

ANNEXE 20 - ARCHITECTURE TECHNOLOGIQUE DU RETEM

1. INTRODUCTION

La Direction générale des télécommunications (DGT), du Sous-secrétariat aux services gouvernementaux, a conclu une entente contractuelle avec la société Bell Canada, d'une durée de cinq (5) ans débutant le 1^{er} janvier 2002, pour la fourniture du Réseau de télécommunication multimédia de l'administration publique québécoise (RETEM). Dans le contexte de la modernisation de l'administration publique et du développement des services gouvernementaux en ligne, ce projet de très grande envergure positionne les télécommunications gouvernementales à la fine pointe de l'évolution technologique, tout en générant des économies importantes de coûts et de processus.

Les domaines des services RETEM concernant le SIIJ sont les services réseaux, les services Internet et certains services de type intranet.

Les services réseaux

L'entente prévoit que le service RICIB et les services environnants actuels seront remplacés progressivement par le service RETEM, et ce, tout au long du déploiement de la nouvelle infrastructure du RETEM, lequel durera jusqu'à l'automne 2002.

Les services Internet, intranet et de sécurité

La DGT vise par le projet RETEM à améliorer la qualité des services, tout en augmentant leur robustesse et leur sécurité. L'entente signée assure :

- Une robustesse accrue par la redondance des réseaux primaires Internet;
- Des services de sécurité évolués (intrusion, virus, information de gestion, etc.);
- Des services de sécurité personnalisés (réseau privé virtuel, authentification, etc.);
- Une gamme de services d'accès à haut débit modelés en fonction des besoins;
- Un service d'accès commuté sans frais interurbains;
- Un service consolidé d'assistance à la clientèle et à plage horaire étendue.

Une version électronique du *Répertoire des produits et services* est disponible à la place d'affaires de la DGT sur l'intranet gouvernemental, à l'adresse suivante : **<http://www.dgt.qc>**. L'édition électronique téléchargeable en format PDF facilite la consultation et permet d'obtenir en tout temps la version la plus récente du document.

2. LES SERVICES DU RETEM

Le RETEM est une infrastructure de services reposant sur une ossature de fibre optique à grand débit et pouvant atteindre toutes les régions du Québec. Cette ossature fait appel à des technologies à la fine pointe des équipements reconnus pour être des leaders dans le marché des télécommunications.

Le protocole stratégique qui sera utilisé pour le RETEM est IP. Les services seront fournis en mode d'intégration de services et selon les exigences du RETEM en vigueur. Les services s'étendent, lorsqu'ils sont nécessaires, jusqu'aux éléments de terminaison (commutateurs ou routeurs) du RETEM faisant interface avec les réseaux locaux dans les sites des clients. Ces commutateurs ou routeurs, ainsi que leur gestion opérationnelle, font, le cas échéant, partie intégrante des services.

La DGT, en concertation avec sa clientèle, va s'employer à toujours exercer une gestion étroite des services fournis et va s'assurer du suivi intensif de la qualité des services offerts par le RETEM.

Les sections suivantes présentent quelques services du RETEM pouvant répondre aux besoins du SIIJ (se référer au *Répertoire des produits et services*, avril 2002).

2.1 Service IP - relais de trames

Les services d'accès de relais de trames du RETEM peuvent fournir des débits de 56 kbit/s jusqu'à 45 Mbit/s. Le protocole relais de trames étant sur la couche 2 du modèle OSI, la couche 3 utilise des routeurs physiques ou virtuels. Les sites clients sont donc équipés de routeurs ou commutateurs. Ces équipements sont gérés, le cas échéant, par le RETEM.

Un réseau relais de trames se compose de circuits virtuels permanents (CVP). Ces CVP permettent de transporter le trafic des différentes applications entre les sites et entre les régions, vers des sites principaux ou vers d'autres services. Chaque CVP possède deux paramètres qui agissent différemment sur le trafic client. Ces paramètres sont le débit d'information convenu, CIR (*Committed Information Rate*) et le débit d'information étendu, EIR (*Excess Information Rate*).

