

Groupe de travail Réseau  
**Request for Comments : 2719**  
 Catégorie : Information

L. Ong, Nortel Networks  
 I. Rytina & M. Garcia, Ericsson  
 H. Schwarzbauer & L. Coene, Siemens  
 H. Lin, Telcordia  
 I. Juhasz, Telia  
 M. Holdrege, Lucent  
 C. Sharp, Cisco Systems  
 octobre 1999

Traduction Claude Brière de L'Isle

## Cadre architectural pour le transport de signalisation

### Statut de ce mémoire

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de copyright

Copyright (C) The Internet Society (1999). Tous droits réservés.

### Résumé

Le présent document définit un cadre architectural et les exigences fonctionnelles pour le transport des informations de signalisation sur IP. Le cadre décrit les relations entre les entités fonctionnelles et physiques qui échangent des informations de signalisation, comme les passerelles de signalisation et les contrôleurs de passerelles de supports. Il identifie les interfaces où le transport de signalisation peut être utilisé et les exigences fonctionnelles et de performances qui s'appliquent à partir des protocoles de signalisation des réseaux à commutation de circuits (SCN, *Switched Circuit Network*) existants.

## Table des Matières

1. Introduction.....	2
1.1 Généralités.....	2
1.2 Terminologie.....	2
1.3 Domaine d'application.....	3
2. Architecture de transport de signalisation.....	3
2.1 Fonctions de composant de passerelle.....	3
2.2 Inter fonctionnement SS7 pour le contrôle de connexion.....	4
2.3 Inter fonctionnement RNIS pour le contrôle de connexion.....	5
2.4 Architecture pour l'accès aux bases de données.....	6
3. Architecture du protocole.....	7
3.1 Composants de transport de signalisation.....	7
3.2 Accès SS7 pour le contrôle de passerelle de supports.....	7
3.3 Accès Q.931 au MGC.....	7
3.4 Accès SS7 à IP/SCP.....	8
3.5 De SG à SG.....	9
4. Exigences fonctionnelles.....	9
4.1 Transport des protocoles de signalisation de SCN.....	9
4.2 Performances des protocoles de signalisation de SCN.....	10
5. Gestion.....	11
6. Considérations pour la sécurité.....	12
6.1 Exigences de sécurité.....	12
6.2 Mécanismes de sécurité actuellement disponibles dans les réseaux IP.....	12
7. Abréviations.....	13
8. Remerciements.....	13
9. Références.....	13
Adresse des auteurs.....	14
Déclaration complète de droits de reproduction.....	14

## 1. Introduction

### 1.1 Généralités

Le présent document définit un cadre architectural pour le transport des protocoles de signalisation fondés sur le message sur les réseaux IP. Le domaine d'application de ce travail comporte la définition des méthodes d'encapsulation, des mécanismes de protocole de bout en bout et d'utilisation des capacités IP existantes pour prendre en charge les exigences fonctionnelles et de performances pour le transport de la signalisation.

La portion cadre décrit les relations entre les entités fonctionnelles et physiques utilisées dans le transport de la signalisation, y compris le cadre du contrôle des passerelles de supports, et d'autres scénarios où le transport de la signalisation peut être nécessaire.

La portion exigences décrit les exigences fonctionnelles et de performances pour le transport de la signalisation comme le contrôle des flux, la livraison en séquence et d'autres fonctions qui peuvent être requises pour des protocoles de signalisation spécifiques de SCN.

### 1.2 Terminologie

Les termes généraux suivants sont utilisés dans le présent document :

Transport arrière (*backhaul*) : se réfère au transport de la signalisation depuis le point d'interface pour le flux de données associé (c'est-à-dire, la fonction de passerelle de signalisation dans l'unité de passerelle de supports) jusque au point de traitement de l'appel (c'est-à-dire, l'unité de contrôle de passerelle de supports) si ce n'est pas local.

Transport de signalisation (SIG, *Signaling Transport*) : se réfère à une pile de protocoles pour le transport des protocoles de signalisation de SCN sur un réseau IP. Il va prendre en charge les primitives standard pour l'interface avec une application de signalisation de SCN non modifiée qui est transportée, et ajouter en dessous un protocole de transport IP standard avec des fonctions conçues pour satisfaire aux exigences de transport de la signalisation de SCN.

Réseau à commutation de circuit (SCN, *Switched Circuit Network*) : le terme de SCN est utilisé pour se référer à un réseau qui porte du trafic au sein de supports organisés en canaux de tailles prédéfinies. Des exemples en sont les réseaux téléphoniques publics commutés (RTPC, en anglais PSTN, *Public Switched Telephone Network*) et les réseaux mobiles terrestres publics (RMTP, en anglais PLMN, *Public Land Mobile Network*). Des exemples des protocoles de signalisation utilisés dans les SCN sont Q.931, et les sous-systèmes MTP niveau 3 et Application/Utilisateur du système de signalisation n° 7.

Les termes suivants décrivent des entités fonctionnelles qui se rapportent au transport de signalisation dans un modèle de passerelle répartie.

Passerelle de supports (MG, *Media Gateway*) : une MG termine les flux de supports de SCN, met en paquet les données du support, si elles ne le sont déjà, et livre le trafic mis en paquet au réseau de paquets. Elle effectue ces fonctions en ordre inverse pour les flux de supports qui s'écoulent du réseau de paquets vers le SCN.

Contrôleur de passerelle de supports (MGC, *Media Gateway Controller*) : un MGC traite l'enregistrement et la gestion des ressources à la MG. Le MGC peut avoir la capacité d'autoriser l'utilisation de ressources sur la base de politiques locales. Pour les besoins du transport de la signalisation, le MGC sert éventuellement de point de terminaison et d'origine des protocoles d'application de SCN, comme le sous-système utilisateur RNIS du SS7 et le DSS1 de Q.931.

Passerelle de signalisation (SG, *Signaling Gateway*) : c'est un agent de signalisation qui envoie/reçoit la signalisation de SCN native à la bordure du réseau IP. La fonction de SG peut relayer, traduire ou terminer la signalisation SS7 dans une passerelle SS7-Internet. La fonction de SG peut aussi être corésidente avec la fonction de MG pour traiter la signalisation de SCN associée avec les terminaisons de ligne ou de réseau contrôlées par la MG (par exemple, le transport arrière de signalisation).

Les termes suivants décrivent des entités physiques qui se rapportent au transport de signalisation dans un modèle de passerelle répartie :

Unité de passerelle de supports (MGU, *Media Gateway Unit*) : c'est une entité physique qui contient la fonction de MG. Elle peut contenir d'autres fonctions, en particulier une fonction de SG pour traiter la signalisation associée à des facilités.

