elle a été reçue dans une demande de configuration. Cette option PEUT être incluse dans un Configure-Nak afin de d'inviter l'homologue à envoyer l'option dans sa prochaine demande de configuration.

Par défaut, aucune compression n'est permise. Un système qui ne négocie pas, ou négocie la désactivation de cette option, ne devrait jamais recevoir un paquet compressé.
Un sommaire du format de l'option Compression Tinygram est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 4
Longueur : 3
Actif/inactif : si la valeur est 1, la compression Tinygram est activée. Si la valeur est 2, la compression Tinygram est désactivée, et aucune décompression ne sera faite. Les mises en œuvre n'ont pas besoin de se mettre d'accord sur l'établissement de ce paramètre. L'un peut vouloir décompresser et pas l'autre.

5.5 Adresse MAC

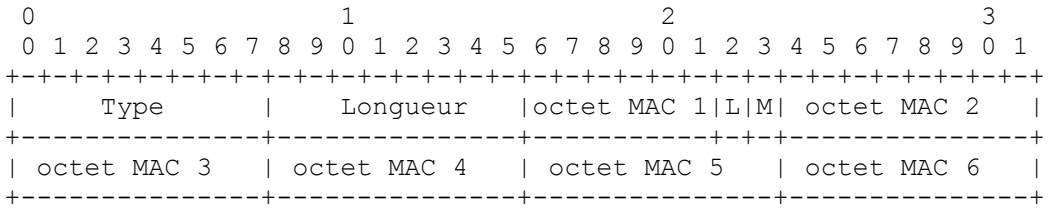
Description
L'option de configuration Adresse MAC permet à la mise en œuvre d'annoncer son adresse MAC ou d'en avoir une allouée. L'adresse MAC est représentée en format canonique IEEE 802.1, qui dit que le bit de diffusion groupée est le bit de moindre poids du premier octet de l'adresse.

Si le système souhaite annoncer son adresse MAC, il envoie l'option avec son adresse MAC spécifiée. Lorsque on spécifie une adresse MAC non à zéro dans une demande de configuration, toute inclusion de cette option dans un Configure-Nak DOIT être ignorée.

Si la mise en œuvre souhaite avoir une adresse MAC allouée, elle envoie l'option avec l'adresse MAC de 00-00-00-00-00-00. Les systèmes qui n'ont pas de mécanisme d'allocation d'adresse vont faire Configure-Reject sur l'option.

Un Configure-Nak DOIT spécifier une adresse physique en format IEEE 802.1 valide ; le bit de diffusion groupée DOIT être à zéro. Il est fortement recommandé (bien que non obligatoire) que le bit "adresse allouée en local" (le second bit de moindre poids du premier octet) soit établi, indiquant une adresse allouée en local.

Un sommaire de l'option Adresse MAC est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 6

Longueur : 8

octet MAC
Six octets d'adresse MAC dans l'ordre canonique 802.1. Pour être clair, la position des bits Allocation locale (L) et Diffusion groupée (M) est montrée sur le diagramme.

5.6 Protocole d'arbre d'expansion (ancien format)

Description
La configuration de protocole d'arbre d'expansion permet à un pont de rester compatible avec de plus anciennes mises en œuvre de BCP [RFC1638]. Cette option de configuration est cependant incompatible avec l'option de gestion en ligne, qui permet à un pont de mettre en œuvre les nombreux protocoles dont l'IEEE s'attend maintenant qu'un pont soit capable d'utiliser.

Si l'homologue rejette l'option de configuration Gestion en ligne, en envoyant un configure-reject, il doit être une mise en œuvre de la [RFC1638], qui est décrite dans l'Appendice A. Le système peut facultativement terminer la négociation ou offrir de négocier de cette manière.

