Groupe de travail Réseau
Request for Comments : 3355
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

A. Singh, Motorola
R. Turner, Paradyne
R. Tio & S. Nanji, Redback Networks
août 2002

Protocole de tunnelage de couche 2 (L2TP) sur couche 5 d'adaptation ATM (AAL5)

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 de tunnelage de couche deux (L2TP, *Layer Two Tunneling Protocol*) fournit une méthode standard pour transporter la couche liaison du protocole point à point (PPP) entre un serveur à numérotation et un serveur d'accès réseau, en utilisant une connexion réseau au lieu d'une connexion physique point à point. Le présent document décrit l'utilisation d'un réseau en technique temporelle asynchrone (ATM, *Asynchronous Transfer Mode*) pour la connexion réseau sous-jacente. La spécification de la version 4.0 ou 3.1 de signalisation d'interface usager-réseau (UNI, *User-Network Interface*) ATM avec la couche 5 d'adaptation ATM (AAL5, *ATM Adaptation Layer 5*) est prise en charge comme interface au réseau ATM.

Applicabilité
La présente spécification est destinée aux mises en œuvre de L2TP qui utilisent ATM pour fournir la liaison de communications entre le concentrateur d'accès L2TP et le serveur réseau L2TP.

Table des Matières

1. Introduction

Le protocole Point à point (PPP) [RFC1661], est fréquemment utilisé sur la liaison entre un ordinateur individuel avec un modem à numérotation et un fournisseur de service réseau (NSP, *Network Service Provider*). Le protocole de tunnelage de couche 2 (L2TP; *Layer Two Tunneling Protocol*) [RFC2661] permet à un serveur à numérotation de fournir l'accès à un

NSP distant en étendant la connexion PPP à travers un tunnel dans un réseau auquel lui et le NSP sont tous deux directement connectés. Un "tunnel" est une connexion de couche réseau entre deux nœuds, utilisée dans le rôle d'une connexion de couche liaison des données entre ces nœuds, éventuellement au titre d'un réseau différent. Dans la [RFC2661] le serveur à numérotation est appelé concentrateur d'accès L2TP (LAC, *L2TP Access Concentrator*). L'appareil distant qui fournit l'accès à un réseau est appelé un serveur réseau L2TP (LNS, *L2TP Network Server*). L2TP utilise un service de livraison de paquets pour créer un tunnel entre le LAC et le LNS. "L2TP est conçu pour être largement isolé des détails du support sur lequel est établi le tunnel ; L2TP exige seulement que le tunnel support fournisse la connexité point à point en mode paquet" [RFC2661]. Un réseau ATM avec AAL5 offre une forme convenable de connexion en mode paquet. La présente norme complète la [RFC2661] en fournissant les détails spécifiques de l'utilisation de AAL5 pour une connexion point à point entre LAC et LNS.

2. Conventions

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].

Une liste des acronymes utilisés dans ce document est donnée à l'Appendice A.

3. Interface de service de couche AAL5

L2TP traite le service de couche AAL5 ATM sous-jacent comme une liaison binaire point à point synchrone. Dans ce contexte, la liaison L2TP correspond à un circuit virtuel (VC) AAL5 ATM. Le VC DOIT être bidirectionnel, point à point, et il PEUT être soit dédié (c'est-à-dire, permanent, établi par provision) ou commuté (établi à la demande).

Le service AAL5 en mode message, dans le mode de fonctionnement non assuré, sans l'option de livraison corrompue DOIT être utilisé.

Format d'interface – La frontière de couche L2TP/AAL5 présente une interface de service d'octet à la couche AAL5. Il n'existe aucune disposition pour fournir ou accepter des sous octets.

3.1 Unité maximum de transfert

Chaque PDU L2TP DOIT être transportée au sein d'une seule PDU AAL5. Donc l'unité de transfert maximum (MTU, *Maximum Transfer Unit*) de la connexion AAL5 constitue une contrainte pour la MTU du tunnel L2TP qui utilise la connexion et pour la MTU de toutes les connexions PPP qui utilisent le tunnel. (La [RFC1661] se réfère à cela sous le nom d'unité de réception maximum (MRU, *Maximum Receive Unit*). Dans [SIG31], c'est la taille maximum de CPCS-SDU vers l'avant et vers l'arrière.)

