Le réseau Transpac et la norme X 25 : la sécurité du transport de l'information

Christian Gateau

Administrateur d'ARMORHISTEL
Adjoint au Directeur Sécurité de France Télécom Transpac
France Télécom Transpac
9, rue du Chêne Germain, B. P. 91235
F-35510 Cesson-Sévigné
christian.gateau@francetelecom.com

1 Introduction

La recommandation X 25 et celles qui lui sont associées (parmi lesquelles X 3, X 28, X 29, X 121) ont servi de base à la réalisation du réseau Transpac[1] notamment. Nous désignerons ces recommandations dans la suite sous l´appellation générique « norme X 25 » ou « X 25 ». L´objet de cette communication est d´analyser ce qui dans X 25 constituait un apport explicite ou implicite à la sécurité du transport de l´information, et comment dans l´implémentation du réseau Transpac l´aspect sécurité a été pris en compte. On se concentrera sur le réseau d´origine, dit « 1re génération », à base d´équipements TRT CP50 et MITRA 125.

2 Un réseau de données par paquets, pourquoi ?

Les principales motivations pour la mise en place d´un réseau de données par paquets étaient :
– l´aspect pratique : faciliter la mise en relations de deux équipements de traitement de données,
– l´aspect économique : mutualiser l´infrastructure de transmission.

1. On trouvera dans l'article de Guy Pichon, « Les débuts du réseau public français de commutation de données par paquets : TRANSPAC », dans ces *Actes du septième colloque sur l'histoire de l'informatique, 2004* une vision plus globale de l'histoire de Transpac. Nous y renvoyons le lecteur notamment pour les dates des divers événements.

Les principaux apports de cette technique sont :
– une utilisation optimisée des liens d´interconnexion,
– la possibilité de mettre en relation chaque utilisateur du réseau avec l´un quelconque des autres utilisateurs,
– une grande souplesse de mise en relation des différents utilisateurs par l´adaptation automatique des caractéristiques des raccordements,
– la possibilité de multiplexer plusieurs communications simultanées avec des correspondants différents sur le même lien d´accès physique au réseau,
– l´amélioration de la qualité de transmission par la mise en œuvre de codes de contrôle pour fiabiliser les données transmises.

3 X 25 et la sécurité

On entend par sécurité tout ce qui concourt à l'amélioration de la disponibilité, de l'intégrité et de la confidentialité d'un système de traitement de données.

Parmi les trois principaux critères de sécurité, X 25 apporte des éléments concernant principalement l´intégrité et la confidentialité.

Une des notions de base est le mécanisme d´acquittement ou de confirmation ; sur cet aspect, la norme X 25 se caractérise par :

— au niveau trame (niveau 2) : le mécanisme de commande-réponse dans la gestion de la liaison entre l´ETTD et le réseau (contrôle réciproque permanent de l´état de la liaison), et le mécanisme d´acquittement ou de rejet (contrôle de flux) dans la gestion des trames de données entre l´ETTD et le réseau, avec surveillance des réponses ou non-réponses et réémission sur temporisation (ce qui permet de gérer les éventuels problèmes de saturation),

— au niveau paquet (niveau 3) : le mécanisme de confirmation dans la gestion de la signalisation lors des établissements ou ruptures des circuits virtuels

De plus, compte tenu de la qualité quelquefois médiocre des liaisons spécialisées support aux raccordements des ETTD au réseau, à chaque trame (niveau 2) est associé un FCS (séquence de contrôle de trame) de 16 bits calculé à l´émission sur le principe d´une division de la séquence de bits constituant la trame par un polynôme générateur, et contrôlé en réception. Par répétition des informations signalées comme mal reçues, on obtient une transmission pour laquelle le taux d'erreur est inférieur à 1 erreur pour 10^8 paquets.

Un des risques perçus par les utilisateurs potentiels de réseaux à infrastructures physiques mutualisées et donc partagées par plusieurs utilisateurs n´ayant pas

de lien entre eux, est le risque d´erreur d´aiguillage des paquets qui constituerait une atteinte à la confidentialité. Par rapport aux transmissions de données basées sur des liaisons spécialisées point à point, on peut dire en schématisant que l´établissement d´une communication entre deux utilisateurs du réseau est équivalent à la mise en place « temporaire » d´une liaison spécialisée, avec des mécanismes d´aiguillage logique permettant de cloisonner les différentes communications.

