Réseau et contrôle d'un ordinateur à distance

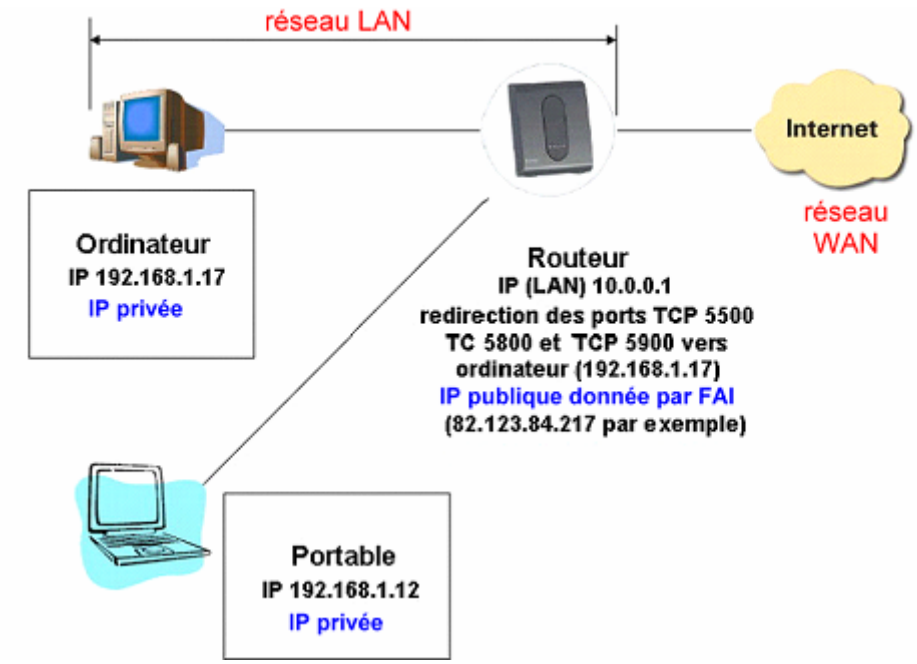
Quand vous vous connectez à Internet, votre Fournisseur d'Accès à Internet, appelé aussi FAI, attribue à votre ordinateur une adresse IP qui identifie votre porte d'entrée sur le réseau Internet : vous êtes seul à disposer de cette adresse au moment où vous vous connectez sur le réseau Internet. A chaque connexion, votre fournisseur d'accès vous délivre une adresse IP nouvelle appelée aussi IP dynamique : chez Wanadoo, cette adresse IP a un bail de 24h, c'est à dire que si vous laissez votre connexion ouverte indéfiniment, elle sera fermée au bout de 24h et une autre sera ouverte.

Entre votre ordinateur de bureau et votre ordinateur personnel, deux principaux chemins peuvent exister :

En général votre ordinateur de bureau est relié directement au réseau de votre entreprise en relation avec un routeur, tandis que votre ordinateur personnel dispose, soit d'une liaison modem simple, soit d'une liaison ADSL permanente par l'intermédiaire d'un modem-routeur (LiveBox, FreeBox…).

Dans le cas d'un ordinateur personnel connecté directement par modem, l'adresse IP fournie par votre FAI et l'adresse IP de votre ordinateur sont les mêmes : c'est l'adresse IP publique. En revanche lorsqu'un routeur est associé à votre modem - Livebox, Freebox… -, votre ordinateur prend une adresse IP différente de celle fournie par le FAI : c'est l'adresse IP privée. Le schéma de votre connexion et de ses adresses IP associées est le suivant (il est rarement fait mention de l'adresse IP privée de votre routeur) :

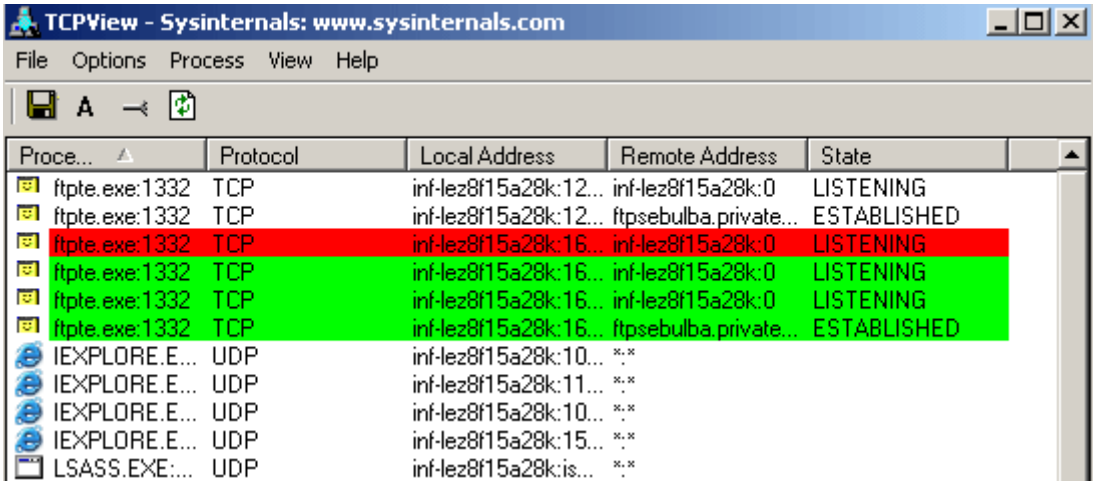
Schéma d'un réseau local simple :



