

# Comment parle-t-on sur un réseau

## Connexions aux périphériques réseaux, client-serveur

### ► BUT :

Connaître les différents moyens de se connecter à un périphérique réseau au travers du réseau que ce soit en CLI (console à écran noir ou bleu) ou en graphique (vnc, http).

### ► GLOSSAIRE :

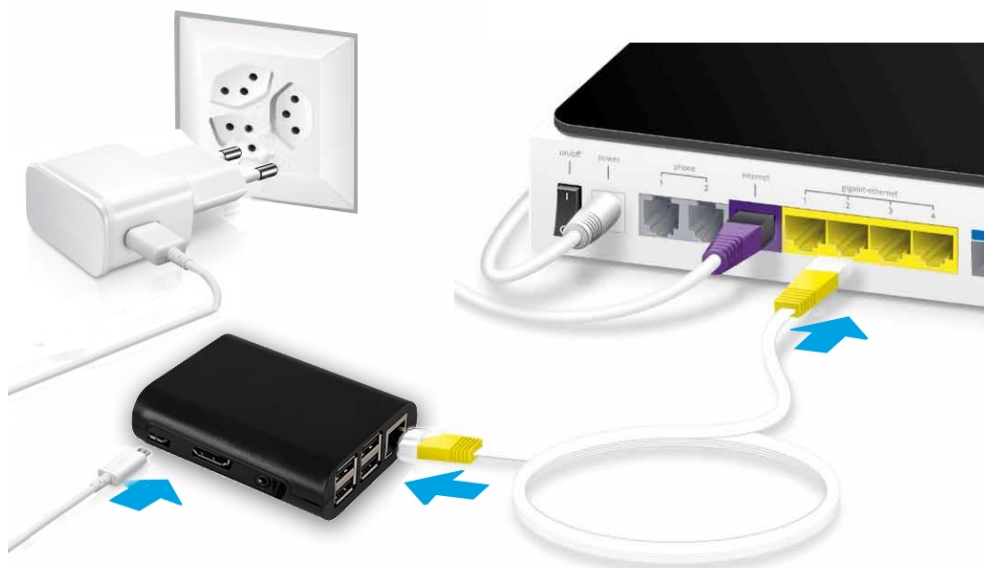
- hacking : Aux environs de 1960, les termes *hacking* et *hacker* sont introduits par le MIT. Ils désignent le fait de bidouiller et d'expérimenter pour le plaisir. ... (<https://fr.wikipedia.org/wiki/Hacking>). On va essayer de jouer comme un hacker, *white hacker* (canal historique).
- TPA : Travail pratique autonome, des TP pour aider les étudiants à JOUER avec l'informatique et le réseau périphérique réseau : n'importe quel « machin » branché sur le réseau (PC, natel, TV, console de jeux, box, routeur, switch, alarmes, webcam, Google home, ...)
- réseau : L'ensemble des liens (câbles, wifi, 4G ...) informatiques qui relient des périphériques
- telnet : Une norme ancienne simple et PAS sécurisée permettant de dialoguer entre périphériques
- ssh : Une norme SECURISEE permettant de dialoguer entre périphériques
- vnc : Une norme complexe SECURISEE permettant de dialoguer entre périphériques de manière graphique. Sa complexité a, par le passé, donné lieu à des piratages informatiques, normalement c'est du passé mais ...
- node-red : Outil de développement utilisant la programmation visuelle (origine IBM)
- http : Ce que vous utilisez tous les jours pour aller sur internet

### ► C'EST PARTI :

— Communication NON SECURE Telnet (*telecommunication network*) —

Brancher le Raspberry Pi sur votre box avec un câble RJ45.

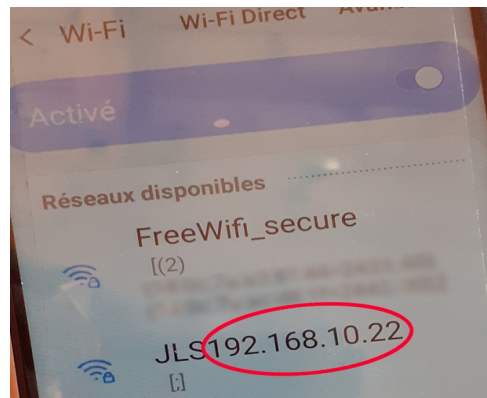
Alimenter le Raspberry Pi avec un chargeur de téléphone, attention au bord large du connecteur (côté Raspberry Pi).



Regarder sur votre natel les réseaux wifi.

Au bout de 30 secondes environ votre adresse IP liée à vos initiales va apparaître (cette connexion n'est pas fonctionnelle, c'est simplement un moyen facile de vous fournir l'adresse de votre Pi).

C'est cette adresse IP qui vous permettra de joindre la « boîte ».