Une mise en œuvre DOIT prendre en charge une MRU PPP d'au moins 1500 octets.

Une mise en œuvre DEVRAIT utiliser une plus grande MTU que la valeur minimum spécifiée ci-dessus. Il est RECOMMANDÉ qu'une mise en œuvre prenne en charge un paquet IP d'au moins 9180 octets dans la PDU PPP.

3.2 Qualité de service

Pour fournir la qualité de service (QS) désirée, et éventuellement des qualités de service différentes à des connexions client différentes, une mise en œuvre PEUT utiliser plus d'une connexion AAL5 entre un LAC et un LNS.

Les mécanismes de QS, tels que le débit binaire non spécifié (UBR, *Unspecified Bit Rate*) différencié [DUBR], qui pourraient impliquer un multiplexage inverse de tunnel à travers plusieurs VC feront l'objet d'études ultérieures. Les mécanismes de QS applicables à un seul tunnel correspondant à un seul VC, sont indépendants du transport ATM et sortent du domaine d'application du présent document.

3.3 Paramètres de connexion ATM

La couche L2TP n'impose pas de restriction en ce qui concerne le taux de transmission ou les paramètres de descripteur de trafic de la couche ATM sous-jacente.

Des paramètres de trafic spécifiques PEUVENT être établis pour une connexion PVC par accord entre les parties communicantes. L'appelant PEUT demander des paramètres de trafic spécifiques au moment de l'établissement de la connexion d'un SVC.

L'autoconfiguration des systèmes d'extrémité pour les PVC peut être facilitée par l'utilisation des extensions facultatives ILMI 4.0 documentées dans [ILMIA]. Cela donne des informations comparables aux éléments d'information (IE) utilisés pour l'établissement de connexion de plan de contrôle.

4. Encapsulation multi protocole

La présente spécification utilise les principes, la terminologie, et la structure de trame décrites dans "Encapsulation multi protocoles sur couche 5 d'adaptation ATM" [RFC2684]. L'objet de la présente spécification n'est pas de répéter ce qui a déjà été normalisé dans la [RFC2684], mais de spécifier comment les mécanismes qui y sont décrits sont à utiliser pour transposer L2TP sur un réseau ATM fondé sur AAL5.

Comme spécifié dans la [RFC2684], les PDU L2TP doivent être portées dans le champ Charge utile des PDU de sous couche de convergence de partie commune (CPCS, *Common Part Convergence Sublayer*) de AAL5, et la sous couche de convergence spécifique du service (SSCS, *Service Specific Convergence Sublayer*) de AAL5 doit être vide.

La Section 1 de la [RFC2684] définit deux mécanismes pour identifier le protocole encapsulé dans le champ Charge utile de la PDU AAL5 :
1. Multiplexage fondé sur le circuit virtuel (VC).
2. Encapsulation de commande de liaison logique (LLC, *Logical Link Control*).

Dans le premier mécanisme, le type de protocole de la charge utile est implicitement accepté par les points d'extrémité pour chaque circuit virtuel utilisant l'approvisionnement ou les procédures du plan de contrôle. Ce mécanisme sera appelé "VC L2TP multiplexé".

Dans le second mécanisme, le type de protocole de la charge utile est explicitement identifié dans chaque PDU AAL5 par un en-tête LLC IEEE 802.2. Ce mécanisme est appelé "LLC L2TP encapsulée".

Une mise en œuvre L2TP :
1. DOIT prendre en charge la LLC L2TP encapsulée sur les PVC.
2. PEUT prendre en charge la LLC L2TP encapsulée sur les SVC.
3. PEUT prendre en charge le VC L2TP multiplexé sur les PVC ou les SVC.

Lorsque un PVC est utilisé, les points d'extrémité doivent être configurés à utiliser une des deux méthodes d'encapsulation.