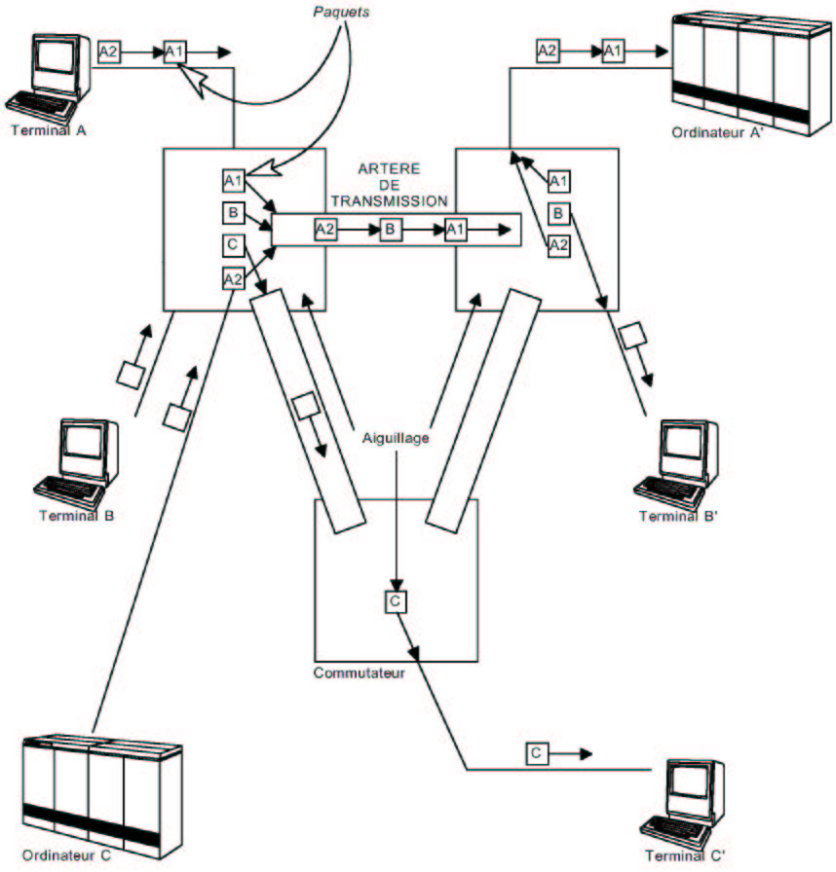

FIGURE 1 – Schéma de principe de la transmission par paquets

4 Le réseau Transpac et la sécurité

La sécurité a été dès le départ une préoccupation permanente dans la conception, la réalisation et la mise en opération du réseau ; il s´agissait, au-delà du choix de la norme X 25, lui-même un élément fort de cette sécurité, de conforter et de renforcer cette sécurité pour fournir au client un service particulièrement performant et sûr. Abordé de façon pragmatique, cet aspect sécurité se révèle à l´analyse a posteriori très pertinent.

Parmi les éléments participant à la sécurité, il est important de citer en premier lieu les aspects méthodologiques : SESA, maître d´œuvre du réseau Transpac initial, était précurseur dans la conception et la mise en œuvre d´une méthode de développement logiciel et de gestion de projet : méthode interne « MELUSINE » (METhode Logique Universelle pour un Software INdustriel Efficace), méthode reprise et adaptée par les équipes Transpac qui évoluera vers une démarche qualité structurée donnant lieu à l´attribution de la certification ISO 9001 en 1994, soit parmi les premiers certificats délivrés aux entreprises du monde de l´informatique et des télécom en France. Cet aspect méthodologique, repris en grande partie pour gérer les développements matériels, a permis d´augmenter considérablement la fiabilité des prestations aussi bien dans les phases de conception et de développement (organisation de la documentation, planification des fournitures, définition de jeux de tests élémentaires, mise en place d´indicateurs permettant de mesurer l´avancement, etc.) que dans les phases d´intégration et de recette (intégration successive en simulant les éléments manquants, puis formalisation des jeux de recette, rejouables lors des différentes phases de recette successives, etc.). Ces modes de fonctionnement ont ensuite été repris pour gérer les phases de maintenance corrective et évolutive, avec un cloisonnement fort entre l´environnement d´étude, de développement et de test d´une part et l´environnement opérationnel d´autre part. Le formalisme associé au passage de la phase « production » à la phase « exploitation » a permis de minimiser les problèmes rencontrés sur le réseau opérationnel.