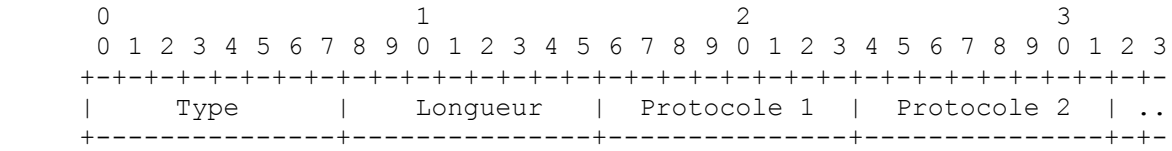
Dans ce cas, si les deux ponts prennent en charge un protocole d'arbre d'expansion, ils DOIVENT se mettre d'accord sur le protocole à prendre en charge. La vieille BPDU décrite dans l'Appendice A DOIT être utilisée plutôt que le format montré aux paragraphes 4.2 ou 4.3. Lorsque les deux ne tombent pas d'accord, le protocole de plus faible numéro des deux protocoles d'arbre d'expansions devrait être utilisé. Pour résoudre le conflit, le système qui a le protocole de plus faible numéro DEVRAIT faire un Configure-Nak pour l'option, suggérant l'utilisation de son propre protocole. Si un protocole d'arbre d'expansion ne fait pas l'accord, sauf pour le cas où un système ne prend en charge aucun protocole d'arbre d'expansion, le protocole de contrôle de pont NE DOIT PAS entrer dans l'état Ouvert.

La plupart des systèmes vont seulement participer à un seul protocole d'arbre d'expansion. Si un système souhaite participer simultanément à plus d'un protocole d'arbre d'expansion, il PEUT inclure tous les types appropriés de protocole dans une seule option de configuration Protocole d'arbre d'expansion. Les types de protocole DOIVENT être spécifiés en

ordre numérique croissant. Pour les besoins de comparaison durant la négociation, les numéros de protocole DOIVENT être considérés comme étant un seul nombre. Par exemple, si le système A inclut les protocoles 01 et 03 et si le système B indique les protocole 03, le système B devrait faire un Configure-Nak et indiquer un type de protocole de 03 car 0103 est supérieur à 03.

Par défaut, une mise en œuvre DOIT prendre en charge soit le protocole IEEE 802.1D d'arbre d'expansion, soit ne prendre en charge aucun protocole d'arbre d'expansion. Une mise en œuvre qui ne prend en charge aucun protocole d'arbre d'expansion DOIT éliminer en silence tout paquet de BPDU IEEE 802.1D reçu, et DOIT soit éliminer en silence, soit répondre aux autres paquets de BPDU reçus avec un paquet LCP Protocol-Reject dans ce cas.

Un sommaire du format de l'option Protocole d'arbre d'expansion est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 7

Longueur : 2 octets plus 1 octet supplémentaire pour chaque protocole qui sera activement pris en charge. La plupart des systèmes vont seulement prendre en charge un seul protocole d'arbre d'expansion, résultant en une longueur de 3.

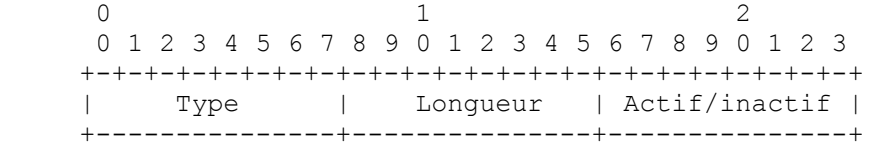
Protocole n
Chaque champ Protocole fait un octet et indique un protocole d'arbre d'expansion désiré. Les valeurs du champ Protocole d'arbre d'expansion à ce jour sont spécifiées comme des nombres DLL PPP dans la plus récente version de la RFC "Numéros alloués" [RFC3232]. Les valeurs actuellement allouées sont les suivantes :

Valeur	**Protocole**
0	Nul (aucun protocole d'arbre d'expansion n'est pris en charge)
1	arbre d'expansion IEEE 802.1D
2	protocole d'arbre d'expansion IEEE 802.1G étendu
3	protocole d'arbre d'expansion d'acheminement de source IBM
4	protocole d'arbre d'expansion DEC LANbridge 100

5.7 Trame IEEE-802 étiquetée

Description
Cette option de configuration permet à la mise en œuvre d'indiquer la prise en charge de la trame étiquetée IEEE 802. La négociation de cette option est fortement recommandée.
Un appareil qui prend en charge la trame étiquetée IEEE 802 doit vouloir prendre en charge la trame étiquetée IEEE 802 montrées au paragraphe 4.3.
Par défaut, la trame étiquetée IEEE 802 n'est pas prise en charge. Un système qui ne négocie pas, ou négocie que cette option soit désactivée, ne devrait jamais recevoir de trame étiquetée IEEE 802.

Un sommaire du format de l'option Trame étiquetée IEEE 802 est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 8
Longueur : 3

Actif/inactif
Si la valeur est 1, la trame étiquetée IEEE-802 est activée. Si la valeur est 2, la trame étiquetée IEEE-802 est désactivée, et NE DOIT PAS envoyer de paquet IEEE-802 à trame étiquetée.