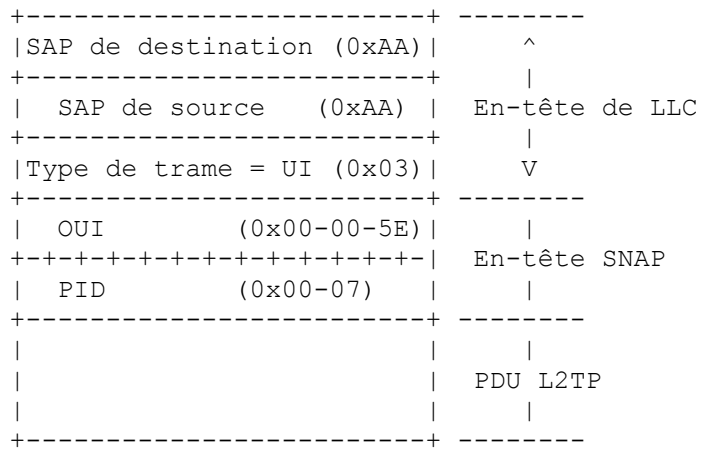
Si une mise en œuvre prend en charge les SVC, elle DOIT utiliser la procédure de l'Annexe C de [Q.2931] pour négocier l'établissement de la connexion, en codant l'élément d'information (IE, *information element*) Interface de couche inférieure large bande (B-LLI, *Broadband Lower Layer Interface*) pour signaler soit un VC L2TP multiplexé, soit une LLC L2TP encapsulée. Les détails de cette procédure du plan de contrôle sont décrits à la section 7.

Si une mise en œuvre se connecte à travers une unité d'inter fonctionnement de service de relais de trame/ATM FRF.8 [FRF8], elle DOIT alors utiliser LLC L2TP encapsulée.

5. L2TP encapsulé dans LLC sur AAL5

Lorsque l'encapsulation dans LLC est utilisée, le champ Charge utile de la PDU CPCS AAL5 DEVRA être codé comme montré à la Figure 1. Les champs pertinents de ce diagramme sont :
1. En-tête LLC IEEE 802.2 : SAP de source et de destination de 0xAA suivi par un type de trame de Information non numérotées (UI, *Un-numbered Information*) (valeur 0x03). Cet en-tête de LLC indique qu'un en-tête de SAP IEEE 802.1a suit [RFC2684].
2. En-tête SNAP IEEE 802.1a : Les trois octets de la valeur d'identifiant unique d'organisation (OUI, *Organizationally Unique Identifier*) de 0x00-00-5E identifient l'IANA (Autorité d'allocation des numéros de l'Internet). Les deux octets de l'identifiant de protocole (PID, *Protocol Identifier*) identifient L2TP comme protocole encapsulé. La valeur du PID est 0x0007.
3. PDU L2TP :

Figure 1 – PDU L2TP encapsulée dans LLC



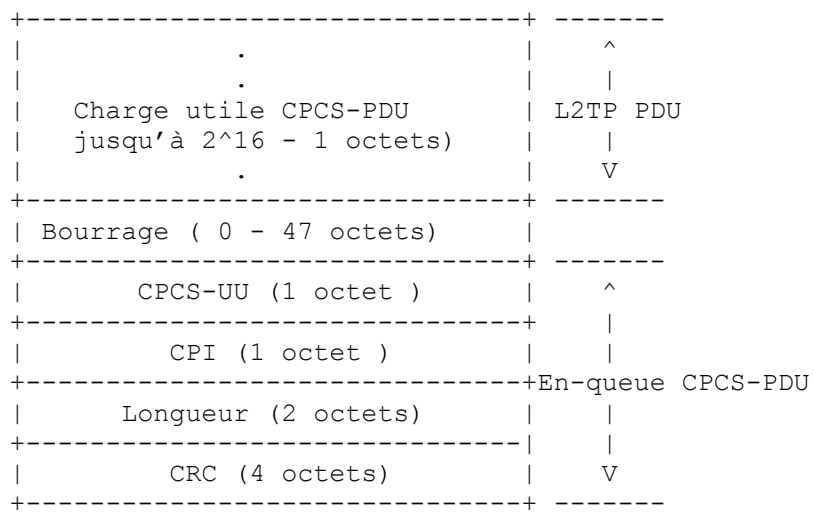
Note : Le format global de la PDU CPCS AAL5 est présenté à la section suivante.