Cette procédure fonctionne tout le temps (dès que vous branchez votre micro/mini ordinateur Raspberry Pi. Le message apparaît 30 secondes. Si vous souhaitez qu'il apparaisse plus longtemps il faut suivre la procédure en annexe. De manière identique vous pouvez changer vos initiales. Toutefois ces 30 sec de message suffisent pour noter l'adresse IP, et lorsque vous serez en cours vos initiales vous aideront pour retrouver la bonne IP parmi tous les messages wifi (de vos voisins) qui apparaîtront.

A partir de votre PC portable ou fixe, branché en filaire ou en wifi, on va maintenant se connecter sur la boîte noire...

#### — Communication NON SECURE Telnet (*telecommunication network*) —

##### Pour Macintosh :

On utilisera la fenêtre de terminal (⌘ N)

on saisit la ligne : telnet adresse\_IP\_Rpi 23 dans notre exemple `telnet 192.168.10.22 23`  
puis on valide avec la touche entrée

##### Pour Windows :

On va utiliser un logiciel de communication Putty

Si vous ne l'avez pas installé, on va le télécharger sur internet

(<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>)

vous choisissez la version suivant votre machine à priori : putty-64bit-0.74-installer.msi, une fois téléchargée vous installez Putty en double-cliquant l'application.

On lance Putty :

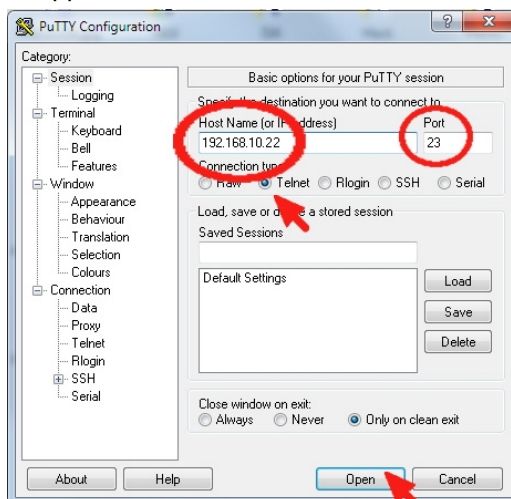
On configure

l'adresse IP ( 192.168.10.22 )

le port ( 23 )

et on n'oublie pas de cocher Telnet

puis on valide cliquant sur le bouton « Open »



Le logiciel Telnetd (d pour daemon ou service en français) est un logiciel qui fonctionne tout le temps (un serveur). On verra le prochain TPA comment arrêter son fonctionnement.

Les logiciels Telnet ou Putty sont des *logiciels client* utiles pour se connecter au service.

Le *protocole* Telnet (la manière de parler au périphérique) n'est pas sécurisée et le serveur Telnetd installé est bridé à quelques commandes. Il faut les essayer, pour vous familiariser avec cette manière classique de parler aux routeurs ou aux switchs (cisco ou autres), par exemple pour les configurer.

## — Communication SECURE Ssh (*Secure Shell*) —

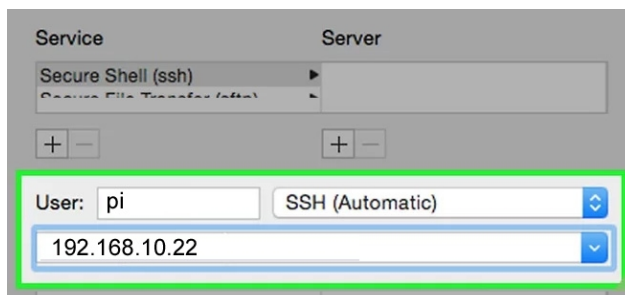
### Pour Macintosh :

On utilisera le fenêtre de terminal (⌘ N) puis dans le menu « Shell » choisir « New Remote Connection ... » ou bien saisir ⌘ K.

Choisir dans Service : Secure Shell (ssh)

L'utilisateur est **pi** par défaut  
Saisir votre adresse IP et fixer SSH

Le mot de passe par défaut est **raspberry**



### Poursuivre au paragraphe commun

### Pour Windows :

On va utiliser un logiciel de communication Putty

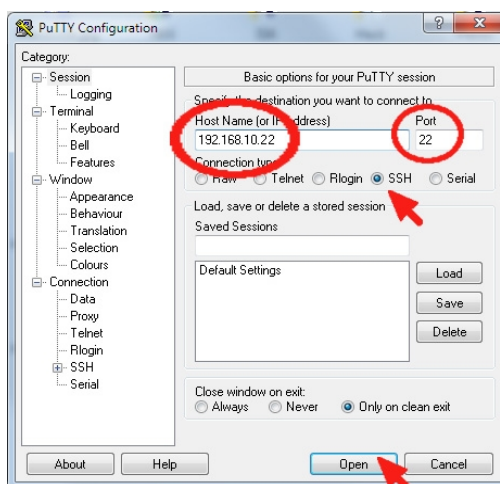
On lance Putty :

On configure

l'adresse IP (192.168.10.22)  
le port (22)  
et on n'oublie pas de cocher SSH

puis on valide cliquant sur le bouton « Open »

L'utilisateur par défaut est **pi**  
Le mot de passe par défaut est **raspberry**



### Partie commune Ssh

Le logiciel Ssh est *sécurisé*, si vous voulez avoir une communication vous devrez accepter la clé proposée. Dans la suite des TPA et du cours nous aurons l'occasion de revenir sur cette action non-anodine.