Dans la conception et l´architecture du réseau, la préoccupation de la sécurité a été très importante :

— commutateurs à architecture redondante (secours 1 pour 1), possibilité de changement de cartes des modules de commutation « sous tension », etc.

— structure d´exploitation distribuée : points de contrôle locaux permettant de gérer un sous-ensemble du réseau, et pouvant être repris en secours par un centre de gestion centralisé,

— mécanismes de routage distribué permettant au réseau de fonctionner même si les équipements d´exploitation étaient indisponibles,

— maillage du réseau : l´ingénierie du réseau est telle que chaque commutateur est accessible par au moins deux liaisons distinctes, et la plupart du temps trois ou plus,

— liaisons internes multilignes : conception et mise en œuvre d´un protocole « propriétaire » de niveau 2 sur les liaisons internes du réseau adapté à la gestion de liaisons d´interconnexion entre les nœuds du réseau avec plusieurs lignes ; cela permettait d´une part de répartir la charge sur les différentes lignes constituant la liaison et d´autre part de rendre transparent pour les utilisateurs la défaillance des lignes de la liaison (tant qu´il en restait au moins une opérationnelle à un instant donné), ces défaillances étant relativement fréquentes à l´époque. La procédure « multilignes » gérait la réémission des trames perdues ainsi que la remise en séquence des trames (deux trames d´un même circuit virtuel pouvaient être émises sur deux lignes différentes d´une même liaison interne et donc éventuellement se doubler).

Dès le départ, il y a eu collecte de nombreuses informations concernant le fonctionnement opérationnel du réseau et analyse précise de ces informations par type d'incident, nombre d'incidents, durée des incidents, impact éventuel sur les clients, avec mise en place de nombreux indicateurs : pourcentage d'indisponibilité de liaisons internes, de liaisons d'accès, d'équipements, taux de panne, calculs de MTBF, etc.

L´ingénierie des sites d´hébergement des équipements du réseau opérationnel est homogène : surfaces dédiées, à accès protégé et contrôlé, détection et extinction incendie, climatisation, énergie électrique secourue ; les éléments de l´infrastructure physique sont télésurveillés et les alarmes éventuelles sont remontées vers les sites de gestion du réseau pour prise en compte, analyse et intervention éventuelle immédiate.

L´exploitation (production, supervision, maintenance des équipements de commutation), faite à distance depuis les points de contrôle locaux et/ou le centre de gestion, utilise la technologie et les ressources du réseau, avec des précautions et protections particulières : utilisation de CVP et de GFA réservés à l´exploitation, contrôle des adresses appelant lors de l´établissement de CVC, trames de données particulières sur des liens physiques spéciaux permettant d´initialiser, réinitialiser et télécharger à distance les nœuds de commutation.

Le personnel de l´exploitation, majoritairement issu à l´origine de l´administration des PTT, a une longue tradition de protection des informations (secret des correspondances) qui s´est perpétuée au sein de l´entreprise Transpac : protection

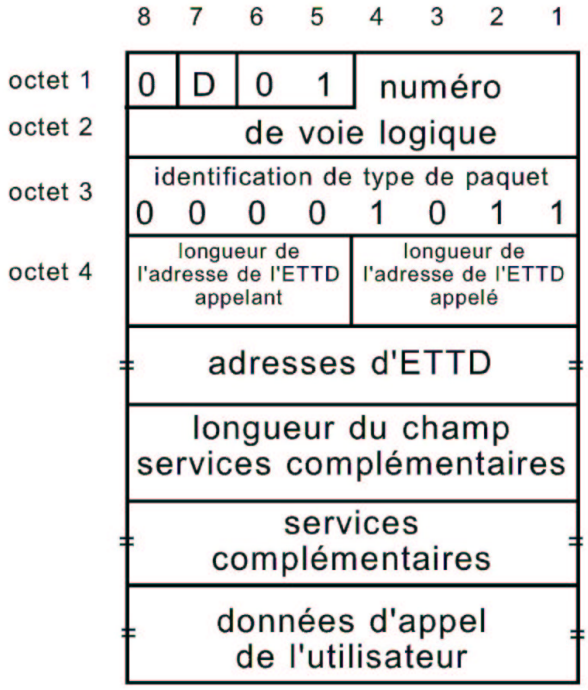

FIGURE 2 – Plan d'adressage Transpac

des informations transportées, protection des informations concernant un client, etc. Par ailleurs, les équipements de gestion du réseau effectuaient une journalisation systématique des opérations de production, de supervision et de maintenance pour permettre l´imputabilité des actions effectuées sur le réseau.