Les points d'extrémité PEUVENT être provisionnés bilatéralement à envoyer d'autres protocoles encapsulés dans LLC à côté de L2TP sur la même connexion virtuelle.

6. L2TP pour circuit virtuel multiplexé sur AAL5

L2TP pour VC multiplexé sur AAL5 est une technique de remplacement de LLC L2TP encapsulée sur AAL5. Dans ce cas, la PDU L2TP est la charge utile AAL5 sans en-tête de LLC. Ceci est parfois appelé "encapsulation nulle".

Figure 2 – Format de PDU CPCS AAL5



Le champ Charge utile de PDU de sous couche de convergence de partie commune (CPCS, *Common Part Convergence Sub-layer*) contient jusqu'à 2^16 - 1 octets d'information d'utilisateur.

Le champ Bourrage de la PDU CPCS est destiné à tenir exactement dans les cellules ATM de telle façon que la charge utile de la dernière cellule de 48 octets créée par la sous couche SAR ait l'en-queue de PDU CPCS justifié à droite dans la cellule.

Le champ CPCS-UU (Indication d'usager à usager) est utilisé pour transférer de façon transparente les informations de CPCS d'usager à usager. Le champ n'a pas de fonction dans l'encapsulation ATM multi-protocole et PEUT être réglé à une valeur quelconque.

Le champ CPI (Indicateur de partie commune) aligne l'en-queue de la CPU CPCS sur 64 bits. Des fonctions supplémentaires possibles sont à l'étude à l'UIT-T. Lorsque la seule fonction d'alignement sur 64 bits est utilisée, ce champ DEVRA être codé par 0x00.

Le champ Longueur indique la longueur, en octets, du champ Charge utile. La valeur maximum du champ Longueur est de 65 535 octets. Un champ Longueur codé 0x00 PEUT être utilisé pour la fonction d'interruption.

Le champ CRC est calculé sur la PDU CPCS entière excepté le champ CRC lui-même.

La charge utile PDU CPCS DEVRA consister en une PDU L2TP comme défini dans la [RFC2661].

7. Signalisation de plan de contrôle hors bande

7.1 Établissement de connexion

Une connexion SVC peut avoir son origine au LAC ou au LNS. Une mise en œuvre qui accepte l'utilisation de SVC DOIT être capable à la fois de générer et de répondre aux demandes d'établissement de SVC. Sauf pour l'IE B-LLI spécifié ci-dessous, tous les autres IE nécessaires pour la spécification de signalisation d'interface usager-réseau (UNI, *User-Network Interface*) ATM version 4.0 [SIG40] devraient être codés selon la [RFC2331].

Lorsque il génère une connexion de SVC AAL5, l'appelant DOIT demander dans le message SETUP *(ÉTABLISSEMENT)* un VC L2TP multiplexé, une LLC L2TP encapsulée, ou les deux. L'IE B-LLI DEVRA être utilisé pour spécifier la méthode d'encapsulation demandée. Lorsque un appelant offre les deux encapsulations, les deux IE B-LLI DEVRONT être codés au sein d'un élément d'information Indicateur de répétition large bande dans l'ordre des préférences de l'envoyeur.

Une mise en œuvre DOIT être capable d'accepter un appel entrant qui offre LLC L2TP encapsulé dans la demande de l'appelant. La mise en œuvre de l'homologue appelé DOIT rejeter une demande d'établissement d'appel qui n'offre qu'une encapsulation qu'il ne prend pas en charge. Les mises en œuvre qui génèrent un appel en offrant les deux techniques de protocole d'encapsulation DOIVENT être capables d'accepter l'utilisation de l'une et l'autre technique d'encapsulation.

Lorsque il génère un appel LLC encapsulé qui doit porter une charge utile L2TP, le champ protocole de couche 2 d'information d'utilisateur d'IE B-LLI [Q.2931] DEVRA être codé à choisir le contrôle de liaison logique de LAN (ISO/IEC8802-2) dans l'octet 6. Voir un exemple dans l'Appendice A de la [RFC2331].