Unité de contrôle de passerelle de supports (MGCU, *Media Gateway Control Unit*) : c'est une entité physique qui contient

la fonction de MGC.

Unité de passerelle de signalisation (SGU, *Signaling Gateway Unit*) : c'est une entité physique qui contient la fonction de SG.

Point d'extrémité de signalisation (SEP, *Signaling End Point*) : c'est un nœud dans un réseau SS7 qui est l'origine ou la terminaison des messages de signalisation. Un commutateur central en est un exemple.

Point de transfert de signal (STP, *Signal Transfer Point*) : c'est un nœud dans un réseau SS7 qui achemine les messages de signalisation sur la base de leur codet de destination dans le réseau SS7.

### 1.3 Domaine d'application

Le transport de signalisation assure un transport transparent sur les réseaux IP des protocoles de signalisation fondés sur le message. Le domaine d'application du présent travail inclut la définition des méthodes d'encapsulation, des mécanismes de protocole de bout en bout et l'utilisation des capacités IP pour prendre en charge les exigences fonctionnelles et de performances pour la signalisation.

Le transport de la signalisation devra être utilisé pour transporter la signalisation de SCN entre une unité de passerelle de signalisation et une unité de contrôleur de passerelle de supports. Le transport de signalisation peut aussi être utilisé pour transporter de la signalisation fondée sur le message entre une unité de passerelle de supports et une unité de contrôle de passerelle de supports, entre des unités dispersées de contrôleur de passerelle de supports, et entre deux unités de passerelle de signalisation qui connectent des points d'extrémité de signalisation ou des points de transfert de signal dans le SCN.

Le transport de la signalisation sera défini d'une façon telle qu'il prenne en charge l'encapsulation et le portage de divers protocoles de SCN. Il est défini de façon à être indépendant de toutes fonctions de traduction de protocole de SCN ayant lieu aux points d'extrémité du transport de signalisation, car sa fonction se limite au transport du protocole de SCN.

Comme la fonction fournie est le transport transparent, les domaines suivants sont considérés comme sortant du domaine d'application du travail sur le transport de signalisation :

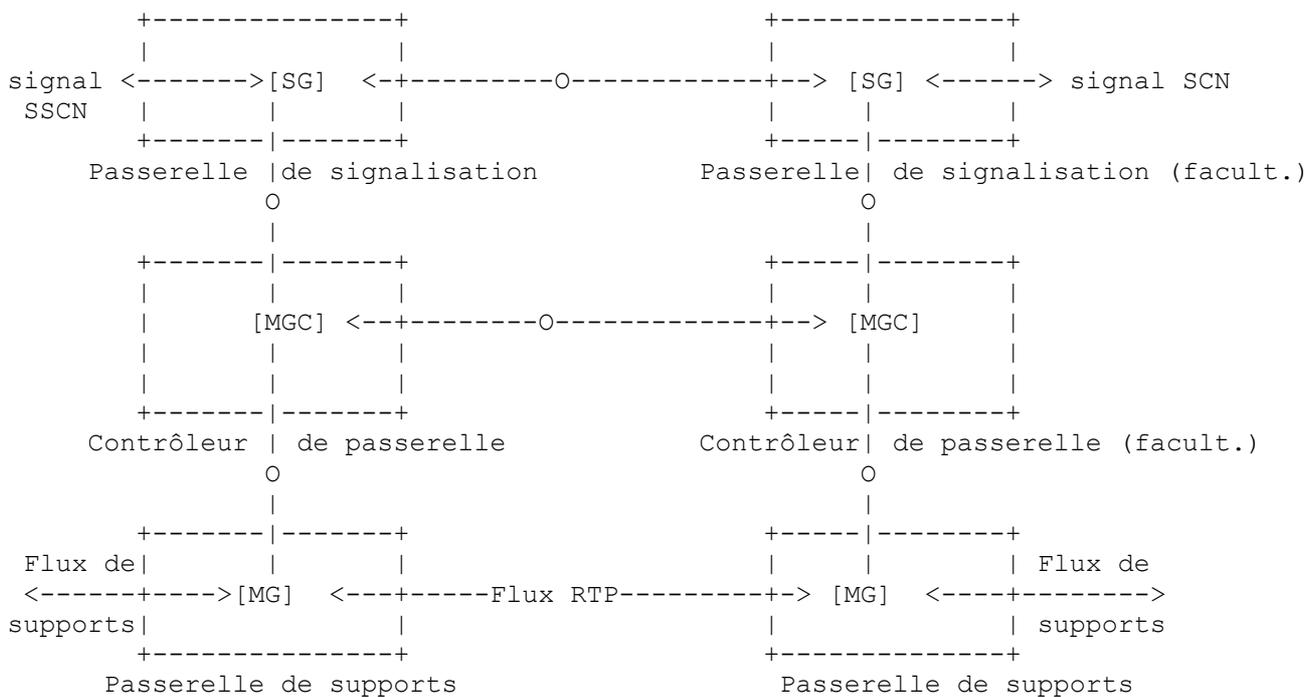
- définition des protocoles de SCN eux-mêmes,
- inter fonctionnement de signalisation tel que la conversion de la signalisation associé au canal (CAS, *Channel Associated Signaling*) en messages de protocole de signalisation,
- spécification des fonctions prenant place au sein de la SGU ou de la MGU,
- en particulier, le présent travail ne traite pas la question de savoir si la SGU assure une médiation/inter fonctionnement, car elle est transparente à la fonction de transport,
- de même, certaines fonctions de gestion et d'adressage qui ont lieu au sein de la SGU ou MGU sont aussi considérées comme sortant de son domaine d'application, comme la détermination de l'adresse IP de destination pour la signalisation, ou les procédures spécifiques d'attestation des performances de la session de transport (c'est-à-dire, des fonctions de vérification et de preuve).

## 2. Architecture de transport de signalisation

### 2.1 Fonctions de composant de passerelle

La Figure 1 définit un modèle fonctionnel commun qui sépare les fonctions de SG, MGC et MG. Ce modèle peut être mis en œuvre d'un certain nombre de façons, avec des fonctions mises en œuvre dans des appareils distincts ou combinées dans une seule unité physique.

Lorsque il existe une séparation physique entre les entités fonctionnelles, le transport de signalisation peut être appliqué pour assurer que les informations de signalisation de SCN sont transportées entre les entités avec les fonctionnalités et les performances requises.



**Figure 1 : Modèle fonctionnel de transport de signalisation**

Comme exposé ci-dessus, les interfaces qui appartiennent au transport de signalisation incluent SG à MGC, SG à SG. Le transport de signalisation peut éventuellement être aussi bien appliqué aux interfaces de MGC à MGC ou de MG à MGC, selon les exigences pour le transport du protocole de signalisation associé.

