

**Aspects techniques  
de l'utilisation de l'application iVisit  
dans les commissions scolaires  
participant au projet  
*École éloignée en réseau***

**Rapport provisoire à l'intention du  
Comité-conseil technique au projet  
*École éloignée en réseau***

**Juin 2007**

# Remerciements

Les auteurs du présent rapport tiennent à souligner la générosité de nombreuses personnes de tous horizons qui ont accepté de partager leur ingéniosité tout au long de la recherche :

- Stéphane Allaire, professeur au Département des Sciences de l'éducation et de psychologie de l'Université du Québec à Chicoutimi;
- Danielle Beauséjour, animatrice du RÉCIT à la Commission scolaire de l'Énergie;
- Mathieu Bilodeau, technicien en informatique à la Commission scolaire des Laurentides;
- Réjean Cloutier, directeur des services de l'informatique et des finances à la Commission scolaire des Laurentides;
- Olivier De la Chevrotière, régisseur au Service des technologies de l'information de la Commission scolaire du Val-des-Cerfs;
- Dominic Gagné, animateur du RÉCIT à la Commission scolaire du Val-des-Cerfs;
- Vincent Gagnon, assistant de recherche au Département des sciences de l'éducation et de psychologie de l'Université du Québec à Chicoutimi;
- Yves Gaillardetz, technicien en informatique, classe principale, Commission scolaire de l'Énergie;
- Christine Hamel, étudiante à la Faculté des sciences de l'Éducation de l'Université Laval;
- Christian Lafrance, directeur adjoint de l'informatique à la Commission scolaire de l'Énergie;
- Yves Le Saux, technicien en informatique à la Commission scolaire des Laurentides;
- Michel Perreault, conseiller pédagogique à la Commission scolaire des Laurentides;
- Robert Rochon, animateur du RÉCIT à la Commission scolaire des Laurentides;
- Brian Rogers, directeur du Service des technologies de l'information de la Commission scolaire du Val-des-Cerfs;
- Réjean Tremblay, technicien en informatique, classe principale, à la Commission scolaire de Charlevoix;
- Patrice Valiquette, analyste en informatique à la Commission scolaire des Laurentides;
- Derek Woodard, technicien en informatique, classe principale, au Service des technologies de l'information de la Commission scolaire du Val-des-Cerfs.

# Table des matières

INTRODUCTION .....	5
1 MISE EN CONTEXTE .....	6
1.1 Défi du projet <i>École éloignée en réseau</i> .....	6
1.2 Assises technologiques du projet <i>École éloignée en réseau</i> .....	7
1.3 Particularités du volet technique .....	8
1.4 Focalisation de l'expertise technique .....	8
2 DÉMARCHE MÉTHODOLOGIQUE .....	10
3 RÉSULTATS DE LA RECHERCHE .....	10
3.1 Fonctionnement simplifié de l'application iVisit .....	10
3.1.1 Mode natif de fonctionnement .....	10
3.1.2 Mode de fonctionnement en adressage IP privé .....	11
3.1.3 Fichier de configuration « config.ivb » .....	12
3.1.4 Cas problématiques .....	13
3.1.5 Résolution des problèmes .....	13
3.2 Solutions privilégiées .....	14
3.2.1 Solution de la Commission scolaire du Val-des-Cerfs .....	14
3.2.1.1 Avantages .....	14
3.2.1.2 Inconvénients .....	15
3.2.1.3 Mise à l'essai .....	15
3.2.2 Solution liée à l'adressage public .....	15
3.2.2.1 Adressage public des postes de travail .....	15
3.2.2.2 Solution de la Commission scolaire de l'Énergie .....	16
3.2.2.3 Solution de la Commission scolaire de Charlevoix .....	18
3.2.3 Solution liée au serveur Microsoft ISA .....	20
3.2.3.1 Avantages .....	22
3.2.3.2 Inconvénients .....	22

3.2.4	Solution PIX/ASA .....	22
3.2.5	Solution liée à l'ouverture partielle des ports .....	22
3.2.5.1	Avantages .....	24
3.2.5.2	Inconvénients .....	25
3.2.5.3	Mise à l'essai .....	25
4	CONDITIONS D'UTILISATION ET D'OPTIMISATION DE L'APPLICATION IVISIT ....	26
	CONCLUSION .....	26
	RÉTROACTION AU SUJET DU RAPPORT .....	28

# INTRODUCTION

Le présent rapport a été produit par un groupe de travail technique à l'intention du Comité-conseil technique au projet *École éloignée en réseau* dont le mandat consiste à prodiguer au ministère de l'Éducation, du Loisir et du Sport (MELS) avis et conseil sur les aspects techniques afférents au projet. Ce rapport propose une gamme de solutions informatiques destinées aux commissions scolaires participant au projet *École éloignée en réseau* pour utiliser l'application iVisit comme outil de vidéoconférence entre des écoles de différentes commissions scolaires. Rappelons que, au cours des dernières années, la connectivité intercommission scolaire a engendré des difficultés qui, dans plusieurs cas, ont empêché l'établissement de toute communication. Le texte qui suit expose des solutions concrètes en vue de résoudre cette problématique pour l'année 2007-2008.

Ce rapport a été réalisé conjointement par les personnes et les organismes suivants :

- Sonia Sehili, coordonnatrice des TIC, de la Société GRICS;
- Claude Lamb, technologie de l'information, de la Direction des ressources didactiques du MELS;
- Réjean Payette, consultant, de la Firme Consultation techno-pédagogique.

Les conseillers techniques de la Société GRICS, Michel Biron et Éric Ledoux, ainsi que les auteurs du présent rapport tiennent à souligner que le temps qui leur a été imparti pour effectuer cette recherche leur a permis de valider la faisabilité des solutions proposées, mais que la stabilité de certaines d'entre elles, dans le temps, n'a pu être vérifiée. Pour ce faire, des recherches plus poussées seront nécessaires, d'où le qualificatif « provisoire » qui apparaît dans le titre.