Lorsque il génère un appel de VC multiplexé qui doit porter une charge utile L2TP, le champ protocole de couche 2 d'information d'utilisateur d'élément d'information B-LLI [Q.2931] DEVRA être codé pour ne pas choisir de protocole de couche 2 dans l'octet 6 et le champ Protocole de couche 3 DEVRA être codé à choisir ISO/IEC TR 9577 [ISO9577] dans l'octet 7. De plus, selon le document du Forum DSL TR-037 [DSLF037], les octets d'extension spécifient un VC L2TP multiplexé en utilisant l'IPI SNAP, suivi par un OUI en la possession de l'IANA, suivi par le PID alloué par l'IANA pour L2TP. Donc, le champ Protocole de couche 3 d'informations d'utilisateur est codé : 0B 80 00 00 5E 00 07. Le champ Charge utile de la trame AAL5 va toujours contenir une PDU L2TP. L'IPI SNAP n'est employé que pour utiliser la valeur de protocole L2TP de l'IANA pour spécifier la PDU du VC multiplexée.

Si l'appelant offre les deux méthodes d'encapsulation et si l'homologue appelé accepte l'appel, l'homologue appelé DEVRA spécifier la méthode d'encapsulation en incluant exactement un IE B-LLI dans le message Connect.

Si un tunnel SVC est rétabli conformément au paragraphe 4.1 de la [RFC2661], les deux extrémités DOIVENT libérer le SVC. Toutes les sessions d'utilisateur sur le tunnel seront terminées par le rétablissement. L'une ou l'autre extrémité PEUT tenter de rétablir le tunnel à réception d'une nouvelle demande d'un client.

7.2 Échec d'établissement de connexion

Lors de l'échec de l'établissement d'une connexion, l'entité L2TP qui a tenté l'établissement de la connexion PEUT considérer que l'entité appelée est injoignable jusqu'à notification de la disponibilité de l'entité injoignable. Les conditions dans lesquelles une entité détermine qu'une autre est injoignable et comment elle détermine que l'autre est à nouveau disponible sont des décisions de la mise en œuvre.

7.3 Suppression de connexion

Lorsque il n'y a pas de session active sur un tunnel SVC, l'une ou l'autre extrémité PEUT facultativement libérer la connexion.

8. Échec de connexion

Sur notification qu'une connexion SVC AAL5 a été libérée, une mise en œuvre DEVRA éliminer le tunnel et remettre la connexion de contrôle à l'état repos.

9. Considérations pour la sécurité

La spécification de base du protocole de tunnelage de couche deux [RFC2661] expose les questions de base de sécurité qui concernent le tunnelage L2TP. Il est possible que la sécurité du tunnel L2TP sur AAL5 puisse être compromise par l'attaque du réseau de transport ATM lui-même. Le Forum ATM a publié un cadre de sécurité [AFSEC1] et une spécification de sécurité [AFSEC2] qui définissent les procédures pour se garder contre les menaces courantes qui pèsent sur un réseau de transport ATM. Les applications qui requièrent une protection contre les menaces concernant un réseau ATM commuté sont invitées à utiliser des en-têtes d'authentification, ou des charges utiles chiffrées, et/ou les services de sécurité de couche ATM décrits dans [AFSEC2].

10. Remerciements

Le présent document a largement emprunté les matériaux de "PPP sur AAL5" (RFC2364) de George Gross, Manu Kaycee, Arthur Lin, Andrew Malis, et John Stephens, et à un document antérieur de "L2TP sur AAL5" de Nagraj Arunkumar, Manu Kaycee, Tim Kwok, et Arthur Lin.

Des remerciements particuliers sont dus à Mike Davison, Arthur Lin, John Stevens pour leurs contributions significatives à la version initiale de ce document.

Un grand merci à David Allan de Nortel pour sa précieuse relecture du document.

La section sécurité de ce document se fonde sur la RFC 3337, "Extensions de classe pour PPP sur couche 2 d'adaptation en mode de transfert asynchrone (AAL2)", par Bruce Thompson, Bruce Buffam et Thima Koren.

11. Références

[AFSEC1] The ATM Forum, "ATM Security Framework Version 1.0", af-sec-0096.000, février 1998

[AFSEC2] The ATM Forum, "ATM Security Specification v1.1", af-sec-0100.002, mars 2001

[DSLF037] DSL Forum Technical Report TR-037, "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM", mars 2001.