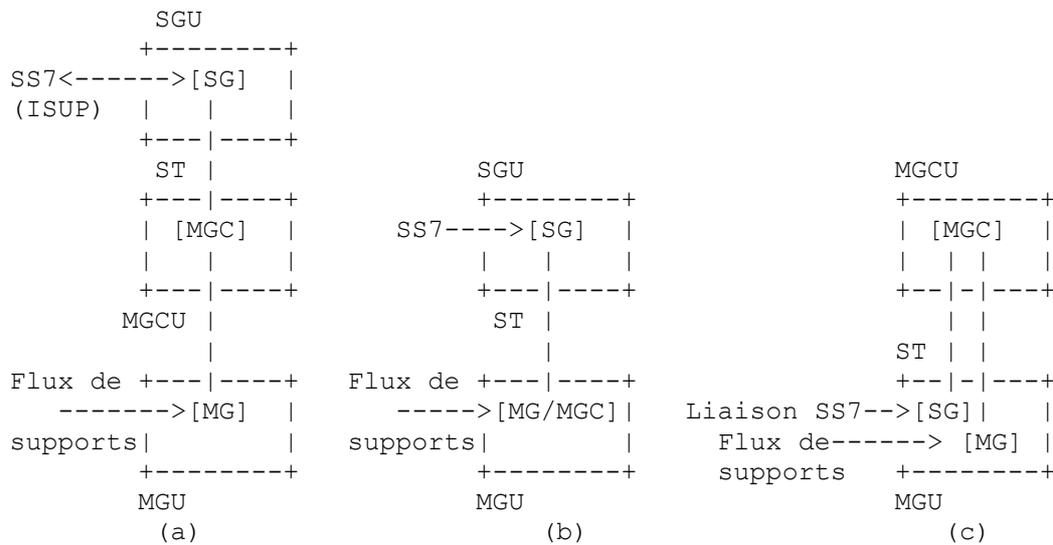
## 2.2 Inter fonctionnement SS7 pour le contrôle de connexion

La Figure 2 ci-dessous donne des exemples de mise en œuvre de ces fonctions dans des entités physiques utilisées pour l'inter fonctionnement de réseaux SS7 et IP pour la voix sur IP, la voix sur ATM, des serveurs d'accès au réseau, etc. Aucune recommandation n'est faite sur la répartition fonctionnelle et de nombreux autres exemples sont possibles mais ne sont pas présentés pour rester concis. L'utilisation du transport de signalisation est indépendante de la mise en œuvre.

Pour inter fonctionner avec les réseaux SCN contrôlés par SS7, la SG termine la liaison SS7 et transfère les informations de signalisation au MGC en utilisant le transport de signalisation. La MG termine la jonction d'inter commutation et contrôle la jonction en s'appuyant sur la signalisation de contrôle qu'elle reçoit du MGC. Comme montré ci-dessous dans le cas (a), la SG, le MGC et la MG peuvent être mis en œuvre dans des unités physiques distinctes, ou comme dans le cas (b), le MGC et la MG peuvent être mis en œuvre dans une seule unité physique.

Dans l'autre cas (c), une liaison SS7 associée à une facilité se termine par le même appareil (c'est-à-dire, la MGU) qui termine la jonction d'inter commutation. Dans ce cas, la fonction de SG est colocalisée avec la fonction de MG, comme on le montre ci-dessous, et le transport de signalisation est utilisé pour "transporter vers l'arrière" la signalisation de contrôle vers la MGCU.

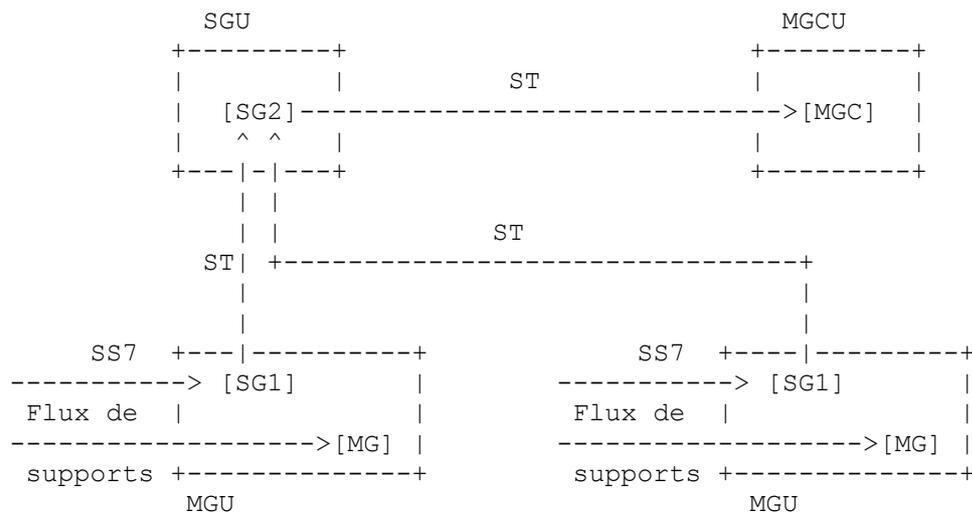
Note : Les liaisons SS7 peuvent aussi être terminées directement sur la MGCU par interconnexion au niveau physique avant ou à la MGU.



Note : ST = Transport de signalisation utilisé pour porter la signalisation de SCN

**Figure 2 : Exemples de mises en œuvre**

Dans certaines mises en œuvre, la fonction de la SG peut être divisée en plusieurs entités physiques pour des raisons d'adaptabilité de la gestion et de l'adressage du réseau de signalisation. Donc, le transport de signalisation peut être utilisé entre les SG aussi bien que de SG à MGC. C'est ce que montre la Figure 3 ci-dessous.



**Figure 3 : Cas de SG multiple**

Dans cette configuration, il peut y avoir plus d'une MGU qui traite une facilité associée à la signalisation (c'est-à-dire, plus d'une contenant sa propre fonction de SG) et seulement une SGU. Il sera donc possible de transporter une couche SS7 entre SG1 et SG2, et une autre couche SS7 entre SG2 et MGC. Par exemple, SG1 pourrait transporter MTP3 à SG2, et SG2 pourrait transporter ISUP au MGC.

**2.3 Inter fonctionnement RNIS pour le contrôle de connexion**

Dans la signalisation d'accès RNIS, le canal de signalisation est porté avec les canaux de données, de sorte que la fonction de SG pour le traitement de la signalisation Q.931 est colocalisé avec la fonction de MG pour le traitement du flux de données. Lorsque Q.931 est ensuite transporté au MGC pour le traitement de l'appel, le transport de la signalisation va être utilisé entre la fonction de SG et le MGC. C'est ce que montre la Figure 3 ci-dessous.