La garantie de débit

Le débit pourra être mesuré de deux façons, soit par le débit d'information convenu (CIR) ou par le débit d'information étendu (EIR). Le résultat sera exprimé en indiquant le taux de réussite à l'intérieur du débit d'information convenu (CIR) et du débit d'information étendu (EIR). Les engagements de qualité de services pour le relais de trames sont les suivants :

- 100 % pour les trames convenues (CIR) délivrées;
- 99,9 % pour les trames étendues (EIR) délivrées (limite = débit de l'accès).

2.2 Service IP - Routeur virtuel

Dans le cas du service IP - relais de trames, les réseaux clients sont maintenus avec une configuration de couche 2, c'est-à-dire au niveau des circuits virtuels permanents (CVP). Cependant, plus le nombre de destinations possibles augmente, plus il est nécessaire d'ajouter des CVP. La complexité des réseaux clients s'accroît donc à mesure que des sites s'ajoutent.

Cette complexité est entièrement résolue avec le nouveau service IP - routeur virtuel qui maintient une configuration de réseaux clients de couche 3. En effet, dans le RETEM, un service de routeurs virtuels est disponible dans les nœuds de réseau. Grâce à ce service, un nœud peut effectuer un routage à partir de l'adresse IP du client. Il est donc possible de diriger le trafic client à partir des adresses IP de ce dernier et des fonctions de qualité de service inhérentes aux différentes applications.

La conception de la couche IP proposée (couche 3) exploite largement la force de la configuration du réseau. Sur le plan de l'architecture logique, l'utilisation des routeurs virtuels associés à des routes dynamiques diminue considérablement le nombre de circuits virtuels permanents (CVP) et contribue ainsi à améliorer notablement la performance. Le client qui, dès le premier jour, désire utiliser le RETEM comme un réseau de couche 3 (IP) peut bénéficier de tous les avantages d'association de classes de services (CoS) et de qualité de services (QoS) propres à ses besoins et qui se répercutent de bout en bout sur le réseau. Les routeurs de tête installés chez les clients, prévus dans les services réseaux, fournissent la couche IP pour le branchement des réseaux locaux des clients. Les tarifs Services IP - routeur virtuel comporteront deux volets, soit l'accès et le type de qualité de services auxquels souscrira le client.

2.3 Service de réseau local transparent

Le service de réseau local transparent du RETEM est offert au moyen des équipements Passport de l'ossature du RETEM. Les accès au RETEM utilisent des liens optiques et chaque service de réseau local transparent se termine sur un commutateur de couche 2 dont la gestion est incluse. Cette approche permet d'étendre un réseau local entre deux sites d'une même ville ou entre deux villes desservies par des CVP du RETEM. La solution proposée fournit, en outre, aux clients qui ont souscrit au service IP - routeur virtuel, la communication et l'interopérabilité entre des circuits relais de trames (ou MTA) en région, avec des sites branchés au RETEM par un accès 10BaseT ou 100BaseT. Tout cela est rendu possible grâce aux routeurs virtuels Passport qui assurent la communication par l'entremise de la couche 3. Le service de réseau local transparent est offert dans sa formule de base avec un débit pouvant atteindre, en rafale, le

maximum que permet le protocole Ethernet sur une connexion 10/100BaseT. Des débits minimaux garantis sont également offerts.

2.4 Service mode de transfert asynchrone

Le service mode de transfert asynchrone (MTA) repose sur une famille de protocoles stratégiques dans le domaine du multimédia. Ce protocole, communément désigné sous son acronyme anglais ATM (*Asynchronous Transfer Mode*), permet notamment d'intégrer conjointement, sur un même lien de télécommunications à haut débit, la voix, les données et les images. Par exemple, le service MTA du RETEM peut faire cohabiter harmonieusement et efficacement sur une même voie à haut débit des conversations téléphoniques, des fichiers informatiques et de la visioconférence. Le service mode de transfert asynchrone est un complément du service IP - relais de trames et des services IP - routeur virtuel. Les clients qui souscrivent au service IP - routeur virtuel sont assurés d'obtenir une communication transparente des services MTA avec les deux autres types de services. Cette caractéristique confère une grande souplesse pour la conception de réseaux hybrides qui répondent à des besoins accrus de débit dans certains axes, et ce, à un coût optimal sur le plan du réseau global. Le service de base comprend les éléments suivants :

- Dispositifs de commutation MTA (gestion, supervision et maintenance incluses);
- Liens d'accès MTA de 1,544 à 622 Mbit/s.

