

Groupe de travail Réseau  
**Request for Comments : 3619**  
Catégorie : Information

S. Shah & M. Yip, Extreme Networks  
octobre 2003  
Traduction Claude Brière de L'Isle

# Version 1 de la commutation de protection automatique Ethernet (EAPS) de Extreme Networks

## Statut de ce mémoire

Le présent mémoire donne des informations pour la communauté de l'Internet. Il ne spécifie en aucun cas une norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

## Notice de Copyright

Copyright (C) The Internet Society (2003). Tous droits réservés.

## Résumé

Le présent document décrit la technologie de commutation de protection automatique Ethernet (EAPS, *Ethernet Automatic Protection Switching*) inventée par Extreme Networks (marque déposée) pour accroître la disponibilité et la robustesse des anneaux Ethernet. Un anneau Ethernet construit en utilisant EAPS peut avoir une résilience comparable à celle fournie par les anneaux SONET, à un moindre coût et avec moins de contraintes (par exemple, de taille d'anneau).

## 1 Introduction

De nombreux réseaux de zone métropolitaine (MAN, *Metropolitan Area Network*) et certains réseaux de zone locale (LAN, *Local Area Network*) ont une topologie en anneau, avec le développement de la fibre optique. La technologie de commutation de protection automatique Ethernet (EAPS) décrite ici fonctionne bien dans les topologies d'anneau pour les MAN ou les LAN.

La plupart des opérateurs de MAN veulent minimiser le temps de récupération dans l'éventualité d'une coupure de fibre. La technologie de commutation de protection automatique Ethernet (EAPS) décrite ici converge en moins d'une seconde, souvent en moins de 50 millisecondes. La technologie EAPS ne limite pas le nombre de nœuds dans l'anneau, et le temps de convergence est indépendant du nombre de nœuds de l'anneau.

## 2 Concept de fonctionnement

Un domaine EAPS existe sur un seul anneau Ethernet. Tout réseau de zone locale virtuel (VLAN, *Virtual Local Area Network*) Ethernet à protéger est configuré sur tous les accès de l'anneau pour le domaine EAPS en question. Chaque domaine EAPS a un seul "nœud maître" désigné. Tous les autres nœuds sur cet anneau sont appelés des "nœuds de transit".

Bien sûr, chaque nœud de l'anneau aura deux accès connectés à l'anneau. Un accès du nœud maître est désigné comme "accès principal" à l'anneau, tandis que l'autre accès est désigné comme "accès secondaire".

En fonctionnement normal, le nœud maître bloque l'accès secondaire pour toutes les trames qui ne sont pas de commande Ethernet qui appartiennent au domaine EAPS concerné, évitant ainsi la création d'une boucle dans l'anneau. Les mécanismes existants de commutation et d'apprentissage Ethernet fonctionnent sur cet anneau selon les normes existantes. Ceci est possible parce que le nœud maître fait apparaître l'anneau bien qu'il n'y ait pas de boucle du point de vue des algorithmes standard de l'Ethernet utilisés pour la commutation et l'apprentissage. Si le nœud maître détecte une panne de l'anneau, il débloque son accès secondaire et permet aux trames de données Ethernet de passer par cet accès. Il y a un "VLAN de contrôle" particulier qui peut toujours passer à travers tous les accès dans le domaine EAPS, y compris l'accès secondaire du nœud maître.

EAPS utilise à la fois un mécanisme d'interrogation et un mécanisme d'alerte, décrits ci-dessous, pour vérifier la connectivité de l'anneau et détecter rapidement toutes les pannes.

## 2.1 Alerte de rupture de liaison

Lorsqu'un nœud de transit détecte une coupure de liaison sur un de ses accès dans le domaine EAPS, ce nœud de transit envoie immédiatement une trame de commande "liaison défailante" sur le VLAN de commande au nœud maître.

Lorsque le nœud maître reçoit cette trame de commande "liaison défailante", le nœud maître passe de l'état "normal" à l'état d'anneau défailant et débloque son accès secondaire. Le nœud maître vide aussi son tableau des pontages, et il envoie aussi une trame de commande à tous les autres nœuds de l'anneau, leur enjoignant de vider aussi leurs tableaux de pontage. Immédiatement après avoir vidé son tableau des pontages, chaque nœud commence à apprendre la nouvelle topologie.