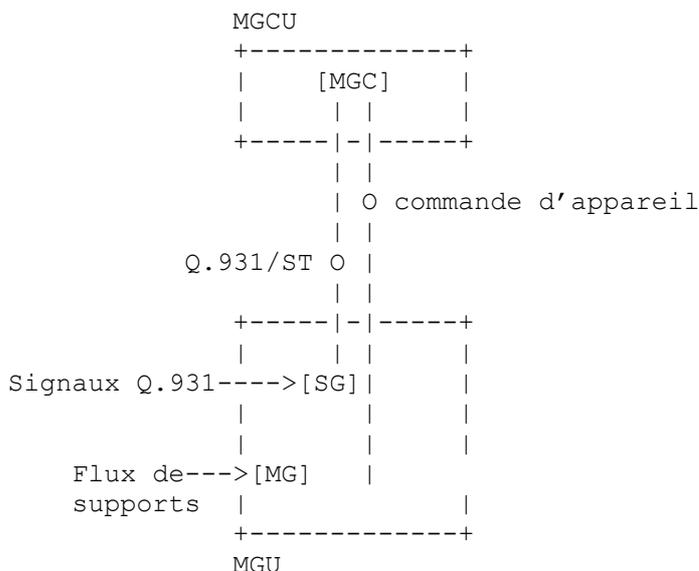


Figure 4 : Modèle de transport Q.931

2.4 Architecture pour l'accès aux bases de données

Le sous-système application pour la gestion des transactions (TCAP, *Transaction Capabilities*) est, au sein du SS7, la partie application qui est utilisée pour la signalisation qui ne se rapporte pas aux circuits.

La signalisation TCAP au sein des réseaux IP peut être utilisée pour un accès croisé entre des entités dans le domaine SS7 et le domaine IP, comme, par exemple :

- l'accès d'un réseau SS7 à un point de contrôle de service (SCP, *Service Control Point*) dans IP,
- l'accès d'un réseau SS7 à un MGC,
- l'accès d'un MGC à un élément de réseau SS7,
- l'accès d'un SCP IP à un élément de réseau SS7.

Un modèle fonctionnel de base pour TCAP sur IP est montré à la Figure 5.

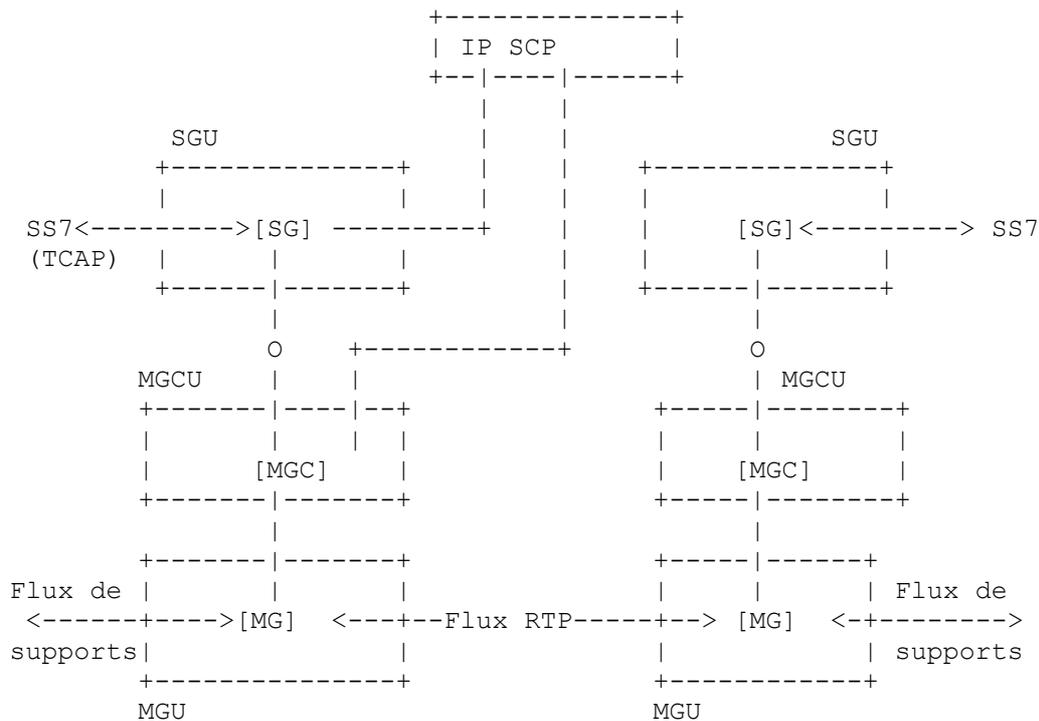


Figure 5 : Signalisation TCAP sur IP

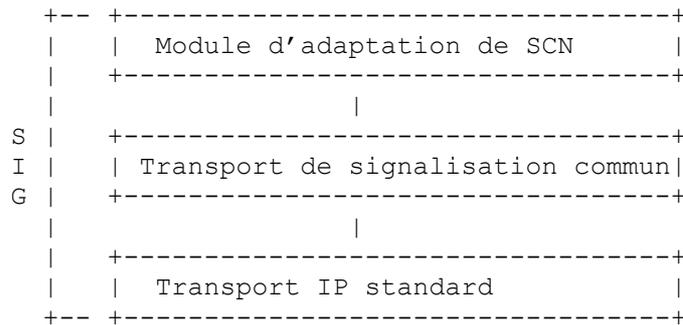
### 3. Architecture du protocole

La présente section donne une série d'exemples d'architecture de protocole pour l'utilisation du transport de signalisation (SIG, *Signaling Transport*).

#### 3.1 Composants de transport de signalisation

Le transport de signalisation dans les figures d'architecture de protocole ci-dessous est supposé comporter trois composants (Figure 6) :

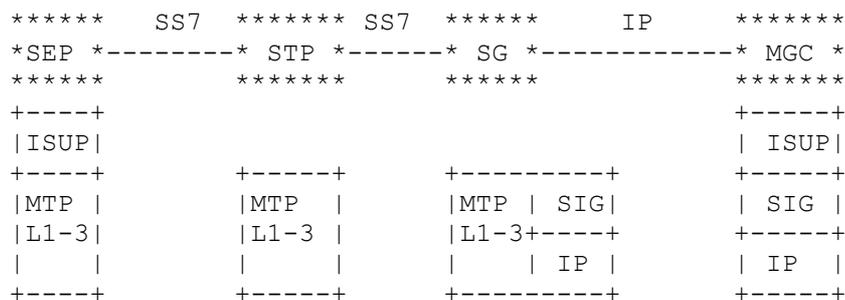
- 1) une sous-couche d'adaptation qui prend en charge les primitives spécifiques, par exemple, les indications de gestion, requises par un protocole d'application de signalisation d'un SCN particulier,
- 2) un protocole de transport de signalisation commun qui prend en charge un ensemble commun de fonctions de transport fiables pour le transport de signalisation,
- 3) un protocole de transport IP standard, non modifié.