5.8 Gestion en ligne

Description
L'option de configuration Gestion en ligne indique que le système veut recevoir tout protocole inter pont défini par l'IEEE, comme des unités de données de protocole de pont et des unités de données de protocole GARP, dans le format de trame montré au paragraphe 4.2 ou 4.3.

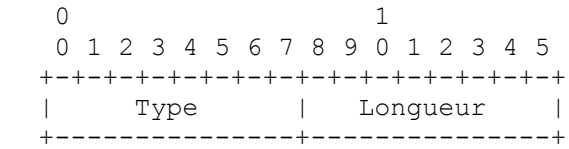
Les vielles mises en œuvre de BCP [RFC1638] vont utiliser la procédure de négociation décrite au paragraphe 5.6. Les mises en œuvre de cette procédure vont utiliser cette option pour indiquer la conformité au nouveau BCP et peuvent facultativement négocier la procédure du paragraphe 5.6, soit sur la même demande de configuration, soit en réponse à un configure-reject. Il est recommandé que seule la demande de configuration affiche cette option lorsque elle est pertinente, et qu'elle réponde par l'option Protocole d'arbre d'expansion (ancien format) si un configure-reject est reçu, comme dans le cas normal, on peut s'attendre à ce que ce soit la négociation la plus rapide.

Si un système reçoit une demande de configuration qui offre les deux solutions, il devrait accepter cette procédure et rejeter l'option Protocole d'arbre d'expansion (vieux format).

On peut s'attendre à ce que les mises en œuvre du vieux BCP [RFC1638] ne comprennent pas l'option et produisent un configure-reject.

Par défaut, la gestion en ligne n'est pas permise. Un système qui ne négocie pas, ou négocie que cette option soit désactivée, ne devrait jamais recevoir d'unité de données de protocole de pont ou d'unité de données de protocole GARP en ligne.

Un sommaire du format de l'option Gestion en ligne est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 9

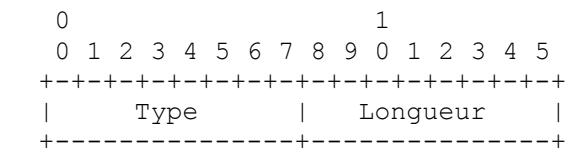
Longueur : 2

5.9 Indicateur de paquet de contrôle de pont

Description
Cette option de configuration permet à la mise en œuvre d'indiquer qu'elle prend en charge l'indicateur de paquet de contrôle de pont. La négociation de cette option est fortement recommandée.
Par défaut, l'indicateur de paquet de contrôle de pont n'est pas pris en charge. Négocier cette option permet l'indicateur de paquet de contrôle de pont. Ne pas négocier cette option désactive l'indicateur de paquet de contrôle de pont.

Un système qui ne négocie pas ne DOIT jamais envoyer ou recevoir de trame avec le bit Indicateur de paquet de contrôle de pont réglé à 1.

Un sommaire du format de l'option Indicateur de paquet de contrôle de pont est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 10

Longueur : 2

6. Changements par rapport à la RFC2878

Cette section énumère les changements faits à la vieille [RFC2878] pour produire le présent document.
1 – Ajout de l'indicateur de paquet de contrôle de pont à l'option de configuration.
2 – Modification de la signification d'un des bits réservés du champ Fanions.

7. Considérations pour la sécurité

Ce protocole de contrôle réseau *(NCP, network control protocol)* compare la configurations de deux appareils et cherche à négocier un sous ensemble acceptable de leur intersection, pour permettre un interfonctionnement correct même en présence de différences mineures de configuration ou de mise en œuvre. Dans le cas de détection de différences majeures de configuration, la négociation ne pourra pas être menée à bien, résultant en la clôture de la liaison ou en son non établissement. Il est possible que si une liaison pontée est établie avec un homologue malveillant, des informations sur le réseau puissent être acquises à partir du trafic de diffusion groupée transmis, ou que des attaques de déni de service soient créées en établissant des boucles qui devraient être détectées et isolées ou en offrant des contenus malveillants.

De telles attaques ne sont pas propres à ce NCP ; tout NCP PPP est soumis à attaque lors de la connexion à un appareil étranger ou compromis. Cependant, aucune situation ne survient qui ne soit pas commune à tous les NCP ; tout NCP activé avec un homologue malveillant est soumis à de l'espionnage et autres attaques. Il est donc recommandé que les liaisons sur lesquelles cela peut arriver soient configurées à utiliser l'authentification PPP durant la phase de démarrage LCP.

