Groupe de travail Réseau
Request for Comments : 3822
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

D. Peterson
Computer Network Technology (CNT)
juillet 2004

Découverte de canal fibre sur des entités TCP/IP (FCIP) en utilisant le protocole de localisation de service version 2 (SLPv2)

Résumé
Le présent document définit l'utilisation du protocole de localisation de service version 2 (SLPv2) par des entités de canal fibre sur TCP/IP (FCIP).

1. Introduction

Le présent document décrit l'utilisation du protocole de localisation de service version 2 pour effectuer la découverte dynamique de canaux fibre participants sur les entités TCP/IP (FCIP). On spécifié des lignes directrices de mise en œuvre, des gabarits de type de service, et des considérations sur la sécurité.

2. Conventions de notation

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

3. Terminologie

Voici quelques définitions qui pourront aider le lecteur qui ne serait pas familier de SLP ou de FCIP. Certaines de ces définitions sont reproduites de la [RFC2608] et de la [RFC3105].

Agent d'utilisateur (UA, *User Agent*)
Processus qui fonctionne au nom du client pour établir le contact avec un service. L'UA restitue les informations de service des agents de service ou des agents de répertoire.

Agent de service (SA, *Service Agent*)
Processus qui fonctionne au nom d'un ou plusieurs services pour annoncer les services et leurs capacités.

Agent de répertoire (DA, *Directory Agent*)
Processus qui collecte les annonces de service. Il ne peut y avoir qu'un seul DA présent pour un certain hôte.

Portée *(Scope)*
Ensemble désigné de services, constituant normalement un groupe administratif logique.

Annonce de service
Un URL, des attributs, et une durée de vie (indiquant pendant combien de temps l'annonce est valide) fournissant des informations d'accès au service et une description des capacités d'un certain service.

Entité FCIP
Point d'interface FCIP avec le réseau IP.

Nom d'entité FCIP
Nom mondial du commutateur si l'entité FCIP réside dans un commutateur ou le nom de nœud mondial du Nx_Port associé.

Domaine de découverte FCIP
Il spécifie quelles entités FCIP ont la permission de se découvrir les unes les autres dans les limites de la portée.

4. Utilisation de SLPv2 pour la découverte de service FCIP

Au moins deux entités FCIP doivent être impliquées dans le processus de découverte d'entité. Le résultat final est qu'une entité FCIP va découvrir une ou plusieurs entités FCIP homologues.

4.1 Découverte des entités FCIP en utilisant SLPv2

La Figure 1 montre les relations entre les entités FCIP et leurs agents SLPv2 associés.