# I Mise en contexte

## 1.1 DÉFI DU PROJET *ÉCOLE ÉLOIGNÉE EN RÉSEAU*

En 2002, le MELS ainsi que le Centre francophone d'informatisation des organisations (CEFRIO), soutenus par des chercheurs universitaires, lancent le projet *École éloignée en réseau*, et ce, en étroite collaboration avec d'autres instances gouvernementales, communautaires et syndicales ainsi que plusieurs commissions scolaires.

Le projet *École éloignée en réseau* se situe alors au carrefour de trois tendances lourdes :

- la décroissance démographique dans les régions périphériques du Québec, ce qui incite à la fermeture des petites écoles. Cette tendance agit dans le sens de l'*atomisation*;
- l'implantation d'infrastructures technologiques dans toutes les commissions scolaires du Québec : réseaux de fibres optiques, ordinateurs, périphériques, serveurs et soutien technique. Cette tendance agit selon un vecteur de la *connectivité*;
- le développement pédagogique avec les technologies de l'information et de la communication (TIC) en appui dans la communauté éducative élargie : MELS, commissions scolaires, universités, instances communautaires, CEFRIO, Réseau pour le développement des compétences par l'intégration des technologies (RÉCIT). Il s'agit, dans ce cas, d'une tendance à l'*association*.

Le défi soulevé par des promoteurs et des partenaires est qu'une judicieuse combinaison des tendances dites de *connectivité* et d'*association* s'avère nécessaire pour maintenir, voire augmenter, la qualité de l'éducation dans un contexte d'*atomisation*. Lorsque la fermeture des petites écoles se produit sur la base de la qualité de l'éducation offerte à l'école, cette fermeture pourrait ainsi être évitée.

Le projet *École éloignée en réseau* comporte également une importante dimension communautaire que le sous-ministre adjoint à l'éducation préscolaire et à l'enseignement primaire et secondaire au MELS, Pierre Bergevin, décrit de la façon suivante :

Le projet *École éloignée en réseau* constitue une formidable réponse à la volonté de maintenir, sur l'ensemble du territoire québécois, l'accessibilité à une éducation de qualité. Il a par ailleurs démontré que la coopération entre les membres d'une communauté et entre les communautés elles-mêmes, favorise l'émergence d'une culture de l'éducation appuyée sur le partage et la transmission du savoir.<sup>1</sup>

Le projet *École éloignée en réseau* compte trois phases. La première phase, de 2002 à 2004, a fait intervenir une dizaine d'écoles réparties dans trois commissions scolaires. La deuxième phase, de 2004 à 2006, a rassemblé plus de 50 écoles primaires et secondaires distribuées dans treize commissions scolaires. Enfin, la troisième phase, qui est en cours depuis 2006 et se terminera en 2008, en a élargi sensiblement le nombre, en incluant, notamment, un volet international.

L'année scolaire 2007-2008 sera donc la dernière année de l'expérimentation proprement dite. D'ores et déjà, les partenaires s'activent à mettre en place les mécanismes internes et les conditions de tous ordres susceptibles d'en assurer la meilleure pérennité possible.

Pour davantage de renseignements sur le projet, il est recommandé de se référer à la documentation officielle consultable sur le site Web du CEFRIO, notamment au document intitulé *L'École éloignée en réseau – Synthèse du rapport final (Phase II)*.<sup>2</sup>

## **1.2 ASSISES TECHNOLOGIQUES DU PROJET *ÉCOLE ÉLOIGNÉE EN RÉSEAU***

Lors des première et deuxième phases du projet *École éloignée en réseau*, les commissions scolaires visées devaient mettre à la disposition des écoles participantes sur leur territoire le matériel informatique voulu, notamment les ordinateurs, les périphériques, les caméras numériques et le canon de projection, tout en incluant les dispositifs nécessaires pour garantir la meilleure connectivité possible. Deux outils technologiques étaient considérés comme obligatoires dans le cadre du projet. Pour la vidéoconférence, il s'agissait de l'application iVisit, tandis que pour l'élaboration commune de connaissances, le logiciel Knowledge Forum était

---

1. BERGEVIN, Pierre. 20 ans d'innovation par les TI. [http://www.cefrio.qc.ca/pdf/brochure\\_20ans.pdf](http://www.cefrio.qc.ca/pdf/brochure_20ans.pdf).

2. MELS, CEFRIO. Rapport synthèse, en partenariat avec le ministère des Affaires municipales et des Régions et le ministère des Services gouvernementaux, format PDF : ISBN-13 : 978-2-923278-42-1, ISBN-10 : 2-923278-42-9, 27 p. <https://extranet.cefrio.qc.ca/indexWeb.cfm?type=produits>.

prescrit. Ces deux applications étaient jugées essentielles pour l'enrichissement de l'environnement d'apprentissage et pour générer les données de recherche utiles aux chercheurs associés au projet.

### 1.3 PARTICULARITÉS DU VOLET TECHNIQUE

Au moment du lancement du projet *École éloignée en réseau*<sup>3</sup>, les réseaux informatiques des commissions scolaires étaient en pleine construction, la large bande passante constituait une denrée rare dans la quasi-totalité des régions administratives du Québec et l'important projet Villages branchés, qui achève maintenant de « brancher le Québec », n'avait pas même vu le jour. Il n'est donc pas étonnant que des difficultés d'ordre technique soient apparues tôt après le démarrage du projet *École éloignée en réseau*. C'est en fait l'utilisation du logiciel de vidéoconférence iVisit qui s'est révélé problématique, plus particulièrement en ce qui a trait à la connectivité entre les commissions scolaires.

### 1.4 FOCALISATION DE L'EXPERTISE TECHNIQUE

Le démarrage imminent de la dernière année d'expérimentation du projet *École éloignée en réseau*, couplé à l'impératif de préparer le terrain pour l'institutionnalisation du projet, a conduit les partenaires à créer le Comité-conseil technique au projet *École éloignée en réseau*.

