# Accès au réseau informatique de l'ENSEEIHT

## depuis l'extérieur

## Z. Hamrouni – septembre 2020

## 1 Le réseau informatique de l'ENSEEIHT

Le réseau informatique d'enseignement de l'N7 comprend quelques centaines d'ordinateurs répartis sur une vingtaine de salles de travaux pratiques (TP). Une grande partie de ces ordinateurs fonctionnent sous le système Linux, principalement pour les enseignements des départements SN et MF2E.

Tous les ordinateurs de TP sont sur réseau, et chaque étudiant peut se connecter sur son compte (login et mot de passe LDAP fournis après l'inscription) depuis n'importe quel ordinateur du réseau ENSEEIHT, mais aussi depuis l'extérieur en suivant une procédure sécurisée.

Chaque ordinateur de TP porte un nom (boole, gobelin, …), et aussi un alias composé du nom de la salle et du numéro de l'ordinateur dans la salle : par exemple c201-05. Ces ordinateurs sont accessibles depuis l'extérieur avec leur adresse IP (pas facile à retenir), mais aussi par leur nom ou leur alias, par exemple gobelin.enseeiht ou c201-05.enseeiht.fr

Dans la situation la plus simple, votre ordinateur servira comme simple terminal, et tout votre travail sera effectué sur un des ordinateurs du réseau N7. Cette facilité présente de nombreux avantages :

- Votre ordinateur personnel n'a pas besoin d'avoir la même configuration que ceux du réseau n7 : il peut fonctionner sous n'importe quel système classique : Windows, Linux, ou MacOs.
- Vous n'avez pas besoin d'installer sur votre ordinateur des logiciels spécifiques pour l'enseignement.
- Vous gardez vos données liées à l'enseignement dans un seul endroit sécurisé (votre compte N7) et vous n'avez pas besoin de gérer et de mettre des copies de ces données sur votre ordinateur.

Pour accéder au réseau N7 depuis l'extérieur, vous devez posséder un ordinateur personnel (Windows, Linux, MacOs, ...), une connexion internet, et installer les outils nécessaire en suivant la procédure décrite dessous.

### 2 Installation du VPN

Un VPN (Virtual Private Network) est un dispositif qui permet la création de connexions directes entre des ordinateurs distants via internet. Dans notre cas, une connexion VPN N7 permettra à votre ordinateur d'être connecté sur le réseau N7, pour pouvoir avoir accès aux

ressources de ce dernier, et vous permettre d'accéder à votre espace de données, aux logiciels et aux outils destinés à l'enseignement.

Pour installer le VPN d'accès au réseau N7, il faut :

• aller sur la page DSI Inp-Toulouse (accès sécurisé par login et mot de passe LDAP)



- cliquer sur le lien Mobilité-Nomadisme(...) dans la rubrique "Mon compte" en haut à gauche de la page
- dans cette page, cliquer sur le lien VPN (Accès au réseau depuis l'extérieur)
- dans cette page, cliquer sur le lien VPN-INP (A7, N7, ...)
- dans cette page, choisir le lien selon votre système (Windows, MacOs ou Linux), et suivre la procédure d'installation, qui est facile pour Windows mais un peu délicate pour Linux.

On peut accéder directement à cette dernière page via ce lien :

Il faut correctement paramétrer l'outil vpn :

- portail : go.inp-toulouse.fr
- passerelle : gpvpn-n7

Pour vérifier si votre ordinateur est connecté au réseau N7 via VPN, il suffit de lancer une commande "ping" vers une machine de ce réseau. Pour cela :

• ouvrir un terminal de commandes. Sur Windows, il faut exécuter "Invite de commandes" que l'on trouve normalement dans la rubrique "accessoires", ou que

l'on peut trouver en tapant "command" dans la barre de recherche du menu de fonctions (en bas à gauche).

- exécuter la commande "ping –n 3 c201-05.enseeiht.fr" et vérifier la réponse :
  - ordinateur connecté au réseau N7: Réponse de 147.127...: octets=32 temps=32ms ....