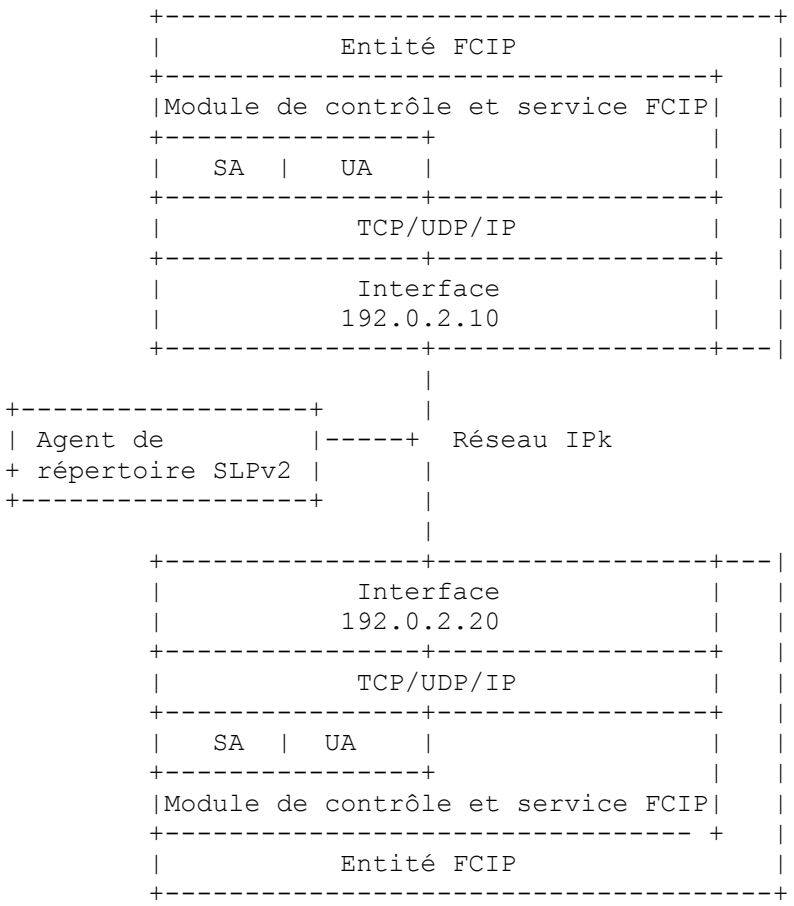

Figure 1 : Relations entre entité FCIP et agent SLPv2

Comme indiqué à la Figure 1, chaque entité FCIP contient un module FCIP de contrôle et de services qui fait l'interface entre un agent de service (SA) et un agent d'utilisateur (UA) SLPv2.

Le SA construit une annonce de service du type "service:fcip:entity" pour chacun des URL de service qu'il souhaite enregistrer. L'annonce de service contient une durée de vie ainsi que d'autres attributs définis dans le gabarit de service.

Le reste du procès de découverte est identique à celui utilisé par toute paire client/serveur mettant en œuvre SLPv2 :

1. Si un agent de répertoire (DA) SLPv2 est trouvé [RFC2608], le SA contacte le DA et enregistre l'annonce de service. Que un ou plusieurs DA SLPv2 soient découverts, le SA conserve l'annonce de service elle-même et répond directement aux interrogations en diffusion groupée d'agent d'utilisateur (UA).
2. Lorsque l'entité FCIP exige des informations de contact pour une entité FCIP homologue, l'UA contacte soit le DA en

utilisant l'envoi individuel, soit le SA en utilisant la diffusion groupée avec une demande de service SLPv2. La demande de service de l'UA comporte une interrogation, sur la base des attributs, pour indiquer les caractéristiques des entités FCIP homologues qu'il demande.

3. Une fois que l'UA a l'adresse IP et le numéro d'accès d'une entité FCIP homologue, il peut commencer la procédure normale de connexion, comme décrit dans la [RFC3821], avec une entité FCIP homologue.

L'utilisation d'un agent de répertoire est RECOMMANDÉE pour les opérations SLPv2 dans un environnement FCIP.

4.1.1 Domaines de découverte FCIP

Le concept d'un domaine de découverte donne une plus fine granularité du contrôle des découvertes permis entre entités FCIP au sein d'une portée spécifique SLPv2.

La Figure 2 donne un exemple des relations entre les entités FCIP et leurs domaines de découverte associés au sein d'une portée SLPv2 spécifiée.