Ce comité est formé des personnes suivantes :

- Josée Beaudoin, directrice du bureau de Montréal et directrice de projet au CEFRIO;
- Thérèse Laferrière, professeure titulaire en Sciences de l'éducation à l'Université Laval et directrice du TACT, chercheure associée au CEFRIO;
- Stéphane Allaire, professeur au département des Sciences de l'éducation et de psychologie de l'Université du Québec, à Chicoutimi;
- Gilles Allen, directeur à la Direction des ressources didactiques du MELS;
- Daniel Besner, vice-président, Produits et services pédagogiques à la Société GRICS;
- Réjean Cloutier, directeur des services de l'informatique et des finances à la Commission scolaire des Laurentides;

---

3. Voir le site Web suivant : [www.cefrio.qc.ca/projets/proj\\_34.cfm](http://www.cefrio.qc.ca/projets/proj_34.cfm).

- Christian Lafrance, directeur adjoint de l'informatique à la Commission scolaire de l'Énergie;
- Claude Lamb, technologie de l'information à la Direction des ressources didactiques du MELS;
- Réjean Payette, consultant à la Firme Consultation techno-pédagogique;
- Brian Rogers, directeur du Service des technologies de l'information à la Commission scolaire du Val-des-Cerfs;
- Jacques Thibault, coordonnateur du programme Villages branchés à la Direction des ressources didactiques du MELS.

En prévision de la première rencontre de ce comité, le 19 juin 2007, il a été convenu de former un groupe de travail technique dont le mandat serait d'actualiser le volet technique du projet à la lumière des développements survenus depuis 2004 et d'en faire état dans un rapport. Ce groupe de travail technique avait pour mission de déposer un rapport sur ses travaux pour favoriser la réflexion lors de la rencontre du 19 juin.

Ce groupe de travail technique réunissait les personnes suivantes :

- Sonia Sehili, coordonnatrice des TIC, de la Société GRICS;
- Michel Biron, directeur, Services techniques, de la Société GRICS;
- Claude Lamb, technologie de l'information, de la Direction des ressources didactiques du MELS;
- Éric Ledoux, analyste, de la Société GRICS;
- Mario Payette, analyste, de la Société GRICS;
- Réjean Payette, consultant, de la Firme Consultation techno-pédagogique.

Le mandat de ce groupe de travail technique consistait :

- à sonder certaines commissions scolaires ciblées pour déterminer des façons de faire, une procédure, une configuration ou toute autre méthode assurant des conditions de fonctionnement de l'application iVisit compatibles avec les finalités du projet *École éloignée en réseau*;
- à mettre au point des solutions fonctionnelles d'utilisation de l'application iVisit, solutions qui seront applicables dans l'ensemble des commissions scolaires participant au projet *École éloignée en réseau* en 2007-2008 et en période d'institutionnalisation, le cas échéant;
- à expérimenter la faisabilité et la fiabilité des solutions retenues;
- à documenter les solutions retenues afin d'en communiquer les modalités de mise en œuvre et tous les éléments liés à cette question, du point de vue des commissions scolaires, au Comité-conseil technique au projet *École éloignée en réseau* pour sa rencontre du 19 juin 2007.

## **2 Démarche méthodologique**

La présente recherche a été effectuée du 15 mai 2007 au 15 juin 2007. Le groupe de travail technique s'est rendu dans deux commissions scolaires afin d'y discuter avec les responsables de l'informatique. Des échanges du type virtuel ont également eu lieu avec deux autres commissions scolaires et des tests ont été faits avec ces dernières. Parallèlement, un banc d'essai à la Société GRICS a permis de mener à bien une série des tests pour valider la solution ISA.

Comme cela a été mentionné plus haut, la stabilité de certaines solutions, dans le temps, n'a pu être vérifiée *in extenso*, mais leur faisabilité a été l'objet de vérifications qui se sont avérées positives. Par ailleurs, le facteur temps n'a pas permis au groupe de travail technique d'explorer les conditions facilitantes au regard de l'utilisation optimale du logiciel de vidéoconférence iVisit, notamment la disponibilité de la bande passante et l'environnement informatique du poste de travail.

## **3 Résultats de la recherche**

### **3.1 FONCTIONNEMENT SIMPLIFIÉ DE L'APPLICATION IVISIT**

#### **3.1.1 MODE NATIF DE FONCTIONNEMENT**

Comme toute application Internet, l'application iVisit a été conçue pour être utilisée en adressage du type Internet Protocol (IP) public. Elle ne fait donc appel qu'à des ports du type User Datagram Protocol (UDP). Dans un tel mode, elle a recours d'abord à l'un des deux ports d'accès (9946 ou 9947) au serveur iVisit.

Une fois entrée sur le serveur, l'application iVisit utilise ensuite le port 9948 pour signaler sa présence et pour communiquer le moyen de la joindre, c'est-à-dire son adresse IP (par exemple : 66.131.55.5), de même que le port 9940 dont il faut faire usage pour permettre le retour de la communication. Comme le type de protocole employé (UDP) n'a aucune

mémoire ni aucune « suite dans son discours », il devient nécessaire de rappeler constamment au serveur iVisit cette information.

Chaque utilisateur iVisit qui se branche au serveur procède de la même manière. Il se rend d'abord dans une salle de discussion où il a alors accès à l'information nécessaire pour joindre les autres postes iVisit de cette salle, c'est-à-dire leur adresse IP et la porte d'entrée à utiliser (port UDP 9940).

Chaque poste iVisit de la salle de discussion reprend ensuite cette information pour communiquer directement avec chacun des participants, sans passer par l'intermédiaire du serveur iVisit. Au cours d'un échange dans la salle de discussion, la communication avec le serveur iVisit est réduite au minimum et elle ne sert qu'à signaler sa présence et le moyen de le joindre ainsi qu'à récupérer la méthode pour joindre les autres participants. Une conférence iVisit à l'intérieur d'une même commission scolaire ne consomme donc que très peu de bande passante Internet.