## 2.2 Ring Polling

Le nœud maître envoie une trame de vérification de bonne santé sur le VLAN de commande à un intervalle configurable par l'utilisateur. Si l'anneau est complet, la trame de vérification de bonne santé sera reçue sur son accès secondaire, et le nœud maître va remettre à zéro son temporisateur de période de défailance et continuer en fonctionnement normal.

Si le nœud maître ne reçoit pas la trame de vérification de bonne santé avant l'expiration du temporisateur de période de défailance, le nœud maître passe de l'état normal à l'état "défaillance d'anneau" et débloque son accès secondaire. Le nœud maître vide aussi son tableau des pontages et envoie une trame de commande à tous les autres nœuds, leur donnant pour instruction de vider aussi leurs tableaux de pontages. Immédiatement après le vidage de son tableau des pontages, chaque nœud commence à apprendre la nouvelle topologie. Ce mécanisme d'interrogation d'anneau fournit un retour d'informations dans l'éventualité où une trame d'alerte de défaillance de liaison serait perdue pour une raison imprévue.

## 2.3 Restauration d'anneau

Le nœud maître continue d'envoyer des trames de vérification de bonne santé périodiques à partir de son accès principal même lorsqu'il fonctionne dans l'état de défaillance d'anneau. Une fois l'anneau restauré, la trame de vérification de bonne santé suivante sera reçue sur l'accès secondaire du nœud maître. Cela causera le retour du nœud maître à l'état normal, bloquera logiquement les trames qui ne sont pas de commande sur l'accès secondaire, videra son propre tableau des pontages, et enverra une trame de commande aux nœuds de transit, leur donnant pour instruction de vider leurs tableaux de pontage et de réapprendre la topologie.

Durant le temps entre la détection de la restauration de sa liaison par le nœud de transit et la détection de la restauration de l'anneau par le nœud maître, l'accès secondaire du nœud maître est toujours ouvert – ce qui crée la possibilité d'une boucle temporaire dans la topologie. Pour l'empêcher, le nœud de transit placera tous les VLAN protégés transitant par l'accès qui vient d'être restauré dans un état temporairement bloqué, mémorisera quel accès a été temporairement bloqué, et passera à l'état "pré transmission". Lorsque le nœud de transit en état de "pré transmission" reçoit une trame de commande lui donnant pour instruction de vider son tableau des pontages, il va vider le tableau des pontages, débloquent les VLAN protégés précédemment bloqués sur l'accès qui vient d'être restauré, et passera à l'état "normal".

## 3 Domaines EAPS multiples

Un commutateur à capacité EAPS peut faire partie de plus d'un anneau. Et donc, un commutateur à capacité EAPS peut appartenir à la fois à plus d'un domaine EAPS. Chaque domaine EAPS sur un commutateur exige une instance distincte du protocole EAPS sur chaque commutateur, une instance par anneau protégé par EAPS.

On peut aussi avoir plus d'un domaine EAPS qui fonctionne à un instant donné sur un seul anneau. Chaque domaine EAPS a son propre nœud maître unique et son propre ensemble de VLAN protégés. Cela facilite la réutilisation spatiale de la bande passante de l'anneau.

## Format de trame EAPS

0	1	2	3	4	4
12345678	90123456	78901234	56789012	34567890	12345678
Adresse MAC de destination (6 octets)					
Adresse MAC de source (6 octets)					
EtherType		PRI	ID de VLAN	Longueur de trame	
DSAP/SSAP		Contrôle		OUI = 0x00E02B	
0x00bb		0x99	0x0b	EAPS_LENGTH	
EAPS_VER	EAPSTYP E	CTRL_VLAN_ID		0x0000	
0x0000		SYSTEM_MAC_ADDR (6 octets)			
HELLO_TIMER			FAIL_TIMER		
État	0x00	HELLO_SEQ		0x0000	
Réservé (0x000000000000)					
Réservé (0x000000000000)					
Réservé (0x000000000000)					
Réservé (0x000000000000)					
Réservé (0x000000000000)					
Réservé (0x000000000000)					

où :

L'adresse MAC de destination est toujours 0x00e02b000004.

