QUALITY OF SERVICE AND THE EFFECTS OF DATA ENCRYPTION ON VSAT NETWORKS (GOVERNMENT NETWORKS)

Bruno VO VAN,
Updated: June 2006

SUMMARY

GOVERNMENT COMMUNICATION

NETWORKS VIA SATELLITE

1 PREAMBLE.

This document describes the technical criteria taken into consideration by LCDC when it becomes necessary to gauge the quality of transmission of data on a satellite network.

2 TECHNICAL CRITERIA.

The criteria used to make informed decisions regarding the investment in telecommunications networks for the Governmental Sector are quite different from those for the Commercial Sector. The key requirements for communication systems in this sector, that is, the Defence, the Finance, the Interior and the Foreign Affairs ministries for example, are in general in the order of importance as follows:

- The Safety and Security of the information being communicated.
- The Quality of the service provided.
- The Cost of the service (The Quality/Price Ratio).

2.1 QUALITY TO PRICE RATIO.

A good quality/price ratio of a satellite network can be obtained by using the technique of Bandwidth on Demand (BoD) where the capacity is related to the amount of traffic at any particular time. A fixed and permanent capacity between two or several sites proves to be expensive because it is not related to the instantaneous use required but on an average usage, which has been pre-determined. This principle of a fixed capacity is associated with the SCPC (Single Channel Per Carrier) protocol in terms of communications via satellite. Thus a star or a meshed network or even a hybrid system using this protocol will become expensive because the use of the capacity becomes less and less optimised as conditions change.

A requirement of any protocol that allows for the amount of bandwidth to be requested as required (BoD), is for it to be able to guarantee, in a suitable way, that sufficient capacity and in the most economic fashion be made available to provide the Quality of Service for the various types of data to be transmitted (Telephony, Video, and applications that have priority over others). The algorithm used to decide on the assignment of the bandwidth in a BoD system must be able to differentiate between the priorities of the data that needs to be transmitted over the system.

2.2 QUALITY OF THE SERVICE.

The priority of traffic can be identified (and treated consequently thereafter) by the satellite modem in 2 ways:

- To evaluate the priority from the information provided according to the protocol of the user interface (for example. IP, FR etc)

- To analyse the origin of the traffic to determine the user ID and decide on a pre-arranged priority.

2.3 RELEVANCE OF THE VARIOUS TRANSMISSION PROTOCOLS.

The IP (Internet Protocol) is not a very effective protocol in terms of user traffic; its use is also penalised in circumstances where the need for a priority to be associated to certain traffic is required. The use of the IP family of protocols is even less appropriate in larger networks. These disadvantages however did not hinder its increasingly important prevalence in the market place and in its use in the transmission of data between sites.

Moreover the abundance of the available capacity, in particular on the underground optical fibre networks, allowed these disadvantages to be largely ignored. The time for the delivery of the data between sites was not considered to be important.

The prevalence of the IP protocol as a basic protocol for all the requests for user traffic, including those qualified as “Real Time” requests, has hastened the progress of improved protocols that are more efficient in the ability to differentiate between the Classes of Services.

The increasing popularity of the IP family of protocols and their use in all the modern sectors of the communications industry is also observed in satellite communication systems, where satellite modems that are designed to transmit using IP have gained a significant share of market in recent years.

The principal alternative protocol to IP providing a similar user interface to the satellite modem continues to be Frame Relay (FR).

The key qualities of FR are its simplicity, effectiveness and the availability of equipment on the market. Frame Relay Access Devices, (FRAD’s) are becoming increasingly more powerful allowing the FR protocol to be well supported. The easy accessibility properties of this protocol permits a simplified integration with other communication protocols, user interfaces etc.

IP and FR, respectively provide the means to classify and to allocate a priority to the user traffic carried in the protocol.

FR, because of its simple structure, allows the creation of easy and reliable improvements in order to refine a protocol, and then obtain the best possible Quality of Service without losing the possibility of networking.

For example, FRAD’s can allow the compression of the voice data and then encapsulate it in FR and pass to the satellite modem along with the indication that the data contains telephony. The satellite modem can then establish a “Real Time” connection of a definite duration and for the exact time that is necessary for the best use of the bandwidth space allocated.

However, in spite of the best effectiveness and the potential superiority of FR with regard to QoS, systems using IP very often take preference. This is mainly due to uniformity of equipment and the ease of integration into various networks and also on advantageous prices of the equipment built on IP.

2.4 IMPACT OF ENCRYPTION ON THE QoS.

The situation changes significantly when, for security reasons, the user data requires some form of encryption before transmission over the satellite.

To respect the very specific requirements with regard to the encryption devices, there is only one suitable way to build a secure communication: It is to introduce an approved encryption device between the user traffic and the satellite modem.

The satellite modem needs to examine the traffic in order to determine the user so as to set the priority and consequently to allocate the bandwidth. Unfortunately the encryption device, inserted between the user traffic and the satellite modem, will encode the majority of the required information necessary to make the decision before the data is received by the satellite modem. This is the case in particular for IPSec tunnels, where all the header information (ID, destination address, quantity of bits etc.) of an IP frame is encoded before forwarding by the tunnel, with a new header.

It then seems impossible to find a resolution to the problem of recovering the lost information, allowing for example, to maintain a certain number of priorities to a certain predetermined bandwidth. That would imply the joint development of satellite equipment (commercial product) in relation to the installation of specific IPsec in the encryption equipment (produced by the military).

In parallel, the majority of the procedures requested from the satellite modem are:

- To assign the bandwidth in the most effectively way possible for each of the nodes with the same priority and at the same time,

- To respect the priority assigned to the user traffic (this will fail in the presence of encryption).

The result would be a poorer Quality of Services and the bandwidth requirements would be considerably higher. Also to be considered is that Voice over IP (VoIP) cannot be compressed in the presence of encryption.

3 CONCLUSIONS:

The SkyWan modem is today the industry standard for the efficient use of satellite bandwidth and provides the most economic use of the available bandwidth to support the best Quality of Service for the user applications independently of the interface or protocol used, IP or FR.

This platform holds in account the contradictory characters described above.

In the context of government networks, including encryption, there is however only one recommendation, that is to use the Frame Relay protocol for the satellite part of the network. The solution is based on the use of a specific FRAD for all the kinds of user traffic such as:-

- the common user interfaces for voice traffic (POTS and digital PBX interfaces with various signal standards)

.

- the Serial Interfaces for various protocols and traditional requests and

- Ethernet interfaces and equipment for routing to and from the local IP infrastructure.

The FRAD sends all the traffic of a user to the SkyWan modem on a unique FR port.

The Frame Relay standardised protocol then makes it possible for the modem to identify the user, assign the correct priority and request the most suitable satellite bandwidth.

This optimised treatment of user traffic will also work when the data of user must be quantified: there is only the need for a simple FR calculator to insert between the FRAD and the modem.

Currently there is the choice between 3 principal manufacturers on the world market whose encryption equipment has been approved for the configuration described above.

The adopted solution does not compromise any of the above-mentioned key requirements for government satellite networks. The effectiveness of the optimisation of the bandwidth usage ensures that the customer has a solution with the lowest cost.

Finally, it is stressed that using the SkyWAN modem provides an extremely high protection for the security of the transmitted information compared to that of other satellite modems based on the popular and standardised technology such as SCPC and DVB, and technology with central intelligence (hub type from Viasat or I-Direct).

When a security of information aspect prevails in the specifications of a network, LCDC proposes the SKYWAN series of equipment from NDSATCom.