### **3.1.2 MODE DE FONCTIONNEMENT EN ADRESSAGE IP PRIVÉ**

Comme toute application Internet, l'application iVisit n'a aucun moyen de se rendre compte si elle utilise le mode natif de fonctionnement (adressage public) ou l'adressage privé. Toutes les applications Internet se comportent donc en mode natif comme si elles étaient dans un environnement à adressage IP public. D'autres mécanismes, tel le coupe-feu, doivent alors entrer en action. Il est bon de se rappeler qu'une adresse IP privée comme 192.168.1.25 peut exister dans tous les réseaux informatiques, contrairement à une adresse IP publique qui, elle, est unique. L'adresse IP privée ne comporte donc pas de caractère distinct. Ainsi, comme il est impossible de situer son emplacement par Internet et de la joindre, elle doit être remplacée par l'adresse IP du coupe-feu qui, lui, dispose d'une adresse publique.

Comme cela a été mentionné précédemment, l'application iVisit exige l'utilisation du port UDP 9940 pour communiquer avec elle. Dans le cas d'un poste iVisit derrière le même

coupe-feu, celui-ci demande également que l'on communique avec lui par le port UDP 9940. Comme le coupe-feu remplace toujours l'adresse IP privée du poste client par la sienne, un problème se dessine alors, car les renseignements fournis dans la salle de discussion iVisit pour joindre ces deux postes sont en ce cas identiques (adresse IP du coupe-feu et même port 9940). Il y a donc conflit d'identité entre ces deux postes.

Puisque ce problème se présente inévitablement chaque fois que deux applications Internet ou plus sont utilisées simultanément, le coupe-feu gère cette situation en assignant de manière aléatoire, ou seulement en cas de conflit, un nouveau port à chaque requête. Le coupe-feu garde en mémoire la demande initiale qu'il associe au nouveau port qu'il a lui-même assigné.

Tel est le mode de fonctionnement normal des applications Internet pour les postes en adressage privé. Pour chacun des postes iVisit ou pour toute application Internet du réseau de la commission scolaire, un port unique est utilisé pour recevoir les données attendues. Pour une même commission scolaire, sauf exception, c'est la même adresse IP publique qui est transmise mais avec un port différent pour joindre chacun des postes. Ainsi, on obtient une combinaison unique pour joindre un poste de travail.

### **3.1.3 FICHER DE CONFIGURATION « CONFIG.IVB »**

L'application iVisit utilise, par défaut, un port de communication source fixe (toujours le port UDP 9940). Le recours à un fichier de configuration facultatif (« config.ivb ») permet de personnaliser le port de communication source utilisé par l'application. Cette configuration peut être nécessaire pour que l'application fonctionne à travers certains coupe-feu de la commission scolaire lorsque plusieurs postes communiquent simultanément.

L'utilisation du fichier de configuration entraîne toutefois une gestion supplémentaire, car il faut s'assurer que chaque poste se sert d'un port de communication unique. Ainsi, si l'on désire brancher X postes iVisit, il faudra X fichiers de configuration différents avec X ports

de communication différents. Si, deux mois plus tard, on voulait avoir recours à l'application iVisit sur un autre poste de travail, il faudrait s'assurer que le port de communication assigné à ce nouveau poste n'aurait pas déjà été associé à un autre. Cela implique donc de garder un journal des ports utilisés sur chaque poste.

### **3.1.4 CAS PROBLÉMATIQUES**

Les problèmes surgissent si l'on donne l'ordre au coupe-feu de fermer tous les ports UDP en sortie. Chacun des coupe-feu demande d'employer un port UDP spécifique pour répondre à chacun des postes iVisit. Si les commissions scolaires configurent leur coupe-feu de manière à bloquer tous les ports UDP en sortie, le contact avec un poste iVisit d'une autre commission scolaire ne pourra s'effectuer en raison même du blocage de tous les ports UDP en sortie.

### **3.1.5 RÉOLUTION DES PROBLÈMES**

Dans le but de résoudre les difficultés mentionnées, les services informatiques des commissions scolaires ont envisagé différentes solutions. Il faut bien comprendre que, s'il y a des problèmes de ce genre, c'est que le fonctionnement normal d'Internet a été entravé pour diverses raisons. À noter que les correctifs appliqués par les commissions scolaires peuvent résoudre seulement des problèmes précis de communication avec certaines commissions scolaires, mais pas forcément avec l'ensemble d'entre elles.

Quelques-unes de ces solutions seront décrites ci-dessous avec un bref sommaire des avantages et inconvénients de chacune.

## 3.2 SOLUTIONS PRIVILÉGIÉES

*Remarque : Certaines des solutions privilégiées par les commissions scolaires peuvent être incompatibles entre elles. Dans un tel cas, il suffirait, en ce qui a trait aux règles de sécurité, d'être plus permissif dans l'ouverture des ports UDP en sortie uniquement pour les postes iVisit.*

### 3.2.1 SOLUTION DE LA COMMISSION SCOLAIRE DU VAL-DES-CERFS

La solution appliquée par la Commission scolaire du Val-des-Cerfs depuis l'implantation d'Internet dans son milieu consiste à ne pas pratiquer aucune restriction ou presque sur les ports du type Transmission Control Protocol (TCP) et UDP tant en entrée qu'en sortie. Cela n'a donné lieu, à ce jour, à aucun problème sérieux de sécurité informatique. Cette solution est mise en application avec une formule de gestion proactive du réseau qui repose sur la surveillance et la détection de tout comportement anormal ou inhabituel. Lorsqu'un abus est détecté à l'interne, l'ensemble des acteurs de la Commission scolaire du Val-des-Cerfs s'engage à intervenir afin de faire cesser le comportement déviant. Jusqu'à maintenant, il n'a pas été nécessaire de fermer des ports pour mettre fin à des abus occasionnels. Au dire des responsables pédagogiques et informatiques à la Commission scolaire du Val-des-Cerfs, l'intervention rapide auprès des utilisateurs fautifs comporte une dimension éducative. Tous semblent accepter les risques informatiques potentiels. Grâce à cette solution, l'usage d'un fichier de configuration dans l'application iVisit n'est pas nécessaire.

