EFFETS D'UN CHIFFRAGE DES DONNEES SUR

LA QUALITE DE SERVICES

SUR LES RESEAUX VSAT

(RESEAUX GOUVERNEMENTAUX)

Bruno VO VAN,
Mise à jour : Juin 2006

SOMMAIRE

RESEAUX GOUVERMENTAUX VIA SATELLITE

1 PREAMBULE

Les critères des décisions d'Investissement de Secteur Gouvernemental sont différents de ceux du Secteur Commercial lorsqu'il s'agit de réseaux de télécommunications.

Les exigences clés pour des systèmes de communications dans ce secteur: les Ministères de Défense, des Finances, l'Intérieur, des Affaires étrangères ou semblables.., sont en général dans l'ordre d'importance suivant:

- La Sécurité et la Sûreté des informations.
- La Qualité de service
- Le rapport Qualité/prix
- ..

Ce document décrit les critères techniques retenus par LCDC lorsqu'il devient nécessaire de chiffrer les données des informations et du transport sur un réseau satellite.

2 CRITERES TECHNOLOGIQUES DES PLATES-FORMES

2.1 RAPPORT QUALITÉ/PRIX

Un bon rapport qualité/prix d'un réseau via satellite peut être obtenu en utilisant la technique d'attribution de capacité de trafic à la demande (BoD).
Une capacité fixe et permanente entre deux ou plusieurs sites s'avère couteuse car elle n'est pas liée à son usage instantané mais à une moyenne. Ce principe est associé au protocole SCPC (Single Channel Per Carrier) lorsque l'on parle de lien satellite. Ainsi un réseau étoilé, maillé ou hybride, utilisant ce protocole est très vite couteux.

Un critère de qualité d'un protocole d'allocation de capacité à la demande (BoD) est de pouvoir garantir de façon idoine (suffisante et économique) la Qualité de Service des divers transports de flux (Téléphonie, Vidéo, et autres applications prioritaires..).

L'algorithme d'assignation de largeur de bande d'une technologie BoD doit pouvoir différencier les classes prioritaires ajustées à chaque spécificité des flux de données transportées.

2.2 QUALITÉ DE SERVICES

Les classes de priorité de trafic peuvent être identifiées puis traitées par le modem satellite de 2 façons :

- Évaluer des informations prioritaires fournies selon le protocole à l'interface utilisateur (par exemple. IP, FR etc)
- Analyser de trafic d'utilisateur avec un mécanisme de marque déposée (propriétaire)

2.3 PERTINENCE DE PROTOCOLES DE TRANSPORT

L'IP (Internet Protocol) n'est pas un protocole très efficace en termes de trafic d'utilisateur, son transport est pénalisé par la nécessité d'une signalisation importante. Les familles du protocole IP sont de plus mal appropriées aux réseaux de grandes latences.
Ces inconvénients n'ont cependant pas occulté sa prédominance de plus en plus importante sur le marché et dans son transport entre sites.

De plus, l'abondance de capacité disponible, en particulier sur les réseaux terrestre de fibres optiques occultent ces inconvénients. Obtenir de grandes bandes passantes n'est plus considéré comme un critère important.

La prédominance du protocole IP comme protocole de base pour toutes les demandes de trafic d'utilisateur incluant ceux qualifiés en ''Temps réel'' catalysent les progrès d'amélioration des protocoles utilisés pour affiner l'efficacité des Classes de Services.

La popularité croissante des familles du protocole IP dans tous les secteurs de communications modernes est aussi observée dans des communications satellites, où des modems satellites conçus pour transmettre en capacités IP ont gagné une part de marché significative ces dernières années.

La seule alternative principale à IP comme protocole à l'interface utilisateur du modem satellite continue à être le protocole de ''Relayage'' de Trames (Frame Relay ou FR).

Les qualités clés du FR sont sa simplicité, efficacité et la disponibilité sur le marché d'équipements (FRAD) de plus en plus puissants et supportés. La facilité d'accès à ce protocole donnant des possibilités de plus en plus grandes permet une intégration simplifiée vers d'autres protocoles de communications, d'interfaces utilisateurs etc..

IP et FR, fournissent respectivement les moyens pour classifier et donner la priorité au trafic d'utilisateur porté dans le protocole.

En raison de sa structure simple, le FR permet la création d'améliorations aisées et fiables afin d'affiner un protocole qui devient propriétaire pour obtenir la meilleure Qualité de Services possible sans perdre la possibilité d'une passerelle d'interopérabilité.

Par exemple, les FRADs permettant la compression de voix et l'encapsulation dans le FR peuvent envoyer la signalisation de téléphonie à la plate forme (modem satellite). Cette plate forme (modem satellite) peut alors établir des connexions en temps réel de durée définie et durant le temps exact qui est alors nécessaire pour le meilleur usage de la bande passante spatial allouée.