- Pour déterminer votre adresse IP publique, il suffit de se rendre par exemple sur le site http://whatismyip.org (il existe de nombreux sites offrant la même fonction) et de lire la suite de chiffres - 82.123.84.217 par exemple – qui apparaît : c'est votre adresse IP publique.

- Pour déterminer votre adresse IP privée, faites **Démarrer** >> **Exécuter** >> taper « **cmd** » puis validez : une fenêtre DOS noire apparait. Tapez « **ipconfig** » et validez. La ligne intitulée « Adresse IP » indique votre adresse - 192.198.1.17 par exemple - : c'est l'adresse IP privée de votre ordinateur.

L'ordinateur situé derrière votre routeur est inconnu pour le réseau Internet. Ainsi, lorsqu'une requête est envoyée vers votre routeur à votre adresse IP publique, il n'est pas possible d'atteindre votre ordinateur sans spécifier au routeur de renvoyer la requête vers votre ordinateur puisque ce dernier possède une adresse IP privée différente : cette opération s'appelle la redirection de port (port forwarding). Internet peut être assimilé à un tube arrivant à votre ordinateur et constitué de tuyaux numérotés de 1 à 65535 appelés « port », chaque application réseau utilisant un port bien défini. La liste des ports TCP et UDP utilisés et des applications Internet associées, ainsi que l'adresse des serveurs distants peuvent être affichés pour un ordinateur quelconque à l'aide de l'application TCPView :



TCPView permet de connaître en temps réel les logiciels qui utilisent votre connexion Internet, de repérer éventuellement les logiciels espions (ou spywares) et de stopper la connexion pour ces derniers (clic droit – **Close connection**).

Par construction, votre routeur est configuré pour transmettre à votre ordinateur tous les paquets de données reçus. Toute requête arrivant vers un routeur avec un port déterminé est envoyée dans le cas d'un réseau constitué de plusieurs PC vers un ordinateur déterminé, désigné par son adresse IP privée ; dans le cas d'un PC unique, chaque requête arrivant vers le routeur sur le port xxxx est renvoyé vers l'adresse IP privée de cet ordinateur : si l'on souhaite accéder depuis l'extérieur au serveur web hébergé sur votre ordinateur dont l'adresse est IP 192.168.1.17, il sera nécessaire de définir sur la passerelle une règle de redirection de port redirigeant tous les paquets TCP reçus sur le port 80 vers l'ordinateur qui abrite le serveur web 192.198.1.17 par exemple, le port 80 étant le port réservé pour ce type de requête.

Prendre le contrôle d'un ordinateur à distance permet d'effectuer des opérations de maintenance, des sauvegardes ou de résoudre un problème de configuration... sans avoir à se déplacer : accéder à son ordinateur en dehors de son domicile, aider un utilisateur inexpérimenté, utiliser un ordinateur qui ne dispose pas d'écran...

Pour prendre le contrôle d'un ordinateur à distance, on utilise deux parties d'un même logiciel :

- un module **Serveur** ou **Server** installé sur l'ordinateur à contrôler ;
- un module **Client** appelé aussi **Viewer** installé sur l'ordinateur à partir duquel on prend le contrôle.

L'**ordinateur distant** - le Serveur - met ses ressources à disposition de l'**ordinateur local** - le Client - : ici, les notions de « serveur » et de « client » utilisées pour le contrôle à distance sont définies différemment des notions habituelles de client/serveur utilisées pour le web.

VNC (ou ses logiciels annexes **Ultr@VNC**, **TightVNC**…) est le logiciel libre de prise de contrôle Open Source le plus utilisé sous Windows ou sous Linux. Dans le cas du système d'exploitation Windows :

- sur l'ordinateur à contrôler, vous installez Ultr@VNC Serveur ;
- sur votre ordinateur, vous installez le viewer, version Client du même logiciel Ultr@VNC.