#### 3.2.1.1 Avantages

L'installation de chaque nouveau poste de travail qui utilise l'application iVisit ne demande pas l'intervention du responsable du réseau de la Commission scolaire du Val-des-Cerfs. Les utilisateurs de l'application iVisit dans cette commission scolaire n'éprouvent aucun problème particulier à communiquer avec d'autres postes iVisit dans les autres commissions scolaires qui se sont elles-mêmes assurées de pouvoir communiquer avec l'extérieur.

Cette configuration du coupe-feu permet également le fonctionnement de toute autre application Internet sans qu'une intervention soit nécessaire de la part du responsable du réseau de la Commission scolaire du Val-des-Cerfs.

### **3.2.1.2 Inconvénients**

Cette approche est marginale dans l'ensemble des commissions scolaires. Dans ce cas-ci, elle oblige au partage de la responsabilité par l'ensemble de la Commission scolaire du Val-des-Cerfs. Une telle approche demande une évaluation des risques réellement encourus et la sécurité du réseau informatique doit être davantage orientée vers la détection de tout comportement anormal sur le réseau Internet de la Commission scolaire du Val-des-Cerfs. La sécurité ne repose pas exclusivement sur les barrières mises en place.

### **3.2.1.3 Mise à l'essai**

À notre connaissance, cette solution est utilisée uniquement par la Commission scolaire du Val-des-Cerfs. Des tests ont été effectués avec quatre postes derrière leur coupe-feu et deux autres postes qui étaient situés derrière un autre coupe-feu.

## **3.2.2 SOLUTION LIÉE À L'ADRESSAGE PUBLIC**

### **3.2.2.1 Adressage public des postes de travail**

Tous les ordinateurs multimédias sont en adressage public.

#### ***Avantages***

La simplicité de l'adressage public représente son grand avantage. Ainsi, aucune gestion du fichier de configuration (« config.ivb ») n'est nécessaire.

### ***Inconvénients***

La sécurité est moindre parce que les postes de travail ne sont pas derrière un coupe-feu. Ce dernier est conçu pour assurer une sécurité de périmètre à un réseau. Celle-ci permet d'ouvrir des fonctionnalités entre les postes de travail du réseau, fonctionnalités qui ne sont pas accessibles à partir de l'autre côté du coupe-feu. Donc, les formes de vulnérabilité associées à ces fonctionnalités ne sont pas exploitables à partir d'Internet. Quand on éloigne un poste de ce périmètre, il ne bénéficie pas de cette protection.

Le nombre d'adresses IP publiques doit être équivalent au nombre de postes de travail, soit une adresse publique par poste de travail utilisant l'application iVisit. Il est possible que cela engendre un coût supplémentaire.

La mise en place de cette solution nécessite la gestion des adresses IP fixes.

Les postes de travail sont isolés du reste du réseau. Comme le poste en adressage public est de l'autre côté du coupe-feu, il ne peut accéder à la plupart des services offerts en toute sécurité à l'intérieur du périmètre de sécurité assuré par celui-ci (par exemple, le serveur de fichiers, l'imprimante réseau ou Intranet).

Il est nécessaire de limiter l'accès à certaines applications (mot de passe et piratage). Lorsqu'on travaille derrière un coupe-feu, on risque d'adopter des pratiques non sécuritaires, telles que le partage d'un dossier sur son poste de travail à l'intention de ses collègues. Si le poste de travail est en adressage public, il importe d'éliminer de telles habitudes. Si l'on conserve les mêmes façons de faire tout en étant en adressage public, le piratage devient une affaire de quelques minutes.

#### **3.2.2.2 Solution de la Commission scolaire de l'Énergie**

La solution adoptée par la Commission scolaire de l'Énergie consiste à avoir recours à la traduction d'adresses de réseau (Network Address Translation (NAT))

statique). Chaque poste qui utilise l'application iVisit pour communiquer avec d'autres écoles à l'extérieur de cette commission scolaire doit être identifié :

- La Commission scolaire de l'Énergie doit pouvoir disposer d'un certain nombre d'adresses IP publiques;
- L'adresse IP privée (adresse interne à la Commission scolaire de l'Énergie) du poste iVisit doit être transmise au responsable informatique du réseau Internet de cette commission scolaire;
- Le responsable du réseau associe, dans son coupe-feu, chaque adresse IP des postes iVisit à une adresse IP publique. Il crée dans son coupe-feu une règle de sécurité (« access\_list ») afin d'autoriser l'utilisation des ports nécessaires au bon fonctionnement de l'application iVisit. Il s'agit de permettre l'utilisation en sortie des ports UDP 9946, 9947 et 9948 pour communiquer avec le serveur iVisit. Le responsable du réseau doit également s'assurer qu'il est possible d'utiliser en entrée et en sortie le port UDP 9940. L'ouverture en sortie des ports UDP supérieurs ou égaux au port UDP 1024 permet de communiquer avec un plus grand nombre de commissions scolaires;
- Le responsable du réseau doit associer cette règle de sécurité à chaque adresse IP privée – adresse IP publique.

Cette procédure permet ainsi à des utilisateurs iVisit dans une école de la Commission scolaire de l'Énergie de joindre des utilisateurs iVisit dans une école située dans une autre commission scolaire.

### **Avantages**

Si toutes les conditions sont réunies, cette solution demeure relativement simple et demande peu d'intervention de la part du personnel technique.

Cette solution permet de contourner la majorité des inconvénients liés à l'utilisation d'un réseau virtuel (Virtual Local Area Network (VLAN)). Ainsi, les postes iVisit ne sont plus isolés du réseau de l'école et de la Commission scolaire de l'Énergie.

Cette solution s'avère une pratique très sécuritaire, car seuls les postes iVisit peuvent accéder, au minimum, à ces quatre ports. Il ne faut pas oublier, dans cette solution comme dans toutes les autres, qu'il est toujours préférable d'ouvrir

en sortie les ports UDP supérieurs ou égaux au port DUP 1024 en vue d'augmenter la compatibilité de cette solution avec les autres.