**Figure 6 : Composants de transport de signalisation**

#### 3.2 Accès SS7 pour le contrôle de passerelle de supports

Ce paragraphe montre l'architecture de protocole pour le transport de signalisation qui prend en charge l'accès SS7 pour le contrôle de passerelle de supports.

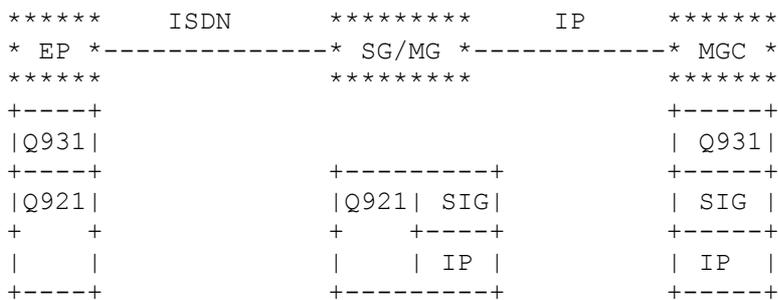


STP – Point de transfert de signal ; SEP – Point d'extrémité de signalisation  
 SG – Passerelle de signalisation ; SIG – Transport de signalisation  
 MGC – Contrôleur de passerelle de supports

**Figure 7 : Accès SS7 au MGC**

#### 3.3 Accès Q.931 au MGC

Ce paragraphe montre une architecture de protocole pour le transport de signalisation prenant en charge l'accès RNIS en point à point (Q.931) pour le contrôle de passerelle de supports.



MG/SG – Passerelle de supports avec une fonction de SG pour le transport arrière  
 EP - Point d'extrémité RNIS

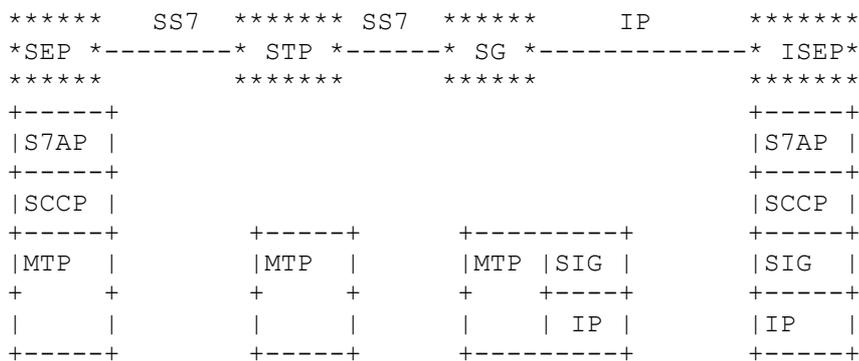
**Figure 8 : Accès RNIS**

**3.4 Accès SS7 à IP/SCP**

Ce paragraphe donne une architecture de protocole pour l'accès de base de données, fournissant par exemple la signalisation entre deux nœuds de réseau intelligent ou deux nœuds de réseau mobile. Il existe un certain nombre de scénarios pour les piles de protocoles et la fonctionnalité contenue dans le SIG, selon l'application du SS7.

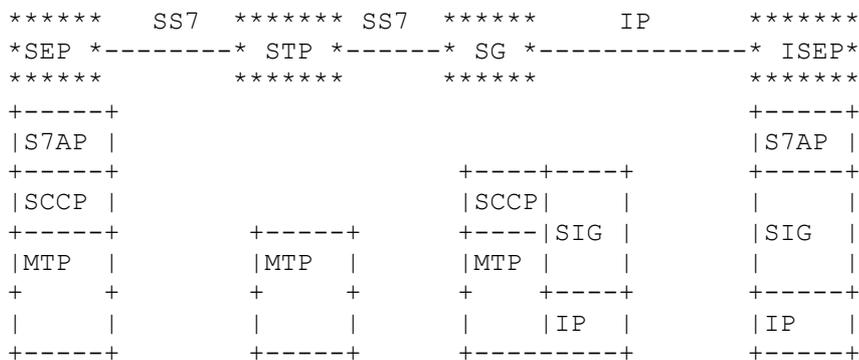
Dans les diagrammes, le sous-système d'application du SS7 (S7AP) est utilisé en général pour couvrir tous les sous-systèmes d'application (par exemple, MAP, IS-41, INAP, etc.). Selon le protocole transporté, S7AP peut inclure ou non TCAP. L'interface à la couche SS7 en dessous de S7AP peut être soit l'interface TC-usager soit l'interface SCCP-usager.

La Figure 9a montre le scénario où SCCP est le protocole de signalisation transporté entre la SG et un point d'extrémité de signalisation IP (ISEP) c'est-à-dire, une destination IP qui prend en charge des protocoles d'application SS7.



**Figure 9a : Accès SS7 au nœud IP - SCCP étant transporté**

La Figure 9b montre le scénario où S7AP est le protocole de signalisation transporté entre la SG et l'ISEP. Selon le protocole transporté, S7AP peut inclure ou non TCAP, ce qui implique que SIG doit être capable de prendre en charge les deux interfaces TC-usager et SCCP-usager.



**Figure 9b : Accès SS7 au nœud IP - S7AP étant transporté**

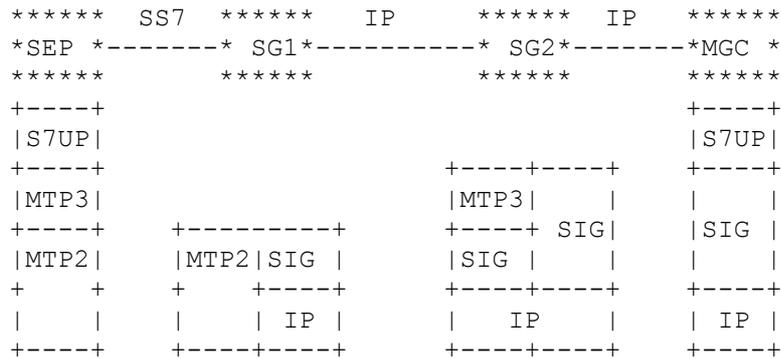
### 3.5 De SG à SG

Ce paragraphe donne une architecture de protocole pour la prise en charge de la signalisation entre deux points d'extrémité dans un réseau de signalisation de SCN, en utilisant le transport de signaux directement entre deux SG.