Invite de commandes
C:\Users\charlie-adm>ping -n 3 c201-05.enseeiht.fr
Envoi d'une requête 'ping' sur gobelin.enseeiht.fr [147.127.133.13] ts de données :
Réponse de 147.127.133.13 : octets=32 temps=34 ms TTL=62
Réponse de 147.127.133.13 : octets=32 temps=32 ms TTL=62
Réponse de 147.127.133.13 : octets=32 temps=32 ms TTL=62
Statistiques Ping pour 147.127.133.13:
Paquels : enouges - 3, reçus - 3, perdus - 0 (perle 0%),
Duree approximative des boucles en millisecondes :
Minimum = 32ms, Maximum = 34ms, Moyenne = 32ms

o Ordinateur non connecté : Délai d'attente de la demande dépassé

```
Invite de commandes
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\charlie-adm>ping -n 3 c201-05.enseeiht.fr
Envoi d'une requête 'ping' sur gobelin.enseeiht.fr [147.127.133.13]
ts de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Statistiques Ping pour 147.127.133.13:
    Paquets : envoyés = 3, reçus = 0, perdus = 3 (perte 100%),
```

**ATTENTION** : quand vous utilisez le VPN, vous êtes connecté au réseau de l'N7, et tous les accès internet de votre ordinateur passent par le réseau de l'école. Il faut donc :

- penser à respecter la charte informatique (pas de téléchargement illégal,...)
- vous déconnecter dès que votre travail est terminé

#### 3 Utilisation d'un outil de connexion sécurisée à votre compte

Une fois connecté au réseau N7 via le VPN, vous pouvez vous connecter à votre compte avec votre login et mot de passe LDAP. Mais pour que cette connexion soit sécurisée, il faut utiliser un outil basé sur un protocole sécurisé tel que SSH.

**SSH** (*Secure Session Host*) est à la fois un outil informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les échanges sont sécurisés (chiffrées).

Le protocole ssh (*Secure Session Host*) est l'un des outils les plus utilisés pour se connecter de façon sécurisée sur un ordinateur distant. Il offre un haut niveau de sécurité et garantit :

- La confidentialité : le chiffrement des paquets permet de garantir celle-ci. Les anciens services tels que telnet, rlogin... envoyaient les données en clair.
- L'intégrité : ssh permet de garantir que les paquets circulant d'un hôte vers un autre ne sont pas altérés.
- L'authentification : chaque connexion ssh vérifie l'identité de la cible (l'ordinateur distant) par sa clé d'hôte, et celle de la source (ordinateur depuis lequel on exécute ssh) par mot de passe ou clé enregistrée.

### <u>Client ssh</u>

Certaines configurations système disposent par défaut d'une installation d'un client ssh. Si cela n'est pas le cas pour le votre, il suffit de rechercher sur internet en utilisant les mots clés client ssh et le nom de votre système. Vous trouverez différents sites pour télécharger cet outil gratuit et des explications sur la procédure d'installation.

Voici ci-dessous un exemple de fenêtre bitvise-ssh sous Windows.

60	Login	Options	Terminal	Remote Desktop	SFTP	Services	C2S	S2C	SSH	About
	Server					Authentication				
	Host c202-07.enseeiht.fr				Username	e	hamroun	İ		
8	Port	22		Enable obfuscation		Initial met	thod	password	i	•
Save profile as	Obfu	scation k	eyword [			Password			•••••	••
	Kerber SPN	ros SPI/Kerb equest di SPI/Kerb	<b>eros 5 key</b> elegation eros 5 autl	exchange hentication		V Store	encry	pted pass	word in	orofile
	Prox	y settings	2	Host key manag	er	Client key	man	ager		Hel
	13:46 13:46 13:46 13:46	:46.524 :46.524 :46.524	Bitvise SSI Copyright Visit www Run 'BvSsi	H Client 6.41, a fully (C) 2000-2015 by Bit bitvise.com for lates h -help' to learn the	featured vise Lin t inform supporte	d SSH2 clier nited. nation about ed comman	nt. : our s d-line	SSH2 prod paramete	ucts. rs.	[

Vous devez y entrer :

- le nom de l'ordinateur distant sur lequel vous souhaitez vous connecter : nom.enseeiht.fr ou salle-num.enseeiht.fr (salle = c201, c202, ... ; num = 01, 02, ...)
- le port 22, généralement mis par défaut
- votre username (login), et votre mot de passe

Lorsque vous vous connectez sur un ordinateur distant pour la première fois, il vous sera demandé de confirmer votre confiance dans cet ordinateur distant en acceptant sa clé (pour une seule session) et de la sauvegarder si vous avez l'intention de réutiliser cette connexion.