Malgré la meilleure efficacité et la supériorité potentielle en ce qui concerne QoS des plates formes FR, les plates formes IP ont très souvent la préférence.
Ceci principalement pour cause d'uniformité au niveau des intégrations de réseaux ou des prix avantageux des équipements bâtis sur IP.

2.4 L'IMPACT D'UN CHIFFRAGE SUR LA QOS.

La situation change significativement aussitôt que l'exigence pour la sécurité de l'information met en application le chiffrage des données de l'utilisateur pendant la transmission sur le satellite.

Pour respecter les exigences très spécifiques en ce qui concerne des dispositifs de chiffrage, il y a seulement une façon appropriée de construire la communication sûre :

C’est d’introduire un dispositif de chiffrage approuvé entre le trafic d'utilisateur et le modem satellite.

Le modem doit savoir examiner le trafic d'utilisateur pour donner la priorité et allouer la largeur de bande en conséquence.
Malheureusement la plupart de l'information nécessaire, si pas ce n’est pas son intégralité, sera chiffrée par le dispositif d’encryptage inséré entre le trafic d'utilisateur et le modem satellite. C'est le cas en particulier pour des tunnels IPSec, où toute l'information d’en-tête (ID, Adresse de destination, quantité de bits etc..) d’une trame IP est chiffrée avant l'expédition par le tunnel, avec une nouvelle ‘’en-tête’’.

Il semble alors impossible à trouver une résolution à ce problème pour récupérer la partie de la fonctionnalité perdue, permettant par exemple, de maintenir un certain nombre de priorités à un certain débit prédéterminé. Cela impliquerait le développement conjoint de fonctionnalités de la plate forme satellite (produit commercial) en relation à la mise en place du spécifique IPsec dans l’équipement d’encryptage (produit militaire).

En parallèle, la plupart des procédures plus ou moins sophistiquées et demandées au modem satellite pour :

- Assigner la largeur de bande le plus efficacement possible entre des nœuds de réseau de même importance et en même temps,
- Respecter les classes de priorité de trafic échoueront en présence de chiffrage.

Le résultat serait une Qualité de Services plus pauvre et la consommation de largeur de bande considérablement plus haute. Par exemple, la Voix sur IP (VoIP) ne peut pas être compressée en présence de chiffrage.

3 CONCLUSIONS :

Le modem SkyWAN est aujourd'hui le point de référence dans l'industrie pour l'économie de largeur de bande satellite et fournit les capacités les plus complètes pour soutenir la Qualité de Service pour des applications d'utilisateur indépendamment de l'interface/protocole, IP ou le FR.
Cette plateforme tient en compte les caractères contradictoires décrits ci-dessus.

Dans le contexte présent de réseaux gouvernementaux incluant le chiffrage il y a seulement une recommandation : utiliser le Relais d'Encadrement comme le protocole pour la partie satellite du réseau.

La solution est basée sur l’utilisation d’un FRAD spécifique, comme le dispositif d'accès pour toutes les sortes de trafic d'utilisateur.

- toutes les interfaces utilisateur communes pour le trafic de voix de POTS analogues aux interfaces PBX digitales avec des standards divers de signaux.
- Des interfaces ‘’série’’ pour des protocoles divers et des demandes traditionnelles et
- Des interfaces d'Ethernet et des fonctionnalités de routage pour se à l'infrastructure IP locale.

Le FRAD envoie tout trafic d'utilisateur au modem SkyWAN sur un port FR unique.

Les améliorations simples propriétaires du protocole normalisé de ‘’relayage de Trames’’ (FR) permettent alors au modem d'assigner des priorités et la largeur de bande satellite à la demande de la façon la plus appropriée.

Ce traitement optimisé de trafic d'utilisateur s'opère aussi lorsque les données d'utilisateur doivent être chiffrées : il y a seulement le besoin d'un simple FR-chiffreur à insérer entre le FRAD et le modem.

Le choix actuel d'un équipement de chiffrage existe entre 3 fabricants principaux au niveau mondial. Leurs équipements de chiffrage ont été approuvés pour ne pas mettre en péril les capacités de la configuration décrite ci-dessus.

La solution retenue n'a aucun compromis sur les exigences clés exposées ci-dessus pour des réseaux satellites gouvernementaux. L'efficacité de l'optimisation de l'usage de la bande passante assure le client d'une solution avec le plus bas le coût de propriété.

Finalement, il est souligné que le protocole propriétaire utilisé par le modem SkyWAN fournit une protection extrêmement haute de sécurité des informations en comparaison à d'autres modems satellites basés sur la technologie populaire et standardisée comme SCPC et DVB, de technologie à intelligence centrale (hub de type Viasat ou I-Direct).

Dès qu'un aspect Sécurité de l'information prédomine dans les spécifications d'un réseau, LCDC propose la plateforme de la série SKYWAN de NDSATCom,