8. Déclaration de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

9. Considérations relatives à l'IANA

Le présent document propose qu'un nouveau numéro d'option BCP soit enregistré par l'IANA. Cette option, décrite au paragraphe 5.9, est Indicateur de paquet de contrôle de pont. L'IANA a alloué la valeur 10 à cette option.

10. Remerciements

Le présent document a été produit par le groupe de travail Extensions au protocole point à point.

Il est fondé sur le protocole de contrôle de pontage PPP, [RFC2878], édité par Higashiyama et Baker et produit par le groupe de travail Extensions au protocole point à point. Il étend ce document en fournissant la prise en charge de l'indicateur de paquet de contrôle de pont, comme précisé aux paragraphes 3.5 et 5.9.

Appendice A. PDU de pont d'arbre d'expansion (ancien format)

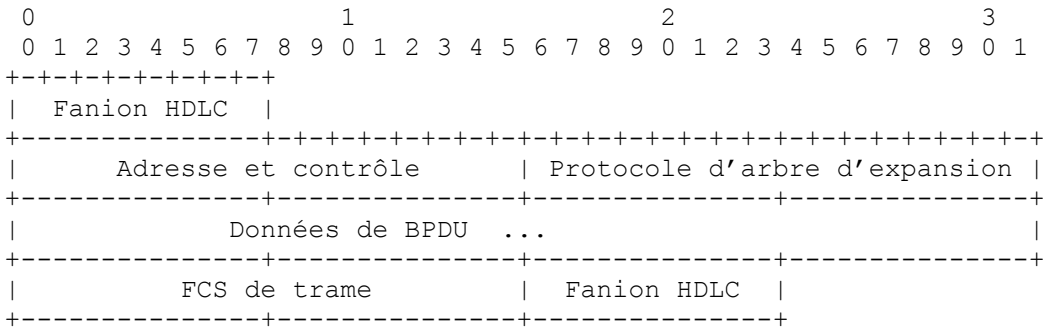
Par défaut, les BPDU d'arbre d'expansion DOIVENT être codées avec un en-tête de LLC MAC ou 802.2 comme décrit aux paragraphes 4.2 ou 4.3 du présent document. Cependant, si l'entité distante fait un Configure-Reject de l'option Gestion en ligne, indiquant par là qu'elle est un appareil purement conforme à la RFC1638, l'entité locale peut ensuite coder les BPDU comme décrit au paragraphe 4.3 de la RFC1638 pourvu que l'utilisation d'un protocole STP non NUL convenable à travers la liaison ait été négociée avec succès en utilisant l'option (ancienne) Protocole d'arbre d'expansion.

Voici la BPDU d'arbre d'expansion utilisée dans la RFC1638, sans aucun en-tête de LLC MAC ou 802.2 (qui sont fonctionnellement équivalents aux champs Adresse, Contrôle, et Protocole PPP). Les champs Bourrage de LAN et Somme de contrôle de trame sont de même superflus et absents.

Les champs Adresse et Contrôle sont soumis à la négociation LCP de compression des champs d'adresse et de contrôle.

Un système PPP qui est configuré à participer à un protocole d'arbre d'expansion particulier et reçoit une BPDU d'un protocole d'arbre d'expansion différent DEVRAIT le rejeter avec le Protocol-Reject LCP. Un système qui est configuré à ne pas participer à un protocole d'arbre d'expansion DOIT éliminer en silence toutes les BPDU.

PDU de pont d'arbre d'expansion :



Adresse et contrôle : comme défini par le tramage utilisé.

Protocole d'arbre d'expansion
Les valeurs à jour du champ Protocole d'arbre d'expansion sont spécifiées sur le site de l'IANA à www.iana.org). Les valeurs actuellement allouées sont :

Valeur (en hex)	**Protocole**
0201	IEEE 802.1 (soit 802.1D, soit 802.1G)0203 Pont de route de source IBM
0205	LANbridge 100 de DEC

Les deux versions de la trame IEEE 802.1 de protocole d'arbre d'expansion peuvent être distinguées par les champs au sein des données de BPDU.

Données de BPDU
Comme défini par le protocole d'arbre d'expansion spécifié.