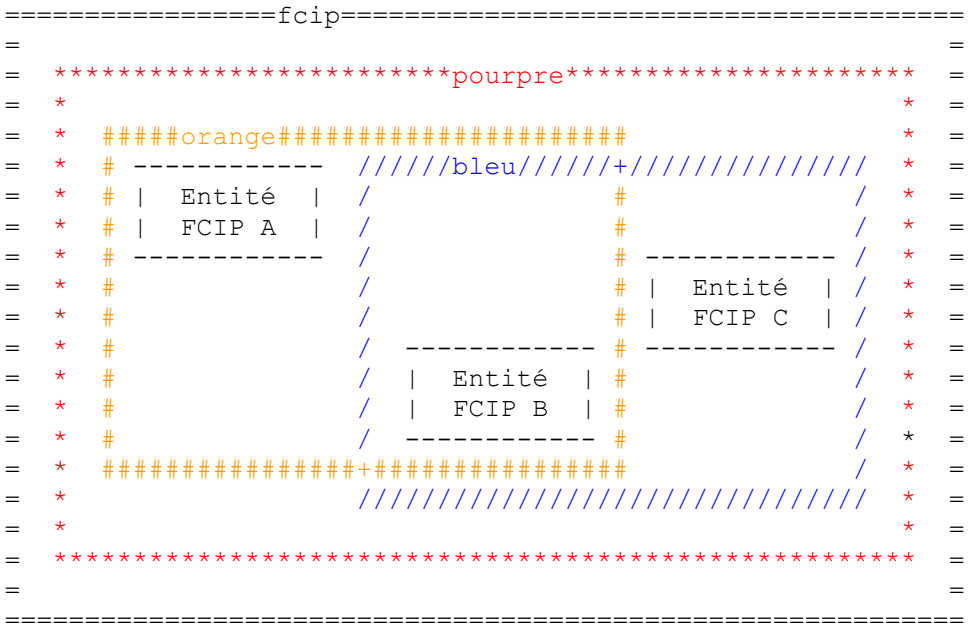

Figure 2 : Exemple d'entité FCIP et de domaine de découverte

Au sein de la portée spécifiée "fcip", l'administrateur a défini un domaine de découverte "pourpre", permettant aux entités FCIP A, B, et C de se découvrir les unes les autres. Ce domaine de découverte est illustré avec le caractère "*".

Au sein de la portée spécifiée "fcip", l'administrateur a défini un domaine de découverte "orange", permettant à l'entité FCIP A de découvrir l'entité FCIP B, mais pas l'entité FCIP C. Ce domaine de découverte est illustré avec le caractère dièse "#".

Au sein de la portée spécifiée "fcip", l'administrateur a défini un domaine de découverte "bleu", permettant à l'entité FCIP C de découvrir l'entité FCIP B, mais pas l'entité FCIP A. Ce domaine de découverte est illustré avec le caractère "/".

Pour l'exemple de relations montré par la Figure 2, la valeur de l'attribut fcip-discovery-domain pour chaque entité FCIP est la suivante :
Entité FCIP A = orange,pourpre
Entité FCIP B = orange,bleu,pourpre
Entité FCIP C = bleu,pourpre

5. Gabarits FCIP SLPv2

Deux gabarits sont fournis : un gabarit d'entité FCIP, et un gabarit abstrait pour fournir un moyen d'ajouter à l'avenir d'autres gabarits en rapport avec FCIP.

5.1 Gabarit de type de service FCIP abstrait

Ce gabarit définit le service abstrait "service:fcip". Il est utilisé comme service de niveau supérieur pour encapsuler tous les autres services en rapport avec FCIP.

Nom du soumettant : David Peterson
Langage du gabarit de service : fr
Considérations pour la sécurité : voir la section 6.

Texte du gabarit :
----------Le gabarit commence ici----------
type-de-gabarit = fcip

version-du-gabarit = 0.1

description-du-gabarit = C'est un type de service abstrait. L'objet du type de service fcip est d'englober tous les services utilisés pour prendre en charge le protocole FCIP.

gabarit-de-syntaxe-d'url = chemin-d'url = ; Dépend du type de service concret.

----------Le gabarit se termine ici----------

5.2 Gabarit de type de service concret d'entité FCIP

Ce gabarit définit le service "service:fcip:entity". Un appareil qui contient des entités FCIP qui souhaite qu'elles soient découvertes via SLPv2 va enregistrer chacune d'elles avec chacune de leurs adresses, comme ce type de service.

Les entités FCIP qui souhaitent découvrir d'autres entités FCIP de cette manière vont généralement utiliser une des chaînes d'interrogation des exemples suivants :

1. Trouver une entité FCIP spécifique, connaissant son nom d'entité FCIP :
Service : service:fcip:entity
Portée : liste-de-portée-d'entité-fcip
Interrogation : (nom-d'entité-fcip=\ff\10\00\00\60\69\20\34\0C)

2. Trouver toutes les entités FCIP au sein d'un domaine de découverte FCIP spécifié :
Service : service:fcip:entity
Portée : liste-de-portée-d'entité-fcip
Interrogation : (domaine-de-découverte-fcip=nom-de-domaine-de-découverte-fcip)

3. De plus, une application de gestion peut souhaiter découvrir toutes les entités FCIP :
Service : service:fcip:entity
Portée : liste-de-portée-de-service-de-gestion
Interrogation : aucune

Nom du soumettant : David Peterson
Langage du gabarit de service : fr
Considérations de sécurité : voir la section 6.