Comme la liaison est *chiffrée* (sécurisée) nous pouvons modifier le mot de passe (**raspberry**). Pourquoi modifier le mot de passe ? Lorsque vous serez en TP, dans un module de réseau ou autre, toute personne connaissant votre adresse IP (elle est donnée sur le wifi) pourra se connecter **en parallèle** à vous sur votre Raspberry Pi et y apporter toutes modifications même celles que vous ne voulez pas. Modifier votre mot de passe permet d'éviter cette connection indésirable.

**ATTENTION : tout étudiant qui entrera sur un Raspberry Pi sans l'autorisation de son propriétaire commettra une faute grave.**

Procédure de changement de mot de passerelle :

Saisir la commande **passwd** puis appuyer sur Entrée  
Vous avez le message « **Changing password for pi.** »

A l'invite **Current password:**

Entrez le mot de passe actuel **raspberry** >> il n'y a pas de caractère affiché c'est normal <<  
Puis appuyer sur Entrée

A l'invite **New password:** entrez votre nouveau mot de passe  
Puis **Retype new password:** recommencer votre saisie

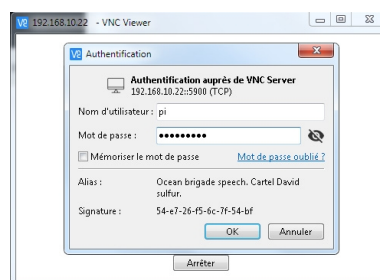
>> N'oubliez pas ce mot de passe "

Le logiciel Sshd (**d** pour *daemon* ou service en français) est un logiciel qui fonctionne tout le temps, on se connecte à lui et à la machine qui l'héberge avec le client Ssh.  
On privilégie ce type de connexion quand elle est présente à cause de sa sécurité de connexion. Une connexion CLI (terminal) au Raspberry Pi se fera le plus souvent possible au travers de Ssh.

#### — Communication graphique VNC (Virtual Network Computing) —

Aller sur le site web : <https://www.realvnc.com/fr/connect/download/viewer/>  
Choisissez le client (viewer VNC) selon votre machine (Windows, Linux ou Mac). Vous pouvez remarquer qu'il existe des versions pour natels mais ce sera votre expérimentation personnelle.  
Télécharger et installer le client VNC.

Lancer le client VNC, puis saisir le mot de passe pour la connexion (sécurisée 'normalement' mais vous pouvez lire les déboires de VNC en cherchant sur Google « crack vnc »)



J'en profite pour rappeler que tester un crack VNC n'est pas légal sur la machine de quelqu'un d'autre, nous faisons du éthical hacking. En revanche **tester sur votre matériel** (votre maquette) est un moyen d'apprentissage. Il faut arriver à mettre en œuvre cette maquette, mettre en place le POC (*Proof Of Concept*, le logiciel qui prouve le passage de la vulnérabilité) et réussir l'essai. C'est très formateur et rien n'est jamais gagné d'avance...

Si vous avez fait le TPA vous devriez avoir validé les options Telnet, Ssh et Vnc dans p1.

Utiliser votre navigateur web pour vous connecter au Raspberry Pi  
Saisir dans la barre d'adresse l'ip du Raspberry Pi.

<http://192.168.10.22>

Cette action devrait valider la coche Http.

Le client est le navigateur, le serveur installé est Nginx.



Un autre serveur fonctionne sur le Raspberry Pi pour ce TPA, c'est Node-Red.

Toujours dans votre navigateur saisir l'adresse : <http://192.168.10.22:1880>

Vous entrez dans le serveur Node-Red (ce qui valide la coche Node-Red)

Si vous testez l'url <http://192.168.10.22:80> on retombe dans le serveur web Nginx et le 80 à disparu. C'est normal un navigateur travaille sur le port 80 par défaut mais on peut lui en préciser un autre au moyen des deux points suivis du numéro du port « :1880 ».

Si vous testez dans votre navigateur les ports 22 (du ssh), 23 (du telnet), 5900 (du vnc) il n'y aura pas de réponse car le navigateur n'est pas un client pour sshd, telnetd ou vnc-server.