PRI contient 3 bits de priorité, avec un autre bit réservé.

EtherType est toujours 0x8100.

DSAP/SSAP est toujours 0xAAAA.

Contrôle est toujours 0x03.

EAPS\_LENGTH est 0x40.

EAPS\_VER est 0x0001.

CTRL\_VLAN\_ID est l'identifiant de VLAN pour le VLAN de contrôle utilisé.

SYSTEM\_MAC\_ADDR est l'adresse MAC système du nœud d'envoi.

HELLO\_TIMER est la valeur établie par le nœud maître.

FAIL\_TIMER est la valeur établie par le nœud maître.

HELLO\_SEQ est le numéro de séquence de la trame Hello.

Valeurs des types EAPS (EAPSTYPE) :

HEALTH	= 5
RING-UP-FLUSH-FDB	= 6
RING-DOWN-FLUSH-FDB	= 7
LINK-DOWN	= 8

Toutes les autres valeurs sont réservées.

Valeurs d'état :

IDLE	= 0 ( <i>repos</i> )
COMPLETE	= 1 ( <i>terminé</i> )
FAILED	= 2 ( <i>échec</i> )
LINKS-UP	= 3 ( <i>Liaison établie</i> )
LINK-DOWN	= 4 ( <i>défaillance de liaison</i> )
PRE-FORWARDING	= 5 ( <i>pré-transmission</i> )

Toutes les autres valeurs sont réservées.

## 4 Considérations pour la sécurité

Toute personne ayant un accès physique aux connexions à la couche physique pourrait falsifier n'importe quelle trame Ethernet, y compris (entre autres) des trames Bridge ou EAPS. De telles falsifications pourraient être utilisées pour perturber de diverses façons un réseau Ethernet, y compris par des méthodes qui sont spécifiques d'EAPS ou par d'autres méthodes sans rapport avec elle, comme de fausses trames de pont Ethernet.

À ce titre, il est recommandé que les utilisateurs ne développent pas un Ethernet sans quelque forme de chiffrement dans des environnements où de telles attaques actives sont considérées comme un risque opérationnel significatif. Il existe d'ores et déjà des normes de l'IEEE pour le chiffrement de la couche de liaison. Ces normes de l'IEEE pourraient être utilisées

pour protéger des liaisons Ethernet. Autrement, on pourrait utiliser des mécanisme de sécurité de couche supérieure si c'est plus approprié au modèle de menace local.

## 5 Notice de droits de propriété intellectuelle

Des revendications de droits de propriété intellectuelle ont été notifiés à l'IETF à l'égard de tout ou partie de la spécification contenue dans le présent document. Pour plus d'informations, consulter la liste en ligne des revendications de droits.

## 6 Remerciement

Le présent document a été édité et mis en format de RFC par R.J. Atkinson à partir de documents internes créés par les auteurs mentionnés ci-dessous. L'éditeur est entièrement responsable de toutes les erreurs commises durant la rédaction.

## 7 Adresse de l'éditeur

R. Atkinson  
Extreme Networks  
3585 Monroe Street  
Santa Clara, CA, 95051 USA  
Téléphone : +1 (408)579-2800  
mél : rja@extremenetworks.com

## 8 Adresse des auteurs

S. Shah  
Extreme Networks  
3585 Monroe Street  
Santa Clara, CA, 95051  
Téléphone : +1 (408)579-2800  
mél : sshah@extremenetworks.com

M. Yip  
Extreme Networks  
3585 Monroe Street  
Santa Clara, CA, 95051  
Téléphone : +1 (408)579-2800  
mél : my@extremenetworks.com

## 9 Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2003). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de copyright ci-dessus et le présent paragraphe soient inclus dans toutes ces copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de copyright ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de copyright définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et LE CONTRIBUTEUR, L'ORGANISATION QU'IL OU ELLE REPRÉSENTE OU QUI LE/LA FINANCE (S'IL EN EST), LA INTERNET SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI-ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

**Remerciement**

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