Texte du gabarit :
----------le gabarit commence ici----------
type-de-gabarit=fcip:entity

version-du-gabarit=1.0

description-du-gabarit=
C'est un type de service concret. Le type fcip:entity est utilisé pour enregistrer des adresses individuelles d'entité FCIP qui seront découvertes par d'autres. Les UA vont généralement les chercher en incluant un des éléments suivants :
- le nom d'entité FCIP pour lequel une adresse est nécessaire,
- le nom de domaine de découverte FCIP pour lequel les adresses sont demandées
- l'URL de service

syntaxe-d'url-de gabarit =
chemin-d'url = accès-d'hôte
accès-d'hôte = hôte [":" accès]
hôte = nom-d'hôte / numéro-d'hôte
nom-d'hôte = *(étiquette-de-domaine ".") étiquette-supérieure
alphanum = ALPHA / CHIFFRE
étiquette-de-domaine = alphanum / alphanum * [alphanum / "-"] alphanum
étiquette-supérieure = ALPHA / ALPHA * [alphanum / "-"] alphanum
numéro-d'hôte = numéro-ipv4
numéro-ipv4 = 1*3CHIFFRE 3("." 1*3CHIFFRE)
accès = 1*CHIFFRE

;
; Un nom d'hôte DNS devrait être utilisé avec le numéro d'accès FCIP bien connu de l'IANA pour fonctionner avec les appareils de NAT/NAPT.
;
; Exemples :
; service:fcip:entity://host.example.com
; service:fcip:entity://192.0.2.0:4000
;

fcip-entity-name = opaque L
Si l'entité FCIP est une mise en œuvre de VE_Port/B_Access [FC-BB-2] qui réside dans un commutateur, le fcip-entity-name est le nom de commutateur canal fibre [FC-SW-3]. Autrement, le fcip-entity-name est le nom de nœud canal fibre [FC-FS] de l'accès (par exemple, un Nx_Port) associé à l'entité FCIP. Une entité représentant plusieurs points d'extrémité doit enregistrer chacun des points d'extrémité en utilisant SLPv2.

transports = chaîne M L
tcp
C'est une liste des protocoles de transport que prend en charge l'entité enregistrée. FCIP n'est actuellement pris en charge que sur TCP.
tcp

mgmt-entity = chaîne M O L
Les URL de la ou des interfaces de gestion sont appropriés pour la gestion par SNMP, la Toile, ou telnet de l'entité FCIP.
Exemples :
http://fcipentity.exemple.com:1080/
telnet://fcipentity.exemple.com

fcip-discovery-domain = chaîne M L
fcip
La chaîne fcip-discovery-domain contient le ou les noms du ou des domaines de découverte FCIP auxquels cette entité FCIP appartient.

----------Le gabarit se termine ici----------

6. Considérations pour la sécurité

Le modèle de sécurité SLPv2 tel que spécifié dans la [RFC2608] n'assure pas la confidentialité, mais fournit un mécanisme d'authentification pour que les UA assurent que les annonces de service ne proviennent que de SA de confiance avec une exception qui est qu'il ne fournit pas de mécanisme pour authentifier les "réponses de résultat zéro". Voir dans la [RFC3723] l'exposé sur le modèle de sécurité SLPv2 [RFC2608].

Une fois qu'une entité FCIP est découverte, l'authentification et l'autorisation sont traitées par le protocole FCIP. Il est de la responsabilité des fournisseurs de ces services de s'assurer qu'un service annoncé ou découvert de façon inappropriée ne compromet pas leur sécurité.

Lorsque aucune sécurité n'est utilisée pour SLPv2, il y a un risque de distribution de fausses informations de découverte. La principale contre mesure pour ce risque est l'authentification. Lorsque ce risque pose un problème significatif, les SA IPsec DEVRAIENT être utilisées pour le trafic FCIP soumis à ce risque pour s'assurer que seul du trafic FCIP s'écoule

entre les points d'extrémité qui ont participé à l'authentification IKE. Par exemple, si un agresseur distribue des informations de découverte prétendant faussement qu'il est un point d'extrémité FCIP, il lui manquera les informations secrètes nécessaire pour réussir à mener à bien l'authentification IKE, et il sera donc empêché d'envoyer ou de recevoir du faux trafic FCIP.