La figure qui suit décrit l'architecture de protocole pour un scénario avec deux SG qui fournissent des niveaux de fonction différents pour l'inter fonctionnement de SS7 et de IP. Cela correspond au scénario de la Figure 3.

Le sous-système utilisateur SS7 (S7UP) présenté est un protocole SS7 qui utilise MTP directement pour le transport au sein du réseau SS7, par exemple, ISUP.

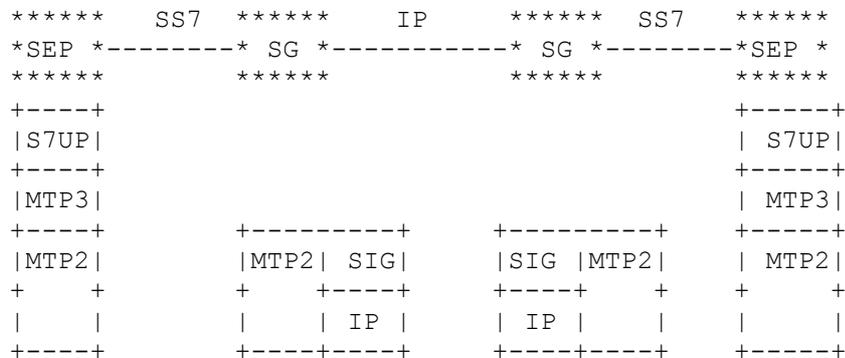
Dans ce scénario, il y a deux cas d'utilisation différents de SIG, un qui transporte la signalisation MTP3, l'autre qui transporte la signalisation ISUP.



S7UP – sous-système utilisateur du SS7

**Figure 10 : de SG à SG, cas 1**

La figure suivante décrit une utilisation plus générique de l'inter fonctionnement SS7-IP pour le transport de la signalisation SS7 de couche supérieure à travers un réseau IP, où les points d'extrémité sont tous deux des SEP du SS7.



**Figure 11 : de SG à SG, cas 2**

## 4. Exigences fonctionnelles

### 4.1 Transport des protocoles de signalisation de SCN

Le transport de signalisation assure le transport des messages natifs de protocole de SCN sur un réseau à commutation de paquets.

Le transport de signalisation devra :

- 1) Transporter divers types de protocoles de SCN, tels que les sous-systèmes application et utilisateur de SS7 (y compris MTP niveau 3, ISUP, SCCP, TCAP, MAP, INAP, IS-41, etc.) et la couche 3 des protocoles DSS1/PSS1 (c'est-à-dire, Q.931 et QSIG).
- 2) Fournir un moyen d'identifier le protocole de SCN particulier qui est transporté.
- 3) Fournir un protocole de base commun qui définisse les formats d'en-tête, les extensions et procédures de sécurité pour

le transport de signalisation, et prendre en charge les extensions nécessaires pour ajouter des protocoles de SCN individuels si et quand ils sont requis.

- 4) En conjonction avec le protocole réseau sous-jacent (IP), fournir la fonctionnalité pertinente définie par la couche inférieure de SCN appropriée.

La fonctionnalité pertinente peut inclure (selon le protocole transporté) :

- le contrôle de flux,
- la livraison en séquence des messages de signalisation au sein d'un flux de contrôle,
- l'identification logique des entités sur lesquelles les messages de signalisation débutent ou se terminent,
- l'identification logique de l'interface physique contrôlée par le message de signalisation,
- la détection d'erreurs,
- la récupération d'une défaillance de composants sur le chemin de transit,
- la retransmission et autres méthodes de correction d'erreurs,
- la détection de l'indisponibilité des entités homologues.

Par exemple :

- si le protocole SCN natif est ISUP ou SCCP, la fonctionnalité pertinente fournie par MTP2/3 devra être fournie,
- si le protocole SCN natif est TCAP, la fonctionnalité pertinente fournie par les classes sans connexion de SCCP et MTP 2/3 devra être prise en charge,
- si le protocole SCN natif est Q.931, la fonctionnalité pertinente fournie par Q.921 devra être prise en charge,
- si le protocole SCN natif est MTP3, la fonctionnalité pertinente de MTP2 devra être prise en charge.

- 5) Prendre en charge la capacité de multiplexer plusieurs sessions de SCN de couche supérieure sur une session de transport de signalisation sous-jacente. Cela permet, par exemple, que plusieurs sessions de canal D de DSS1 soient portées dans une session de transport de signalisation.

En général, la livraison en séquence est exigée pour les messages de signalisation au sein d'un seul flux de contrôle, mais n'est pas nécessairement requise pour les messages qui appartiennent à des flux de contrôle différents. Le protocole devrait si possible tirer parti de cette propriété pour éviter de bloquer la livraison des messages dans un flux de contrôle à cause d'erreurs de séquence au sein d'un autre flux de contrôle. Le protocole devrait aussi permettre à la SG d'envoyer des flux de contrôle différents à différents accès de destination si désiré.

- 6) Être capable de transporter des messages complets de longueur supérieure aux limitations de segmentation/réassemblage du SCN. Par exemple, le transport de signalisation ne devrait pas être restreint par les limitations de longueur définies pour le protocole de couche inférieure SS7 (par exemple 272 octets dans le cas de SS7 en bande étroite) mais devrait être capable de porter de plus longs messages sans exiger de segmentation.
- 7) Permettre une gamme de schémas de sécurité d'une robustesse convenable pour protéger les informations de signalisation transportées à travers les réseaux. Par exemple, le transport de signalisation devra être capable de fonctionner sur des sessions gérées par des mandataires, et être capable de passer à travers des pare-feu.
- 8) Assurer l'évitement d'encombrement sur l'Internet, en prenant en charge les contrôles appropriés sur la génération du trafic de signalisation (y compris la signalisation générée dans le SCN) et la réaction à l'encombrement du réseau.

## 4.2 Performances des protocoles de signalisation de SCN

Ce paragraphe donne les valeurs de base concernant les exigences de performances des protocoles clés de SCN à transporter. Actuellement, seuls les protocoles de SCN fondés sur le message sont pris en compte. Ne pas réussir à satisfaire à ces exigences résultera vraisemblablement en un comportement inapproprié et indésirable de la signalisation et des appels.

### 4.2.1 Exigences pour la MTP SS7

Les exigences de performances ci-dessous ont été spécifiées pour le transport des messages de gestion de réseau de MTP niveau 3. Les exigences données ici ne sont applicables que si tous les message MTP de niveau 3 sont à transporter sur le réseau IP.