Appendice B Pseudo-code de compression Tinygram

Émetteur PPP :

```
  si (ZeroPadCompressionEnabled &&
     BridgedProtocolHeaderFormat == IEEE8023 &&
     PacketLength == Minimum8023PacketLength) {

/* Retire tout jeu continu d'octets à zéro précédant, mais n'incluant pas, la FCS de LAN, mais ne s'étendant pas dans l'en-
tête MAC. */
     Établir (ZeroCompressionFlag);                  /* Signale le receveur */
     si (is_Set (LAN_FCS_Present)) {
        FCS = TrailingOctets (PDU, 4);               /* mémorise la FCS */
```

```
        RemoveTrailingOctets (PDU, 4);          /* Retire la FCS */
        tandis que (PacketLength > 14 &&        /* Arrêter à l'en-tête MAC ou au dernier octet non zéro */
            TrailingOctet (PDU) == 0)
          RemoveTrailingOctets (PDU, 1);        /* Retirer l'octet  zéro */
        Appendbuf (PDU, 4, FCS);                /* Restaurer la FCS */
      }
      autrement {
        tandis que (PacketLength > 14 &&        /* Arrêter à l'en-tête MAC ou au dernier octet non zéro */
            TrailingOctet (PDU) == 0)
          RemoveTrailingOctets (PDU, 1);        /* Retirer l'octet zéro */
      }
    }
```

Receveur PPP :

```
    si (ZeroCompressionFlag) {                  /* Le fanion est-il établi dans l'en-tête ? */
                                                /* Restaurer la longueur du paquet au minimum 802.3 */
      Supprimer (ZeroCompressionFlag);
      si (is_Set (LAN_FCS_Present)) {
        FCS = TrailingOctets (PDU, 4);          /* Mémoriser la FCS */
        RemoveTrailingOctets (PDU, 4);          /* Retirer la FCS */
        Appendbuf (PDU, 60 - PacketLength, zeroes);  /* Ajouter des zéros */
        Appendbuf (PDU, 4, FCS);                /* Restaurer la FCS */
      }
      autrement {
        Appendbuf (PDU, 60 - PacketLength, zeroes);  /* Ajouter des zéros */
      }
    }
```

Références

[802.1g] IEEE 802.1, "Draft Standard 802.1G: Remote MAC Bridging", P802.1G/D7, décembre 30, 1992.

[802.1D] IEEE 802.1D-1993, "Media Access Control (MAC) Bridges", ISO/IEC 15802-3:1993 ANSI/IEEE Std 802.1D, édition 1993, juillet 1993.

[802.1D-98] IEEE 802.1D-1998, "Information technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges: Revision". Révision de la norme ISO/CEI 10038: 1993, 802.1j-1992 et de 802.6k-1992. Elle incorpore P802.11c, P802.1p et P802.12e." ISO/CEI 15802-3: 1998.

[802.1Q] IEEE 802.1Q, ANSI/IEEE Standard 802.1Q, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", 1998.

[IBM] IBM, "Token-Ring Network Architecture Reference", 3ème édition, septembre 1989.

[RFC1570] W. Simpson, "Extensions LCP pour PPP", janvier 1994. *(P.S., MàJ par* 2484*)*

[RFC1638] F. Baker et R. Bowen, "Protocole de contrôle de pontage (BCP) en point à point", juin 1994. *(P.S., voir la* RFC2878*, elle-même rendue obsolète par la présente RFC*)

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153*)*

[RFC1990] K. Sklower et autres, "Protocole multiliaison en PPP (MP)", août 1996. (*Remplace* RFC1717) *(D.S.)*

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

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6", décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

[RFC2686] C. Bormann, "Extension Multi-classe à PPP multi-liaison", septembre 1999. *(P.S.)*

[RFC2878] M. Higashiyama, F. Baker, "Protocole de contrôle de pont en PPP (BCP)", juillet 2000. (*Obsolète, voir* RFC3518) *(P.S.)*

[RFC3232] J. Reynolds, "Numéros alloués : la RFC 1700 est remplacée par une base de données en ligne", janvier 2002.

Adresse des auteurs

Mitsuru Higashiyama
Anritsu Corporation
1800 Onna
Atsugi-shi
Kanagawa-prf.
243-8555 Japan
téléphone : +81 (46) 296-6625
mél : Mitsuru.Higashiyama@yy.anritsu.co.jp

Fred Baker
1121 Via Del Rey
Santa Barbara,
California
93117 USA
téléphone : (408) 526-4257
mél : fred@cisco.com

Tawei Liao
cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
USA
téléphone : (408) 853-8905
mél : tawei@cisco.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.