Il reste un risque d'attaque de déni de service fondée sur l'utilisation répétée de fausses informations de découverte qui vont causer l'initiation d'une négociation IKE. Les contre mesures sont la configuration administrative de chaque entité FCIP à limiter les homologues avec lesquels elle va accepter de communiquer (c'est-à-dire, par gamme d'adresses IP et/ou domaine DNS) et l'entretien d'une mémoire tampon d'authentification négative pour éviter de contacter de façon répétée une entité FCIP qui a échoué à l'authentification. Ces trois mesures (c'est-à-dire, les limites de gamme d'adresse IP, les limites de domaine DNS, la mémoire tampon d'authentification négative) DOIVENT être mises en œuvre.

6.1 Mise en œuvre de la sécurité

La sécurité pour SLPv2 dans un environnement de mémorisation IP est spécifiée dans la [RFC3723]. IPsec est de mise en œuvre obligatoire pour les clients et serveurs IPS. Donc, tous les clients de mémorisation IP, y compris ceux qui invoquent SLP, peuvent être supposés prendre en charge IPsec. Les serveurs SLP ne peuvent cependant pas être supposés mettre en œuvre IPsec, car une telle exigence n'existe pas dans la norme SLP. En particulier, les agents de répertoire (DA, *Directory Agent*) SLP peuvent fonctionner sur des machines autres que celles qui utilisent les protocoles IPS.

IPsec DEVRAIT être mis en œuvre pour SLPv2 comme spécifié dans la [RFC3723] ; cela inclut ESP avec une transformation non nulle pour fournir à la fois l'authentification et la confidentialité.

Comme les services de mémorisation IP ont leurs propres capacités d'authentification lorsque ils sont localisés, l'authentification SLPv2 est de mise en œuvre et d'utilisation FACULTATIVE (comme exposé plus en détails dans la [RFC3723]).

7. Considérations relatives à l'IANA

Le présent document décrit deux gabarits SLP à la Section 5. Ils devraient être enregistrés dans le registre IANA "SVRLOC Templates". Ce processus est décrit dans la section Considérations relatives à l'IANA de la [RFC2609].

8. Considérations d'internationalisation

SLP permet d'enregistrer et de restituer des chaînes internationalisées. Les attributs qui dans les gabarits ne sont pas marqués d'un 'L' (littéral) seront enregistrés de façon localisée. Une localisation "en" (English) DOIT être enregistrée, et d'autres PEUVENT être enregistrées.

9. Résumé

Le présent document décrit comment SLPv2 peut être utilisé par des entités FCIP pour trouver d'autres entités FCIP. Il présente les gabarits de type de service pour les entités FCIP.

10. Remerciements

Le présent document a été produit par l'équipe de découverte de FCIP, comprenant Todd Sperry (Adaptec), Larry Lamars (SanValley), Robert Snively (Brocade), Ravi Natarajan (Lightsand), Anil Rijhsinghani (McData), et Venkat Rangan (Rhapsody Networks). Merci aussi à Mark Bakke (Cisco) pour son aide au démarrage et ses conseils, et à David Black, Erik Guttman, et James Kempf pour leur assistance durant la révision par les experts.

11. Références

11.1 Références normatives

[FC-SW-3] Fibre Channel Switch Fabric - 3, ANSI INCITS 384-2004.

[FC-BB-2] Fibre Channel Backbone - 2, ANSI INCITS 372-2003.

[FC-FS] Fibre Channel Framing and Signaling, T11 Project 1331-D, Rev 1.90, 9 avril 2003.

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

[RFC2608] E. Guttman et autres, "Protocole de localisation de service, version 2", juin 1999. (*MàJ par* RFC3224) *(P.S.)*

[RFC2609] E. Guttman, C. Perkins, J. Kempf, "Gabarits de service et service : schémas", juin 1999. *(P.S.)*

[RFC3723] B. Aboba et autres, "Protocoles de sécurisation de mémorisation de blocs sur IP", avril 2004. *(P.S.)*

[RFC3821] M. Rajagopal, E. Rodriguez, R. Weber, "Canal fibre sur TCP/IP (FCIP)", juillet 2004. *(P.S.)*

11.2 Références pour information

[RFC3105] J. Kempf et G. Montenegro, "Trouver un serveur RSIP avec SLP", octobre 2001. *(Exp.)*

12. Adresse de l'auteur

David Peterson
Computer Network Technology (CNT)
6000 Nathan Lane North
Minneapolis, MN 55442

téléphone : 763-268-6139
mél : dap@cnt.com

13. Déclaration complète de droits de reproduction

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.

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