### ***Inconvénients***

La commission scolaire de l'Énergie doit pouvoir disposer d'un certain nombre d'adresses IP publiques.

Si, pour une raison quelconque, l'adresse IP privée du poste iVisit change, ce poste de travail ne pourra plus communiquer avec d'autres postes dans d'autres commissions scolaires sans une nouvelle intervention du responsable du réseau (il doit reprendre les opérations mentionnées au point 3.2.2.2). C'est le principal inconvénient de cette solution. Comme l'utilisation de l'application iVisit fonctionnera à l'intérieur de la Commission scolaire de l'Énergie, il n'est pas certain que le problème sera détecté rapidement.

### ***Mise à l'essai***

À notre connaissance, cette solution est uniquement utilisée par la Commission scolaire de l'Énergie. Des tests ont été effectués à plusieurs reprises lors de sessions de vidéoconférence entre plusieurs postes iVisit situés derrière leur coupe-feu en communiquant avec deux autres postes iVisit derrière un autre coupe-feu.

#### **3.2.2.3 Solution de la Commission scolaire de Charlevoix**

À la Commission scolaire de Charlevoix, la situation est complexe. On y dispose de trois coupe-feu : un coupe-feu PIX de Cisco, un serveur Microsoft ISA et un serveur Fortinet. Ce dernier a été introduit en vue d'exercer une forme de contrôle parental à l'égard du Web. En conséquence, il comporte un module coupe-feu. Il offre également un serveur du type Dynamic Host Configuration Protocol (DHCP).

On doit donc tenir compte de la présence de trois coupe-feu dans cette commission scolaire.

Comme le serveur Fortinet offre un bon nombre de possibilités de configuration, il a été utilisé dans l'élaboration d'une solution pour l'application iVisit. Il faut préciser dès maintenant que les connexions iVisit qui passent par le serveur Fortinet ne transitent ni par le coupe-feu PIX de Cisco ni par le serveur Microsoft ISA.

Chaque poste devant employer l'application iVisit pour communiquer avec d'autres écoles à l'extérieur de la Commission scolaire de Charlevoix doit être identifié :

- La Commission scolaire de Charlevoix doit pouvoir disposer d'un certain nombre d'adresses IP publiques;
- Le responsable du réseau informatique établit un réseau virtuel entre chaque poste qui utilise l'application iVisit jusqu'au serveur Fortinet. Cela suppose que le poste iVisit qui est lié par un réseau virtuel doit toujours être relié à la même place dans le commutateur (switch) de l'école;
- Le DHCP du serveur Fortinet fournit toujours la même adresse IP privée au poste iVisit raccordé à la prise du commutateur de l'école;
- Le responsable du réseau associe, dans son coupe-feu (serveur Fortinet), chaque adresse IP des postes iVisit à une adresse IP publique. Ainsi, le contrôle parental demeure en fonction puisque ce dernier et le coupe-feu sont sur le même serveur;
- Le responsable du réseau ouvre son coupe-feu pour chacune de ces adresses IP afin d'autoriser l'utilisation des ports nécessaires au bon fonctionnement de l'application iVisit. Il s'agit de permettre au minimum l'utilisation en sortie des ports UDP 9946, 9947 et 9948 pour communiquer avec le serveur iVisit. Le responsable du réseau doit également s'assurer qu'il est possible d'utiliser en entrée et en sortie le port UDP 9940. S'il désire permettre à ses écoles de prendre contact avec un plus grand nombre d'utilisateurs dans d'autres commissions scolaires, il devra ouvrir en sortie l'ensemble des ports UDP supérieurs ou égaux au port UDP 1024.

Cette procédure permet ainsi à des utilisateurs de l'application iVisit dans une école de la Commission scolaire de Charlevoix de joindre des utilisateurs de la même application dans une école d'une autre commission scolaire.

## ***Avantages***

Si toutes les conditions sont réunies, cette solution est fonctionnelle et elle permet de conserver un contrôle parental sur les postes iVisit.

Cette solution s'avère une pratique très sécuritaire, car seuls les postes iVisit peuvent accéder aux ports qui sont ouverts. Le réseau virtuel permet également d'isoler ces postes du reste du réseau interne.

## ***Inconvénients***

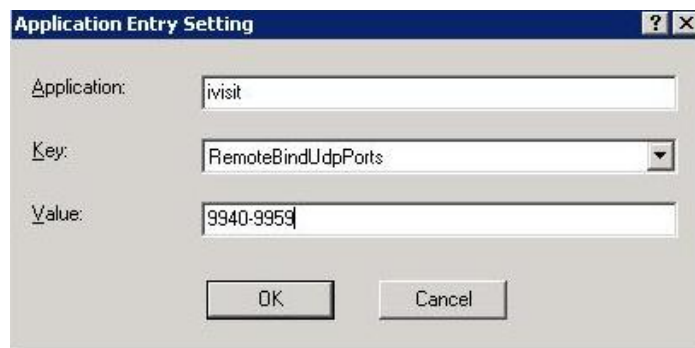
La Commission scolaire de Charlevoix doit pouvoir disposer d'un certain nombre d'adresses IP publiques.

Le poste qui utilise l'application iVisit doit être connecté dans la prise du commutateur prévue à cet effet et dans aucune autre. Le poste iVisit est isolé des autres postes de l'école et de la Commission scolaire de Charlevoix. Par exemple, l'accès à l'imprimante réseau de l'école n'est plus possible.

### **3.2.3 SOLUTION LIÉE AU SERVEUR MICROSOFT ISA**

L'une des fonctionnalités intéressantes du serveur Microsoft ISA est de permettre au coupe-feu de réagir (ouverture de port) à une application sur le poste client. Sans un tel logiciel client, un coupe-feu ne peut réagir qu'à des trames réseau.