5 Les éléments de sécurité disponibles pour le client sur sa liaison d´accès

Une des fonctionnalités pouvant apporter une grande sécurité aux utilisateurs du réseau est la gestion par Transpac des adresses lors du processus d´établissement de circuit virtuel : en effet, lorsqu´un utilisateur du réseau reçoit sur sa liaison d´accès un paquet d´appel entrant (demande d´établissement d´une communication, figure 2), la structure du champ « adresse de l´ETTD appelant » permet de déterminer l´origine et la fiabilité de ce champ, ce qui limite considérablement les possibilités d´usurpation d´adresse ; en particulier, lorsque le « préfixe » de l´adresse appelant (premier digit de l´adresse) a la valeur « 1 », cela signifie qu´il

s´agit d´un appel provenant d´un accès permanent au réseau Transpac (grande majorité des cas), et dans ce cas, le numéro de l´appelant est initialisé par le réseau dans le paquet d´appel lors de sa transmission depuis la liaison d´accès de l´appelant. L´appelé peut ainsi vérifier l´identité de l´appelant et accepter ou non l´appel. Les autres valeurs du préfixe donnent des indications sur l´origine de l´appel, comme indiqué ci-dessous. figure 3.

FORMAT 0

0	N° Réseau (DNIC)	Adresse de l'abonné dans le réseau

International Pour un abonné du réseau TRANSPAC : DNIC = 2080

FORMAT 1

1	N° Dépt.	N° Abonné	Adr. Compl.

Accès synchrone ou asynchrone par LS

FORMAT 2

2	NUM. TELEX

Abonné TELEX français

FORMAT 3

3	ND	NAD

Accès asynchrone via RTC. Service EBAM
Si non identifié : ND+NAD : porte RTC d'accès à TRANSPAC
Si identifié (NUI) : ND+NAD : NUA

FORMAT 4X

40	ZABPQMCDU (fourni à l'abonnement)

Accès synchrone via RTC X32-V32 (EBS)

FORMAT 5X

5	ZABPQMCDU (fourni à l'abonnement)

Accès synchrone EBS/SBS via RTC X32-V27 ter

FORMAT 6x

6	N° d'accès PAVI.	type d'accès (TELETEL 1, 2, ...)

Point d'Accès Vidéotex. (PAVI en France)
Cette adresse ne peut être qu'appelante.

FIGURE 3 – Format du paquet d´appel

Parmi les autres paramètres et options disponibles permettant au client de gérer la sécurité de ses accès, les principaux sont :

— l´utilisation des groupes fermés d´abonnés (GFA) : un accès peut appartenir à un ou plusieurs GFA, avec possibilité de restreindre le sens des appels au sein d´un GFA (appels entrants seuls acceptés ou appel sortants seuls acceptés) ; la gestion des GFA dans Transpac est formalisée de façon très rigoureuse : un

GFA est sous la responsabilité d´un seul client avec un interlocuteur identifié seul habilité à accepter l´entrée d´un accès dans le GFA,

— la spécialisation des voies logiques : le nombre de voies logiques sur un accès détermine le nombre maximum de communications simultanées possibles sur cet accès ; il existe quatre types de voies logiques : voies logiques CVP (circuit virtuel permanent : une communication est établie en permanence vers un accès unique pré-défini à la configuration de l´accès), voies logiques spécialisées arrivée (n´acceptant que les appels entrants), voies logiques mixtes (acceptant les appels entrants ou sortants), voies logiques spécialisées départ (n´autorisant que les appels sortants) ; en jouant sur ces paramètres, le client pouvait sécuriser son accès dans une optique de disponibilité (réserver des voies logiques pour un sens d´établissement d´appel) ou de protection (par exemple interdire les appels entrants),

— les paramètres « taxation au demandé » (PCV) : c´est pour une bonne part à partir d´accès non identifiés, donc ne pouvant pas être taxés, que les tentatives d´intrusion dans les systèmes d´information via le réseau étaient effectuées ; ces demandes d´établissement de communications comportent le paramètre PCV, indiquant que la communication sera facturée à l´accès appelé ; deux solutions permettent au client de se protéger de ce type de tentative : soit examiner au cas par cas ce paramètre lors du traitement d´un appel entrant et éventuellement rejeter les appels correspondants, soit demander lors de la configuration de l´accès que le réseau rejette systématiquement les appels ayant ce paramètre positionné.