Délai du message

- Les procédures d'homologue à homologue de MTP niveau 3 exigent une réponse dans les 500 à 1200 ms. Cette valeur inclut le temps d'aller-retour et de traitement à l'extrémité distante. Échouer à satisfaire à cette limitation va résulter en l'initiation des procédures d'erreur pour les temporisateurs spécifiques, par exemple, le temporisateur T4 de la Recommandation UIT-T Q.704.

#### 4.2.2 Exigences pour la MTP SS7 niveau 3

Les exigences de performances ci-dessous ont été spécifiées pour le transport des messages du sous-système d'utilisateur de MTP niveau 3 au titre des Recommandations de l'UIT-T sur le système de signalisation n° 7 [SS7].

Perte de message

- Pas plus de 1 sur 10E+7 messages ne sera perdu à cause d'un échec du transport.

Erreur de séquence

- Pas plus de 1 sur 10E+10 messages ne sera livré déclassé (y compris les messages dupliqués) à cause d'un échec du transport.

Erreurs de message

- Pas plus de 1 sur 10E+10 ne devra contenir d'erreur non détectée par le protocole de transport (l'exigence est de 10E+9 pour les spécifications de l'ANSI).

Disponibilité

- La disponibilité de tout ensemble de chemins de signalisation est de 99,9998 % ou mieux, c'est-à-dire, un temps d'arrêt du système de 10 min/an ou moins. Un ensemble de chemins de signalisation est l'ensemble complet de chemins de signalisation permis d'un certain point de signalisation vers une destination spécifique.

Longueur de message (charge utile acceptée des sous-systèmes utilisateur SS7)

- 272 octets pour SS7 à bande étroite, 4091 octets pour SS7 à haut débit.

#### 4.2.3 Exigences du sous-système utilisateur SS7

Une analyse plus détaillée des exigences du sous-système d'utilisateur du SS7 se trouve dans [Lin].

Délai du message ISUP – exigences du temporisateur du protocole

- Un exemple des exigences du temporisateur ISUP est la procédure de l'essai de continuité, qui exige qu'une tonalité générée du côté envoyeur soit retournée de l'extrémité receveuse dans les 2 secondes de l'envoi d'un IAM indiquant un essai de continuité. Cela implique qu'un transport de message de signalisation unidirectionnel, plus l'accomplissement des fonctions nodales, doit se faire en moins de 2 secondes.

Délai du message ISUP – exigences de bout en bout

- Les exigences pour le délai d'établissement d'appel de bout en bout dans l'ISUP sont qu'un message de réponse de bout en bout soit reçu dans les 20 à 30 secondes de l'envoi de l'IAM. Note : bien que ce soit la valeur du temporisateur de garde du protocole, les utilisateurs vont généralement s'attendre à un temps de réponse plus court.

Exigences de TCAP – exigences de délai

- TCAP ne définit pas par lui-même d'ensemble d'exigences de délai. Un travail a été effectué [Lin2] pour identifier les exigences de délai en fonction de l'application pour TCAP.

#### 4.2.4 Exigences de signalisation du RNIS

Délai de message Q.931

- Le délai d'aller-retour ne devrait pas excéder 4 secondes. Un temporisateur de cette durée est utilisé pour un certain nombre de procédures, en particulier, LIBÉRATION/LIBÉRATION\_ACHEVÉE et CONNEXION/ACCUSÉ\_DE RÉCEPTION\_DE\_CONNEXION où un délai excessif peut résulter en une action de gestion sur le canal, ou en la libération d'un appel en cours d'établissement. Noter que bien que cette valeur soit indiquée par les spécifications de temporisateur du protocole, l'utilisateur s'attend normalement à un temps de réponse plus court.

- Un temporisateur de 12 s (T309) est utilisé pour entretenir un appel actif en cas de perte de la liaison de données, pendant le rétablissement. Les documents d'ETSI qui s'y rapportent spécifient une valeur maximum de 4 secondes tandis que les spécifications de l'ANSI [T1.607] ont une valeur par défaut de 90 secondes.

-

## 5. Gestion

Le fonctionnement l'administration et la gestion (OA&M, *Operations, Administration & Management*) des réseaux IP ou des réseaux SCN sort du domaine d'application de SIGTRAN. Des exemples d'OA&M incluent les systèmes traditionnels de gestion du téléphone ou les gestionnaires de SNMP de l'IETF. Les mises en œuvre et les utilisateurs d'OA&M devraient être conscients des interactions fonctionnelles de la SG, du MGC et de la MG avec les unités physiques qu'ils occupent.

## 6. Considérations pour la sécurité

### 6.1 Exigences de sécurité

Lorsque de la signalisation en rapport avec un SCN est transportée sur un réseau IP, deux scénarios de réseau possibles peuvent être distingués :

- Signalisation transportée seulement au sein d'un Intranet ;  
Les mesures de sécurité sont appliquée à la discrétion du gestionnaire du réseau.
- Signalisation transportée, au moins dans une certaine mesure, dans l'Internet public ;  
L'Internet public devrait généralement être considéré comme un réseau "non sûr" et l'utilisation de mesures de sécurité est requise.

La sécurité comporte généralement plusieurs aspects

- Authentification : elle est exigée pour s'assurer que les informations sont envoyées de/vers un partenaire connu et de confiance.
- Intégrité : elle est requise pour s'assurer que les informations n'ont pas été modifiées dans le transit.
- Confidentialité : elle peut être parfois requise pour s'assurer que les informations transportées sont chiffrées pour éviter une utilisation illégale.
- Disponibilité : il est exigé que les points d'extrémité en communication restent en service pour une utilisation autorisée même pendant une attaque.

### 6.2 Mécanismes de sécurité actuellement disponibles dans les réseaux IP

Plusieurs mécanismes de sécurité sont actuellement disponibles dans les réseaux IP.

- IPSEC ([RFC2401]):  
IPSEC fournit des services de sécurité à la couche IP qui traitent les exigences sus-mentionnées. Il définit les deux protocoles AH et ESP qui fournissent essentiellement les services respectivement de protection de l'intégrité des données et de la confidentialité.

Le mécanisme ESP peut être utilisé dans deux modes différents :

- mode transport ;
- mode tunnel.

En mode transport, IPSEC protège la portion des données de protocole de couche supérieure d'un paquet IP, tandis qu'en mode tunnel, un paquet IP complet est encapsulé dans un tunnel IP sûr.

Si le point d'extrémité SIG incorpore des adresses IP en dehors de la SA/DA dans l'en-tête IP, le passage à travers une fonction de NAT va poser des problèmes. La même chose est vraie pour l'utilisation de IPsec en général, sauf si une fonction RSIP IPsec est utilisée comme décrit dans la [RFC2663].