Cette solution permet d'ouvrir le port en écoute sur le serveur Microsoft ISA seulement quand l'application (« ivisit.exe ») est démarrée. Sur le serveur Microsoft ISA, dans les paramètres du client, on définit un nouveau paramètre où l'on associe l'application « ivisit.exe » à une série de ports UDP (dans le cas présent on a utilisé les ports 9940 à 9959, car dix-neuf adresses étaient amplement suffisantes pour les tests).



Ensuite, sur chaque poste de travail ayant recours à l'utilisation iVisit, on installe le client du serveur Microsoft ISA à partir d'un partage fait sur le serveur en question sur lequel on a défini le paramètre. Sur ces postes de travail, on fixe le protocole source utilisé par l'application iVisit dans le fichier « config.ivb » de façon que chaque poste de travail fasse usage d'un port différent.

Au démarrage de l'application iVisit, le client ISA avisera le serveur Microsoft ISA d'être à l'écoute sur le port UDP utilisé par cette application sur ce poste de travail, tel qu'il est défini dans le fichier « config.ivb », dans la mesure où celui-ci est inclus dans l'éventail des ports définis dans les paramètres du client (ports UDP 9940 à 9959 dans l'exemple mentionné plus haut).

### **3.2.3.1 Avantages**

Cette solution offre un maximum de sécurité et une seule adresse IP publique est nécessaire.

### **3.2.3.2 Inconvénients**

L'inconvénient de cette solution est qu'elle nécessite un coupe-feu de type Microsoft ISA Server. Elle exige en outre l'installation du client ISA Server (testé avec le serveur Microsoft ISA 2004).

## **3.2.4 SOLUTION PIX/ASA**

Le temps imparti au groupe de travail technique pour effectuer la présente recherche ne lui a pas permis de rendre à terme la solution PIX/ASA. Des travaux ultérieurs apporteront l'éclairage attendu à cet égard.

## **3.2.5 SOLUTION LIÉE À L'OUVERTURE PARTIELLE DES PORTS**

La solution qui consiste à faire l'ouverture partielle des ports permet de communiquer avec un certain nombre de commissions scolaires avec qui il était, auparavant, impossible de le faire à l'aide de l'application iVisit si l'on était derrière un coupe-feu.

À l'heure actuelle, il est très difficile de communiquer avec une commission scolaire qui aurait comme politique de n'ouvrir en sortie que les ports UDP 9940, 9946, 9947 et 9948 et en entrée que le port UDP 9940. Dans un tel cas, il serait nécessaire, dans les autres commissions scolaires, que l'adresse IP de chaque poste iVisit soit associée à une adresse IP publique de manière à forcer l'utilisation du port UDP 9940.

Chaque poste qui compte utiliser l'application iVisit pour communiquer avec d'autres écoles à l'extérieur de la commission scolaire doit être identifié.

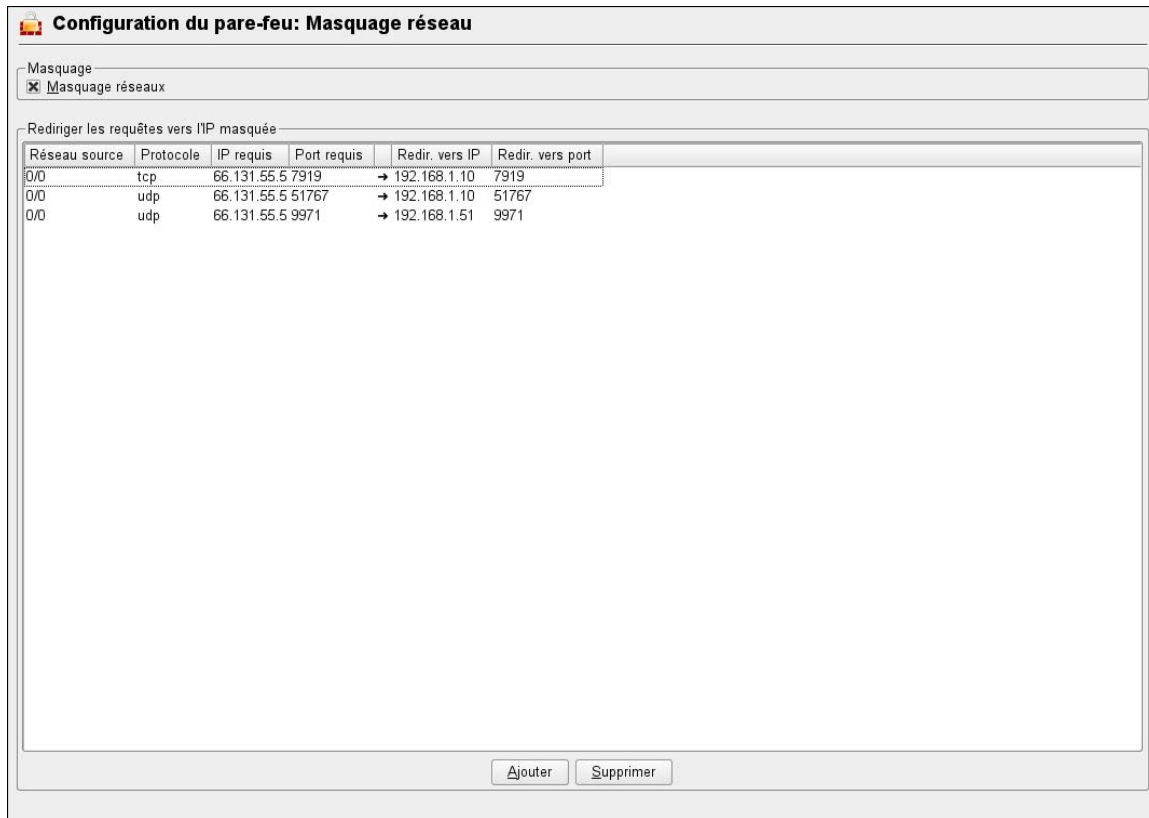
On doit s'assurer que ce poste de travail utilise la version 3.7.3 de l'application iVisit ou toute autre version plus récente de cette dernière qui tient compte du fichier de configuration « config.ivb » :