Si la connexion à votre compte est réussie, vous verrez 2 fenêtres s'ouvrir :

 une fenêtre de transfert de fichier : vous pouvez ainsi naviguer dans votre espace de données, transférer des fichiers depuis votre ordinateur vers votre compte N7 (et inversement), éditer et modifier des fichiers de votre compte N7 avec un éditeur de votre ordinateur local.

Window Local Remote Upload queue	Download queue Log			
PBrowse 🛐 Upload queue 🛛 🛂 Downloa	ad queue 🏼 🦻 Log			
Local files		Remote files		
3 🕄 🎰   🗷 🖻 🏡 😂   F:\	- 💷 -	3 🕄 🙆 📧 🗟 🏠 /home/ha	mrouni	-
Name	*	Name	Size	Туре
L \$RECYCLE.BIN	III	👢 .adobe	4 096	Dossier d
AA .		📜 .cache	4 096	Dossier d
AAACONTPED		👢 .compiz	4 096	Dossier d
ADM_1A		📜 .config	4 096	Dossier d
	I.M.	1 Add	1 006	Dessiond
•	•	III	1	•

 et un terminal shell dans lequel vous pourrez taper vos commandes qui vont être exécutées sur l'ordinateur distant (de l'N7). Votre ordinateur ne sert que comme un terminal pour saisir les commandes et afficher leurs résultats.

Bitvise xterm - hamrouni@c202-07.enseeiht.fr:22	
hamrouni@phosphore:~\$	*

### <u>Putty</u>

Putty est un outil de connexion qui utilise le protocole SSH, mais n'offre par défaut qu'une interface shell simple (terminal). Et peut s'avérer moins pratique.

### Commande ssh / Linux et MacOs

Depuis Linux, on peut se connecter à une machine distante avec la commande ssh : ssh login\_utilisateur@nom\_machine.enseeiht.fr

Lors d'une première connexion par ssh à un ordinateur distant, ssh demande à confirmer l'authenticité du serveur distant et d'enregistrer une empreinte de sa clé sur la machine locale, de manière à ce que les connexions futures se fassent avec authentification automatique grâce à la clé enregistrée : répondre « Yes ».

Ce mécanisme repose sur le concept de cryptographie par clés découvert à la fin des années 70, et qui n'a cessé d'être enrichi avec différents protocoles (RSA, ECDSA, ...).

Cette phase d'authentification de l'ordinateur distant est un important élément de sécurité, car se connecter à un serveur dont on n'est pas sûr de l'identité et du rôle peut s'avérer très risqué.

hostAAA \$ *ssh C205-11* The authenticity of host 'c205-11 (147.127.143.111) can't be established. ECDSA key fingerprint is bd:xx:xx:xx:xx:xx:xx:xx:xx... Are you sure you want to continue connecting (yes/no)? En tapant yes, l'empreinte de l'ordinateur C205-11 est ajoutée au fichier ~/.ssh/known\_hosts de l'ordinateur local.

Après l'authentification du serveur, ssh doit sécuriser la connexion soit :

- par mot de passe : en entrant votre mot de passe, vous vous connectez sur la machine distante. Attention, rien n'est affiché lorsque vous tapez votre mot de passe.
- par un mécanisme de clés, qui fonctionne grâce à 2 éléments
  - une clé publique qui doit être déposée sur chaque hôte sur lequel on souhaite pouvoir se connecter. Cette clé est générée par la commande ssh-keygen, et est déposée par la commande ssh-copy-id nom\_orinateur\_distant
  - une clé privée, qui est locale, et qui permet de prouver son identité à la machine distante

C'est la correspondance entre ces clés qui permet d'authentifier la connexion.

hostAAA \$ *ssh-keygen* ... TAPEZ LA TOUCHE RETURN POUR TOUTES LES QUESTIONS ....