L'utilisation de IPSEC n'entrave pas l'utilisation de TCP ou d'UDP comme base sous-jacente de SIG. Si la distribution automatique des clés est requise, le protocole IKE ([RFC2409]) peut être appliqué.

- SSL, TLS ([RFC2246]) : SSL et TLS fournissent aussi des services de sécurité appropriés mais ne fonctionnent que par dessus TCP/IP.

Il n'est pas nécessaire de définir de nouveaux mécanismes de sécurité dans SIG, car l'utilisation des mécanismes actuellement disponibles est suffisante pour assurer la sécurité nécessaire. Il est recommandé que IPSEC ou une méthode équivalente soit utilisé, en particulier lors du transport de la signalisation de SCN sur l'Internet public.

## 7. Abréviations

CAS (*Channel-Associated Signaling*) signalisation associée au canal  
 DSS1 (*Digital Subscriber Signalling System no.1*) système de signalisation n°1 pour abonné numérique  
 INAP (*Intelligent network application part*) sous-système application du réseau intelligent  
 ISEP (*IP Signaling End Point*) point d'extrémité de signalisation IP  
 ISUP (*ISDN User Part (of signalling system No. 7)*) sous-système Utilisateur RNIS (du système de signalisation n°7) ;  
 MAP (*Mobile Application Part*) sous-système application mobile  
 MG (*Media Gateway*) passerelle de supports  
 MGU (*Media Gateway Unit*) unité de passerelle de supports  
 MGC (*Media Gateway Controller*) contrôleur de passerelle de supports  
 MGCU (*Media Gateway Controller Unit*) unité de contrôleur de passerelle de supports  
 MTP (*Signaling System 7 Message Transfer Part*) sous-système transfert de message du système de signalisation n° 7  
 PLMN (*Public Land Mobile Network*) RMTP, réseau mobile terrestre public  
 PSTN (*Public Switched Telephone Network*) RTPC, réseau téléphonique public commuté  
 S7AP (*SS7 Application Part*) sous-système application du système de signalisation n° 7  
 S7UP (*SS7 User Part*) sous-système utilisateur du système de signalisation n° 7  
 SCCP (*Signalling Connection Control Part*) SSCS, sous-système de commande de connexions sémaphores  
 SCN (*Switched Circuit Network*) réseau à commutation de circuits  
 SEP (*Signaling End Point*) point d'extrémité de signalisation  
 SG (*Signaling Gateway*) passerelle de signalisation  
 SIG (*Signaling Transport protocol stack*) pile de protocoles de transport de signalisation  
 SS7 (*Signaling System No. 7*) système de signalisation n° 7  
 TCAP (*Transaction Capabilities Part*) SSGT, sous-système application pour la gestion des transactions du SS7

## 8. Remerciements

Les auteurs tiennent à remercier K. Chong, I. Elliott, Ian Spiers, Al Varney, Goutam Shaw, C. Huitema, Mike McGrew et Greg Sidebottom de leurs précieux commentaires et suggestions.

## 9. Références

- [Lin] Lin, H., Seth, T., et al., "Performance Requirements for Signaling in Internet Telephony", (*non publiée*)
- [Lin2] Lin, H., et al., "Performance Requirements for TCAP Signaling in Internet Telephony", (*non publiée*)
- [PSS1/QSIG] ISO/CEI 11572 éd. 2 (1997-06), "Technologies de l'information - télécommunications et échange d'informations entre systèmes – réseaux privés à intégration de services – services support en mode circuit – procédures et protocole de signalisation inter-échange".
- [Q.931/DSS1] Recommandation UIT-T Q.931, "Spécification de la couche 3 d'interface usager-réseau RNIS", mai 1998
- [RFC2246] T. Dierks et C. Allen, "[Protocole TLS version 1.0](#)", janvier 1999.
- [RFC2401] S. Kent et R. Atkinson, "[Architecture de sécurité](#) pour le protocole Internet", novembre 1998. (*Obsolète, voir [RFC4301](#)*)
- [RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. (*Obsolète, voir la [RFC4306](#)*)
- [RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les [traducteurs d'adresse réseau](#) IP (NAT)", août 1999. (*Information*)
- [SS7] Recommandations UIT-T Q.700-775, "Système de signalisation n° 7".
- [SS7 MTP] Recommandation UIT-T Q.701-6, "Sous-système Transfert de message du système de signalisation n° 7".
- [T1.607] ANSI T1.607-1998, "Digital Subscriber Signaling System Number 1 (DSS1) - Layer 3 Signaling Specification

for Circuit-Switched Bearer Services".

## Adresse des auteurs

Lyndon Ong  
Nortel Networks  
4401 Great America Parkway  
Santa Clara, CA 95054, USA  
mél : [long@nortelnetworks.com](mailto:long@nortelnetworks.com)

Ian Rytina  
Ericsson Australia  
37/360 Elizabeth Street  
Melbourne, Victoria 3000, Australia  
mél : [ian.rytina@ericsson.com](mailto:ian.rytina@ericsson.com)

Matt Holdrege  
Lucent Technologies  
1701 Harbor Bay Parkway  
Alameda, CA 94502 USA  
mél : [holdrege@lucent.com](mailto:holdrege@lucent.com)

Lode Coene  
Siemens Atea  
Atealaan 34  
Herentals, Belgium  
mél : [lode.coene@siemens.atea.be](mailto:lode.coene@siemens.atea.be)

Miguel-Angel Garcia  
Ericsson Espana  
Retama 7  
28005 Madrid, Spain  
mél : [Miguel.A.Garcia@ericsson.com](mailto:Miguel.A.Garcia@ericsson.com)

Chip Sharp  
Cisco Systems  
7025 Kit Creek Road  
Res Triangle Pk, NC 27709, USA  
mél : [chsharp@cisco.com](mailto:chsharp@cisco.com)

Imre Juhasz  
Telia  
Sweden  
mél : [imre.i.juhasz@telia.se](mailto:imre.i.juhasz@telia.se)

Hai-an Paul Lin  
Telcordia Technologies  
Piscataway, NJ, USA  
mél : [hlin@research.telcordia.com](mailto:hlin@research.telcordia.com)

HannsJuergen Schwarzbauer  
SIEMENS AG  
Hofmannstr. 51  
81359 Munich, Germany  
mél : [HannsJuergen.Schwarzbauer@icn.siemens.de](mailto:HannsJuergen.Schwarzbauer@icn.siemens.de)

## Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). 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 droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction 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 droits de reproduction 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 ses 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.