2.5 Services ligne numérique à paire asymétrique (LNPA) et commuté RETEM

2.5.1 Service LNPA RETEM

Le service d'accès haute vitesse de type LNPA RETEM est offert comme un service d'extension de réseau local. Comme son nom l'indique, il s'agit d'une extension du réseau local du site principal du client. Le lien LNPA est dédié au réseau local du client et utilise le RETEM pour le transport du trafic IP. Le service d'accès haute vitesse de type LNPA est offert par une passerelle MTA qui relie le RETEM au réseau public. Cette passerelle se retrouve répliquée en région et dans les principaux centres, soit ceux de Québec et de Montréal. Des mesures de sécurité supplémentaires (réseau privé virtuel [RPV]) peuvent donc être nécessaires pour assurer un niveau de sécurité comparable à celui des services directement reliés à l'ossature du RETEM. Ce service est offert là où la technologie le permet.

2.5.2 Service commuté RETEM

Ce service offre aux usagers la possibilité de se brancher par l'entremise du réseau téléphonique public, en mode commuté, à des applications dont l'accès leur est préalablement autorisé. Les abonnés du service commuté RETEM ont la possibilité d'accéder aux réseaux ministériels et à l'intranet gouvernemental. Les extranets d'organismes non gouvernementaux peuvent également être rejoints en fonction des politiques établies par les ministères et les organismes. Le service d'accès commuté comprend deux types d'accès, soit l'accès asynchrone en mode PPP et l'accès numérique RNIS.

2.6 Service LNPA et commuté Internet

2.6.1 Service LNPA Internet

Le service Internet haute vitesse sur le RETEM utilise la technologie LNPA. Différents débits sont offerts, tout dépendant de l'introduction de nouveaux logiciels sur les équipements reliés à ce service. Le service haute vitesse est offert là où la technologie est disponible au Québec et ailleurs dans le monde. Il est recommandé que l'accès haute vitesse Internet soit sécurisé par les passerelles de sécurité centralisées du RETEM ou par une passerelle de sécurité appartenant au client qui a souscrit au service.

2.7 Service Internet et sécurité

Cette section regroupe des services RETEM qui font appel aux autres technologies du réseau Internet pouvant répondre aux besoins du SIIJ.

2.7.1 Branchement par l'entremise du RETEM

Ce service permet de relier les abonnés du RETEM aux réseaux fédérateurs Internet de façon sécuritaire. Aucune nouvelle infrastructure n'est nécessaire si ce n'est pour ajuster le débit des réseaux des clients afin de répondre à la demande générée par le trafic Internet.

2.7.2 Réseaux privés virtuels (RPV)

La DGT offre un service de réseaux privés virtuels (RPV), communément désigné sous son acronyme anglais VPN, permettant à certains individus (télétravailleurs, mandataires et partenaires gouvernementaux) d'accéder de façon contrôlée et sécuritaire à l'intranet gouvernemental et à toutes autres applications gérées de façon centrale, ainsi qu'aux

réseaux ministériels reliés à l'environnement partagé du RETEM. Le raccordement se fait par Internet à partir d'un poste de travail autonome.

Cette technologie peut également être utilisée à l'intérieur du RETEM pour permettre à des individus d'accéder de façon contrôlée et sécuritaire à des réseaux ministériels, et ce, à partir d'un autre réseau ministériel. Ce type de service RPV, client-réseau, est également connu sous le terme de téléaccès sécurisé.

La sécurité est assurée par l'utilisation du protocole de tunnellation et de chiffrement IPsec Triple DES amorcé à distance par l'ordinateur de l'utilisateur. L'authentification des utilisateurs se fait par l'intermédiaire de serveurs de type RADIUS.