Vous pouvez également accéder à un ordinateur distant sans installer Ultr@VNC Client en utilisant simplement Internet Explorer (ou un autre navigateur) associé à une machine Java installée sur votre ordinateur (il faut que Ultr@VNC Serveur soit installé sur l'ordinateur distant et le Client Java activé). Dans ce cas, l'adresse à taper dans le navigateur est par exemple http://82.123.84.217:5800 où 82.123.84.217 est l'adresse IP publique de l'ordinateur à contrôler et 5800 le port utilisé par l'applet Java (port à spécifier sur votre routeur pour le NAT Network Address Translation).

Microsoft intègre aux systèmes Windows XP Pro, Windows 2000 serveur et Windows 2003 un logiciel de prise de contrôle appelé **TSE** pour Terminal Server Edition. Pour utiliser le module TSE, il faut :

- Installer le module Serveur : clic droit sur **Poste de travail** >> **Propriétés** et dans l'onglet **Utilisation à distance**, cocher la case « Autoriser les utilisateurs à se connecter à distance à cet ordinateur ». Dans ce cas de figure, le port à spécifier sur votre routeur pour le NAT est le port 3389 ;
- Installer le module Client : sous Windows XP, allez dans **Démarrer** >> **Tous les programmes** >> **Accessoires** >> **Communication** >> **Connexion bureau à distance**. Saisir l'adresse IP Publique de votre ordinateur dans le champ **Ordinateur**, puis cliquer sur **Connexion**. Les réglages sont disponibles en cliquant sur **Options**. Il est préférable d'utiliser un affichage réduit en couleurs et en taille pour que l'affichage soit le plus fluide possible (mode d'emploi).

Microsoft intègre aussi avec Windows XP Pro et Windows 2003 serveur la fonction Web Interface for Remote Administration **:**

- Installation du module Serveur : clic droit sur **Poste de travail** >> **Propriétés** et dans l'onglet « Utilisation à distance », cocher la case « Autoriser les utilisateurs à se connecter à distance à cet ordinateur ». Allez ensuite dans **Ajout suppression de programmes** >> **Ajouter ou supprimer des composants de Windows** >> **Services Internet IIS** >> **Service World Wide Web** ; puis cocher la case intitulée « Connexion Web au bureau à distance ». Validez ensuite **OK** à chaque fois (il sera nécessaire d'insérer le CD d'installation de Windows). Dans ce cas de figure, le port à spécifier sur votre routeur pour le NAT est le port 80.
- Sur votre ordinateur personnel, ouvrir Internet Explorer et taper dans la barre d'adresse par exemple http://82.123.84.217/tsweb (où 82.123.84.217 est l'IP publique de l'ordinateur à contrôler). Votre navigateur vous demandera d'installer le contrôle ActiveX associé à tsweb.

Votre ordinateur intègre surement un pare feu (ou firewall). Pour utiliser les logiciels de prise de contrôle, ceux associés à Windows XP ou les autres, vous devez obligatoirement laisser passer les requêtes vers les ports utilisés par ces logiciels de contrôle :

- 5500 pour le module Ultr@VNC module Client Viewer (en mode Ecoute)
- 5900 pour le module Ultr@VNC module Serveur
- 5800 pour Ultr@VNC par le web
- 3389 pour TSE
- 80 pour Web Interface for Remote Administration (si ce port n'est pas ouvert, vous n'atteindrez jamais votre ordinateur personnel)

Ces modifications sont souvent réalisées automatiquement sous réserve de votre autorisation au moment de l'installation des logiciels de contrôle à distance.

Il est possible que l'ordinateur à contrôler soit placé derrière un proxy qui ne laisse passer par exemple que les requêtes utilisées pour surfer sur Internet, le port 80. Dans ce cas, le choix du logiciel à

utiliser pour contrôler simplement votre PC est plus restreint : c'est Web Interface for Remote Administration ou un logiciel équivalent passant nativement par le port autorisé. Par contre, lorsque vous souhaitez accéder depuis votre bureau à votre ordinateur personnel, vous allez lancer une requête vers ce dernier en traversant le plus souvent plusieurs routeurs : cette procédure est possible pour la plupart des logiciels de contrôle à distance car le routeur de votre bureau laisse passer les requêtes en sortie vers l'extérieur ; par contre, il est le plus souvent programmé pour stopper les requêtes en sens inverse.