[DUBR] ATM Forum, "Addendum to TM 4.1: Differentiated UBR", af-tm-0149.000, finalisé en juillet 2000 ; disponible à ftp://ftp.atmforum.com/pub.

[FRF8] The Frame Relay Forum, "Frame Relay/ATM PVC Service Interworking Implementation Agreement", FRF.8, avril 1995.

[ILMIA] ATM Forum, "Addendum to the ILMI Auto-configuration extension", af-nm-00165.000, avril 2001.

[ISO9577] ISO/IEC DTR 9577.2, "Information technology - Telecommunications and Information exchange between systems - Protocol Identification in the network layer", 1995-08- 16.

[ITU93] Recommadation UIT-T I.363, "B-ISDN ATM Adaptation Layer (AAL) Specification", mars 1993.

[Q.2931] Recommadation UIT-T Q.2931, "Broadband Integrated Service Digital Network (B-ISDN) Digital Subscriber Signaling System No.2 (DSS2) User Network Interface Layer 3 Specification for Basic Call/Connection Control", février 1995.

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

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

[RFC2331] M. Maher, "Prise en charge de la signalisation ATM pour IP sur ATM – Mise à jour de la signalisation UNI 4.0", avril 1998. *(P.S.)*

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de tunnelage de couche 2 "L2TP"", *(P.S.)*

[RFC2684] D. Grossman, J. Heinanen, "Encapsulation multiprotocole sur la couche 5 d'adaptation ATM", septembre 1999. *(P.S.)*

[SIG31] The ATM Forum, "ATM User-Network Interface Specification V3.1", af-uni-0010.002, 1994.

[SIG40] ATM Forum, "ATM User-Network Interface (UNI) Signaling Specification Version 4.0", af-sig-0061.000, finalisé en juillet 1996 ; disponible à ftp://ftp.atmforum.com/pub.

Appendice A Acronymes

AAL5 *(ATM Adaptation Layer Type 5)*	couche d'adaptation ATM de type 5
ATM *(Asynchronous Transfer Mode)*	technique temporelle asynchrone
B-LLI *(Broadband Low Layer Information)*	(élément d'information) Informations de couche basse haut débit
CPCS *(Common Part Convergence Sublayer)*	partie commune de sous-couche de convergence
FAI	fournisseur d'accès Internet
IANA *(Internet Assigned Numbers Authority)*	autorité d'allocation des numéros de l'Internet
IE (*Information Element)*	élément d'information ;
L2TP *(Layer 2 Tunnelling Protocol)*	protocole de tunnelage de couche 2 (RFC2661)
LAC *(L2TP Access Concentrator)*	concentrateur d'accès du protocole de tunnelage de couche 2
LLC *(Logical Link Control*	commande de liaison logique
LNS *(L2TP Network Server)*	serveur de réseau L2TP
MRU *(Maximum Receive Unit)*	unité de réception maximale
MTU *(Maximum Transfer Unit)*	unité maximum de transfert
OUI *(Organisation Unique Identifier)*	identifiant univoque d'organisation
PDU *(Protocol Data Unit)*	unité de données de protocole
PID *(Protocol Identifier)*	identifiant de protocole
PPP *(Point-to-Point Protocol)*	protocole point à point
PVC *(Permanent Virtual Circuit)*	circuit virtuel permanent
SAP *(Service Access Point)*	point d'accès au service
SNAP *(subnetwork access protocol)*	protocole d'accès à un sous-réseau
SVC *(Switched Virtual Circuit)*	circuit virtuel commuté
VC *(Virtual Circuit)*	circuit virtuel

Adresse des auteurs

Rollins Turner
Paradyne Corporation
8545 126th Avenue North
Largo, FL 33773
USA
mél : rturner@eng.paradyne.com

Rene Tio
Redback Networks, Inc.
300 Holger Way
San Jose, CA 95134
USA
mél : tor@redback.com

Ajoy Singh
Motorola
1421 West Shure Dr,
Arlington Heights, IL 60004
USA
mél : asingh1@motorola.com

Suhail Nanji
Redback Networks, Inc.
300 Holger Way
Sunnyvale, CA 95134
USA
mél : suhail@redback.com

Déclaration complète de droits de reproduction

Remerciement

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