hostAAA \$ *ssh-copy-id C205-11* ... MOT DE PASSE EVENTUELLEMENT DEMANDE

hostAAA \$ *ssh C205-11* 

... aucun mot de passe demandé pour toutes les connections futures sur C205-11

### Affichage graphique

Les flux de données graphiques ne sont pas, par défaut, transmis à travers la connexion ssh. Par conséquent, pour pouvoir afficher, sur l'ordinateur local, les fenêtres graphiques des applications lancées sur l'ordinateur distant, il faut explicitement autoriser le flux graphique en ajoutant l'option -Y à la commande ssh. Cette option est plus sûre que l'ancienne -X, et ne fonctionne que si les environnements graphiques des deux ordinateurs sont compatibles. Cela est possible dans le monde Unix/X\_windows, mais assez difficile entre systèmes avec des modes graphiques hétérogènes non basés sur X\_windows.

### <u>x2go</u>

x2go est un logiciel client-serveur qui permet de se connecter en mode graphique à un ordinateur distant. C'est une solution du type « Remote Desktop » ou « Remote application », qui permet de transférer l'affichage du bureau de l'ordinateur distant sur l'ordinateur client (le votre).

Le site officiel d'X2GO présente une procédure de téléchargement libre et d'installation pour la plupart des OS. Voici un aperçu d'une session x2go de connexion sur un ordinateur de l'N7 : lors du premier lancement d'x2go, créez une nouvelle session (bouton dans la barre des menus), et paramétrez la avec le nom que vous souhaitez lui donner (ici connexion\_N7), le nom de l'ordinateur distant (ici : boole.enseeiht.fr), votre identifiant, et le type de session (ici MATE : environnement graphique utilisé sur les ordinateurs Linux de l'N7).

X2Go Client	Préférences de session - connexion_N7
Session Option	Session       Connection       Input/Output       Media       Dossiers partagés         Session name:       connexion_N7         Image: Connexion_N7       Image: Connexion_N7         Image: Co
	Server       Host:       boole.enseeiht.fr       Identifiant:       hamrouni       SSH port:       22       Use RSA/DSA key for ssh connection:
	<ul> <li>Try auto login (via SSH Agent or default SSH key)</li> <li>Kerberos 5 (GSSAP1) authentication</li> <li>Delegation of GSSAPI credentials to the server</li> <li>Use Proxy server for SSH connection</li> <li>Session type</li> <li>MATE Command:</li> </ul>
	Ok Cancel Défauts

X X2Go Client	
Session Options Aide	
connexion_N7 MATE on boole.enseeiht.fr	
Identifiant: hamrouni Password:	
Ok Cancel	

Pour vous connecter, cliquez sur la session voulue, et entrez votre mot de passe :

Si tout se passe bien, vous verrez apparaître sur votre écran, une fenêtre qui déporte l'affichage du bureau « MATE » depuis l'ordinateur distant, et sur laquelle vous pouvez agir comme si vous étiez devant l'ordinateur distant :

- lancer des applications via le bouton « Menu », sur l'ordinateur distant
- ouvrir des terminaux shell : Menu / Outils système / Terminal MATE
- en maintenant un clic gauche et en glissant l'icône d'une application vers la barre noire, vous pouvez y enregistrer les outils que vous utilisez régulièrement ; cela vous évitera d'aller les chercher dans le menu.

	connexion_N7					
	🚳 Menu 🍅	2	t	<b>↓</b> ◀)))	🔱 lun.	7 sept.,
	*					
	Dossier					
	ha <u>mrou</u> ni					
	Downloads					
I						

Comme lorsque vous quittez votre ordinateur N7, il faut veiller à :

- fermer toutes les applications lancées depuis le début de votre session (si vous laissez firefox ouvert, vous ne pourrez plus le lancer depuis une autre machine)
  - **♯ l**un.
- vous déconnecter en cliquant sur le bouton interrupteur en haut à droite

ATTENTION : Dans certaines situations (plantage, session mal fermée), x2go semble générer des fichiers « logs » très volumineux, risquant de saturer votre espace de données. Pensez à vous fermer correctement votre session, et à surveiller votre quota régulièrement, avec la commande quota par exemple : quota –s.