Conseils :

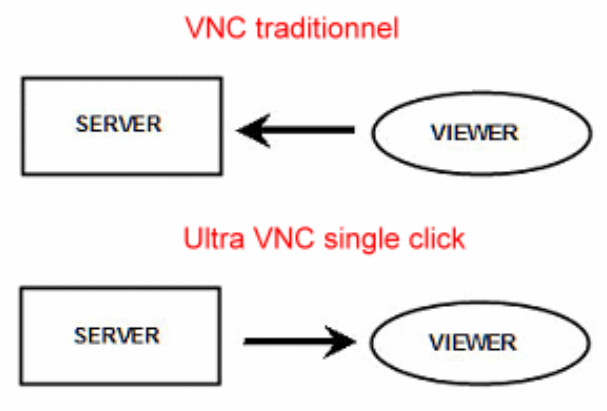
- Si vous disposez d'un routeur qui ne garde pas la connexion Internet ouverte indéfiniment, vous devrez installer un logiciel qui se charge de ré ouvrir cette connexion pour vous comme Casc'ADSL (http://cascadsl.free.fr/download/cascadsl.exe) ou tout autre logiciel remplissant la même fonction.

- Pour éviter les inconvénients liés au changement d'IP journalier ou à chaque connexion nouvelle, il existe une méthode simple pour authentifier votre ordinateur sur le réseau Internet : créer un nom de domaine unique. Il vous faut pour cela ouvrir un compte gratuit sur http://www.dyndns.com ou http://www.no-ip.com, puis créer un nom de domaine. Ce nom de domaine se substituera à votre adresse IP : par exemple, au lieu de taper http://82.123.84.217/tsweb, vous taperez http://nomdedomaine/tsweb (tutorial). Vous pouvez aussi attribuer par l'intermédiaire de votre fournisseur d'accès une adresse fixe à votre ordinateur (service en général non gratuit).

- Pour que votre adresse IP publique corresponde bien à votre nom de domaine, il faut une mise à jour constante de votre nouvelle IP publique sur les serveurs Dyndns ou No-Ip chaque fois que vous connectez votre ordinateur à Internet. Pour cela, votre routeur intègre en général une gestion des comptes Dyndns ou No-Ip : il suffit juste de configurer votre compte Dyndns ou No-Ip dans votre routeur pour actualiser définitivement votre adresse publique et votre nom de domaine. En revanche, si vous ne disposez pas d'un routeur de ce type, vous pouvez utiliser un logiciel comme Casc'ADSL qui gère aussi cette fonctionnalité.

La difficulté principale du contrôle à distance est que, dans les solutions classiques comme VNC ou Ultr@VNC par exemple, la connexion s'établit du client - le poste de l'assistant (ou viewer) - vers le serveur la machine à assister (ou server), ce qui implique qu'une connexion entrante vers le poste à contrôler puisse être établie. Dans la majorité des cas, cette connectivité entrante ne peut être réalisée que si les réglages correspondant à cet ordinateur ((firewall, routeur, proxy, autorisations, règles de translation de port et/ou d'adresse…) intègrent cette connexion entrante dans sa configuration : rien de simple si le poste que vous souhaitez contrôler est éloigné ou administré par une personne ayant peu d'expérience, ou si encore celui-ci est géré par des administrateurs réseaux « pointilleux », notamment lorsque la sécurité est primordiale comme pour un réseau d'entreprise (Intranet…).

Pour contourner ce problème, la solution **Ultr@VNC SingleClic** ou **Ultra@VNC SC** inverse le sens de la connexion : la connexion entrante est établie du Serveur (le poste à assister) vers le Client (le poste de l'assistant), et non plus l'inverse :



L'intérêt est que c'est du côté du poste de l'assistant, c'est-à-dire votre ordinateur, que l'infrastructure informatique doit être modifiée et correctement paramétrée pour accepter une connexion entrante en

principe le port 5500 : vous êtes plus compétent sur les problèmes de réseau et il vous est plus facile d'intervenir sur votre ordinateur que sur la machine que vous vous proposez de contrôler. Le seul point qui subsiste est que le poste à dépanner doit pouvoir ouvrir une connexion directe vers le port 5500 d'une machine extérieure. Ce point dépend là encore de l'infrastructure du poste informatique sur lequel vous souhaitez intervenir (firewall personnel ou réseau, proxy…). Ultr@VNC SingleClic est utilisable dans la plupart des cas, mais il subsiste malgré tout quelques situations d'impossibilité ou de complexité parfois non résolues. UltaVNC SimpleClic III ou la nouvelle version PcHelpWare permet de résoudre ces difficultés.

L'objectif de cette mise au point est d'apporter les explications nécessaires pour exploiter et mettre en œuvre Ultr@VNC, Ultr@VNC SingleClic et PcHelpWare. Cette logique d'utilisation expliquée simplement est reprise pour un panel d'applications commerciales mises gratuitement à disposition sur le web pour un usage non commercial.

Jean-Claude Dufresne

jcdestinator@gmail.com

Avril 2007

Impression
Mot de passe : jcd