- Le responsable du réseau de la commission scolaire doit employer, pour chaque poste iVisit, un fichier « config.ivb » qui contient un port différent. Ce fichier doit être placé à la racine du répertoire iVisit;
- L'adresse IP privée (adresse interne à la commission scolaire) du poste iVisit doit être transmise au responsable informatique du réseau Internet de la commission scolaire ainsi que le numéro du port utilisé dans le fichier « config.ivb »;
- Le responsable du réseau doit associer, dans son coupe-feu, chaque adresse IP des postes iVisit et le port employé dans l'adresse IP publique de son coupe-feu;
- Le responsable du réseau doit permettre l'utilisation en sortie des ports UDP 9946, 9947 et 9948 de même que de chacun des ports spécifiés dans tous les fichiers « config.ivb ». Il doit également ouvrir en entrée chacun des ports UDP des fichiers « config.ivb ».

Voici un exemple du fichier « config.ivb » :

```
s=1  
local_port=9971
```

Voici des exemples d'une association d'une adresse IP à un port :



Pour harmoniser entre elles les pratiques des commissions scolaires qui choisissent de fermer en sortie tous les ports UDP, il faudrait convenir d'ouvrir en sortie un certain nombre de ports UDP. Ce serait alors la commission scolaire qui disposerait du plus grand nombre de postes iVisit qui servirait à déterminer le nombre minimal de ports à ouvrir. Toutes les commissions scolaires désirant communiquer entre elles devraient en conséquence utiliser les mêmes ports UDP.

Cette procédure devrait permettre à des utilisateurs de l'application iVisit dans une école de la commission scolaire de joindre des utilisateurs de cette application dans une école d'une autre commission scolaire.

### 3.2.5.1 Avantages

Si toutes les conditions sont réunies, cette solution demeure relativement simple et demande peu d'intervention de la part du personnel technique.

Cette solution permet de contourner la majorité des inconvénients liés à l'utilisation d'un réseau virtuel, communément appelé VLAN.

Lorsqu'il y a coordination entre les commissions scolaires, cette solution permet d'éviter d'ouvrir tous les ports UDP en sortie.

### **3.2.5.2 Inconvénients**

Si, pour une raison quelconque, l'adresse IP privée du poste iVisit change, ce poste de travail ne pourra plus communiquer avec d'autres classes dans d'autres commissions scolaires sans une nouvelle intervention du responsable du réseau (il doit reprendre les opérations mentionnées au point 3.2.5). C'est le principal inconvénient de cette solution. Il serait préférable que l'adresse IP des postes iVisit demeure fixe.

Comme l'utilisation de l'application iVisit fonctionnera à l'intérieur de la commission scolaire, il n'est pas certain que le problème sera être détecté rapidement.

Cette solution nécessite une volonté de coordination entre chacune des commissions scolaires quant à la plage des ports UDP qui sera utilisée.

### **3.2.5.3 Mise à l'essai**

Un seul test a été effectué à ce jour. Il est donc nécessaire d'en faire d'autres avec les principaux coupe-feu qui utilisent les commissions scolaires. En théorie, cette solution devrait pouvoir s'appliquer à tous les types de coupe-feu et être fonctionnelle partout.

## **4 Conditions d'utilisation et d'optimisation de l'application iVisit**

Une fois les problèmes liés à la connectivité surmontés, il existe des conditions facilitantes pour l'utilisation du logiciel de vidéoconférence iVisit, notamment la disponibilité de la bande passante et le paramétrage d'un logiciel du type anti-virus. Cependant, le temps qui était imparti au groupe de travail technique pour la production du présent rapport ne lui a pas permis d'explorer ces avenues ou toute autre solution connexe. Soit dit en passant, dans certains environnements informatiques, on a rapporté une dégradation progressive de la communication, d'abord du signal vidéo et ensuite du signal audio. Bien que cette situation ne soit pas généralisée, elle ne doit pas être négligée pour autant. Des études additionnelles sont donc nécessaires.

Le groupe de travail technique juge important que la version française la plus récente de l'application iVisit soit installée dans les écoles, et ce, pour tenir compte de l'existence d'un fichier de configuration sur le client iVisit.

De plus, il est suggéré de configurer l'antivirus (c'est-à-dire exclure la vérification du répertoire iVisit).

Enfin, la vidéo et l'audio demandent une grande stabilité du lien réseau. La configuration de la carte réseau doit correspondre à la configuration du commutateur pour éviter des lenteurs ou conflits.

## **Conclusion**

Le groupe de travail technique considère que toutes les solutions décrites plus haut et leurs variantes constituent des solutions viables pour les commissions scolaires. Depuis leur mise en œuvre, aucune des solutions avancées n'a occasionné de faille connue concernant la sécurité informatique, tel que cela a été rapporté par les commissions scolaires aux auteurs du présent rapport.

À noter que, en tant que telle, la solution idéale n'existe pas. Chaque solution comporte des avantages et des inconvénients. Si la sécurité représente un facteur pouvant influencer sur le choix en faveur de l'une ou l'autre solution, la gestion des postes de travail est un autre facteur à prendre en considération. En grande partie, le choix d'une solution dépend de la priorité accordée à ces questions. Bien sûr, il appartient aux commissions scolaires de privilégier celles qui s'harmonisent le mieux avec leur *modus vivendi* informatique et les priorités internes qu'elles se sont données.

## **Rétroaction au sujet du rapport**

Les auteurs du présent rapport sollicitent la rétroaction des lecteurs quant à son contenu. Pour joindre le groupe de travail technique, il suffit de communiquer avec Sonia Sehili, coordonnatrice des TIC à la Société GRICS et co-auteure de cette recherche par courriel ([sonia.sehili@grics.qc.ca](mailto:sonia.sehili@grics.qc.ca)) ou par téléphone (514 251-3700, poste 3913).