Le logiciel client du service RPV pour le mode téléaccès sécurisé est compatible avec les plates-formes Windows 95, 98, Millenium, NT, 2000 et XP. La gestion des comptes des utilisateurs peut être assurée de façon centrale par la DGT ou de façon décentralisée par les ministères et les organismes à partir des serveurs d'authentification de la DGT.

2.7.3 Gestion des passerelles de sécurité

La DGT offre un service de location et de gestion de passerelles de sécurité (coupe-feux ou *firewall*) pour les ministères et les organismes qui veulent se protéger du réseau Internet ou qui désirent augmenter le niveau de sécurité de leur réseau. Des rapports d'analyse des journaux peuvent être fournis de façon régulière et ad hoc.

2.7.4 Noms de domaine Internet

La DGT gère les domaines « *gouv.qc.ca* » et « *gov.qc.ca* » utilisés par les ministères et les organismes, que ce soit pour l'identification des sites WEB, des sites FTP ou pour les domaines de courrier Internet gouvernemental. La gestion des noms de domaine des ministères et des organismes s'effectue à l'aide de serveurs DNS (*Domain Name System*).

2.7.5 Courrier Internet

Dans le domaine du courrier Internet, la DGT offre des services de relais de courrier, des services de bureau de poste et des services de listes de distribution.

2.7.5.1 Relais de courrier

La DGT offre un service de relais qui redirige le courrier en provenance du réseau Internet vers les serveurs ministériels de courrier. Ces serveurs de relais protègent les serveurs ministériels de courrier Internet contre la prise de contrôle par des sources externes dans le but d'effectuer des envois massifs de courrier non sollicité (polluriels ou, en anglais, spam). Ce service permettra, dans un avenir rapproché, de filtrer du

courrier non sollicité en provenance du réseau Internet (blocage du pollupostage) et, pour les clients qui y adhéreront, permettra de filtrer la majorité des virus propagés par l'intermédiaire du courrier Internet.

2.7.5.2 Bureaux de poste

Pour les ministères et les organismes qui ne possèdent pas leurs propres serveurs de courrier Internet, la DGT offre également un service SMTP accessible par les protocoles POP3 et IMAP. Elle n'assume cependant aucune responsabilité en ce qui concerne le courrier expédié sur le réseau Internet qui n'est pas effectivement livré à son destinataire. La gestion des boîtes aux lettres peut être centralisée ou décentralisée.

- Gestion centralisée : la création, la modification ou la suppression des boîtes aux lettres est réalisée par le CADGT (Centre d'assistance de la DGT);
- Gestion décentralisée : les ministères ou les organismes désignent des responsables locaux Internet (RLI) qui créent, modifient ou suppriment les boîtes aux lettres de leurs clients.

Dans le cas de la gestion décentralisée, le traitement des modifications est effectué durant la nuit en mode différé. Un espace de 5 Mo est alloué pour chaque boîte aux lettres.

2.7.5.3 Liste de distribution

Les listes de distribution de courrier (de type *mailing lists*) permettent à un utilisateur d'envoyer un message à de multiples destinataires prédéfinis en une seule opération. Les réponses aux messages de la liste peuvent être redistribuées à tous les abonnés de la liste. Chaque liste doit être administrée par un modérateur. Il existe trois types de listes. Dans le cas d'une liste privée, c'est le modérateur qui définit les membres de la liste et qui approuve les messages distribués. Pour les listes semi-privées, le modérateur ne contrôle que la liste des abonnés. Enfin, dans le cas des listes publiques, toute personne intéressée peut s'inscrire et aucun contrôle n'est effectué sur les messages envoyés. Le modérateur peut toutefois remettre à l'ordre certains abonnés qui dérogent du thème de la liste ou qui ont un comportement non désirable.

2.7.5.4 Nouvelles ou Newsgroup

Dans le cadre d'une entente, les abonnés des services Internet de la DGT peuvent avoir accès au service de nouvelles (*newsgroup*) géré par le RISQ (Réseau d'informations scientifiques du Québec). C'est l'administrateur du service chez le fournisseur qui fixe les modalités de gestion et la durée de vie de l'information y apparaissant avant que celle-ci ne soit effacée du serveur.