6 Conclusion

Ce panorama non exhaustif est néanmoins très représentatif de la réalité de la prise en compte de la sécurité aussi bien au niveau de la norme X 25 que dans l´implémentation qui en a été faite dans le réseau public Transpac. Cette approche pragmatique de la sécurité s´est révélée très efficace : le niveau de qualité de service atteint et le nombre particulièrement faible d´incidents de sécurité rencontrés en témoignent. L´approche de la sécurité sur cette première génération du réseau Transpac a été poursuivie et améliorée encore lors de la conception et de l´intégration dans le réseau X 25 des générations successives d´équipements (2e puis 3e génération), de la prise en compte des évolutions de la norme et la définition de nouveaux services. Au-delà, l´expérience acquise a été capitalisée et fortement réutilisée pour la mise en œuvre des technologies successives : frame relay, réseaux IP, etc. L´approche sécurité s´est structurée tout en restant fortement intégrée à tous les échelons de l´entreprise. La pertinence de cette démarche est d´ailleurs confortée par le fait que l´analyse formalisée de la sécurité effectuée à partir de la norme ISO 17799 a permis bien sûr d´améliorer l´existant, mais n´a pas

mis en évidence de manques significatifs dans la prise en compte de la sécurité dans l´entreprise.

6.1 Glossaire

CCITT	Comité Consultatif International Télégraphique et Téléphonique
CVC	circuit virtuel commuté
CVP	circuit virtuel permanent
ETCD	équipement de terminaison de circuit de données
ETTD	équipement terminal de traitement de données
FCS	frame check sequence ou séquence de contrôle de trame
GFA	groupe fermé d´abonné
ISO 9001	norme d´exigence sur les Systèmes de Management de la Qualité
ISO 17799	norme de bonne pratique sur la gestion de la Sécurité de l´Information
UIT	Union Internationale des Télécommunications
X 3	recommandation CCITT : dispositif d´assemblage et de désassemblage de paquets dans un réseau public de données
X 25	recommandation CCITT : interface entre ETTD et ETCD fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données
X 28	recommandation CCITT : interface ETTD/ETCD pour équipement terminal de traitement de données arythmique accédant à un dispositif d´assemblage et de désassemblage de paquets dans un réseau public pour données situé dans le même pays
X 29	recommandation CCITT : procédure d´échange d´informations de commande et de données d´utilisateur entre deux dispositifs d´assemblage et de désassemblage de paquets ou entre un tel dispositif et un ETTD fonctionnant en mode paquet
X 121	recommandation CCITT : plan de numérotage international pour les réseaux publics pour données.

Biographie de l´auteur

Christian Gateau, Adjoint au Directeur Sécurité de France Télécom Transpac, a environ 35 ans d'expérience dans les technologies de l'information et de la communication, dont environ 15 ans avec des missions et des responsabilités en matière de sécurité de l'information. Il a participé aux développements logiciels puis à la mise en place opérationnelle du réseau initial Transpac. Actuellement en charge de l'ani-

mation de la démarche de sécurité dans l'entreprise il est aussi membre du CLUSIF, ayant participé notamment au groupe de travail ISO 17799, président de l'association GRANIT (GRoupe ArmoricaiN en Informatique et Télécommunications) et administrateur de l'association ARMORHISTEL.
Cette communication est un témoignage d´un acteur ayant participé aux tous débuts de l´implémentation et de la mise en opérations du réseau Transpac X 25, avec depuis 15 ans des missions en matière de sécurité dans l´entreprise :
– de 1976 à 1982, pour l´entreprise SESA : développements et intégrations de logiciels des commutateurs Transpac, évolutions, transfert de compétences entre les équipes SESA et les équipes Transpac,
– de 1983 à 1988, activités techniques, commerciales et de management en SSII en particulier dans le domaine des réseaux, avec parmi les clients, Transpac,
– depuis 1989 à Transpac avec notamment des missions en matière de sécurité : sécurité du réseau, sécurité des infrastructures, sécurité de l´exploitation, éléments de sécurité disponibles pour les utilisateurs, etc.