Il ne vous reste plus qu'à « Envoyer » votre participation. Le TPA est sans note mais votre envoi nous encourage sur votre participation donc sur la faisabilité du TPA.

**Il reste un moyen de parler aux périphériques style routeurs ou switches (difficile sur Rpi sauf à ajouter une carte électronique), à votre avis lequel est ce ?**  
(la réponse sera donnée au prochain TPA)

Au plaisir de vous retrouver pour le prochain TPA la semaine prochaine...



## ► ANNEXE :

### — Changement d'initiales et/ou de durée d'affichage de l'adresse IP —

Il faut éteindre le Raspberry Pi, enlever la carte SD, la placer dans un support lisible par votre PC



Ouvrez le répertoire `/boot` et ouvrez le fichier avec l'éditeur de texte notepad.exe.

Remplacer vos initiales et/ou modifier la durée d'affichage puis sauvegarder le fichier.  
Éjecter votre carte SD.

Replacer la carte dans le Raspberry Pi et redémarrer ... (photo à la fin de l'Annexe)

### — Refaire sa carte SD —

Télécharger l'image de l'OS à partir de l'url suivante : <https://www.idreso.org/TPA/TPA-Rpi-HEG.img>

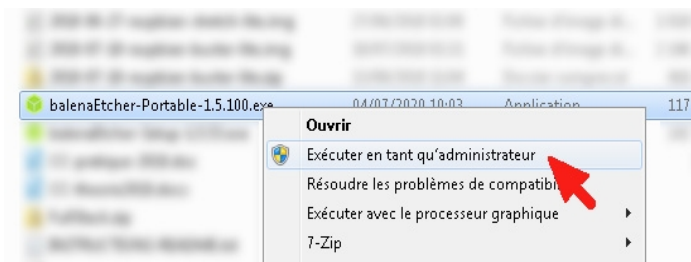
Téléchargez le logiciel balenaEtcher depuis l'url <https://www.balena.io/etcher/> en fonction de votre OS d'ordinateur (Windows-Mac-Linux).

C'est un logiciel libre open source, si vous voulez le recompiler utiliser le code source à <https://github.com/balena-io/etcher>, le plus simple est de télécharger et d'installer l'application.

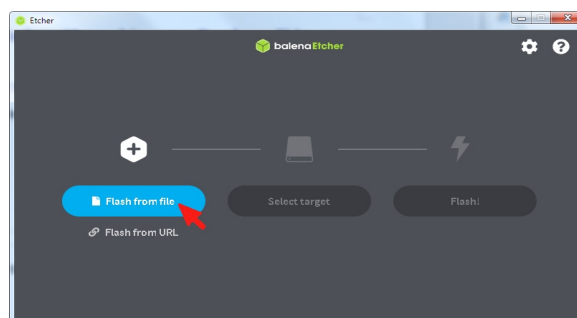
Lancez l'application balenaEtcher

L'application est à démarrer en tant qu'administrateur :

Clic droit sur l'application  
balenaEtcher puis



Choisir l'emplacement de la source  
fichier image du système (\*.img)





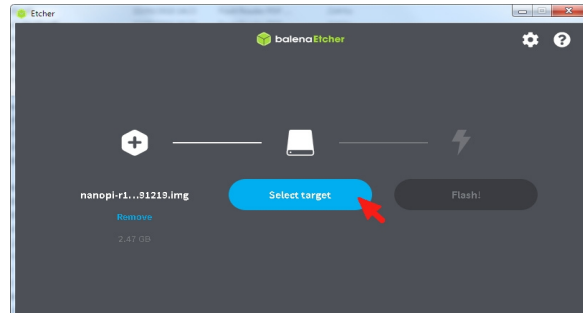
Placer la carte SD l'adaptateur, le tout dans dans le lecteur de carte de l'ordinateur.



Choisir l'emplacement du répertoire de destination.

**ATTENTION A BIEN CHOISIR LA LETTRE DU BON DISQUE EXTERNE**

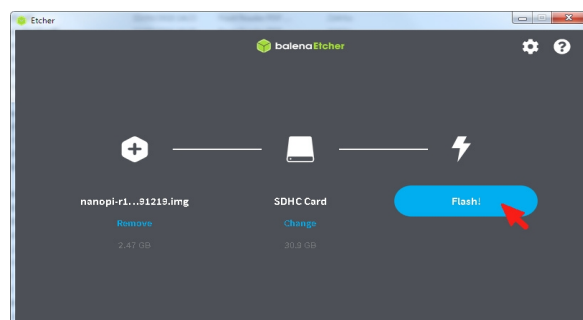
**IL Y A EFFACEMENT DU SUPPORT DE DESTINATION**



Lancer le transfert du fichier.

...

Puis attendre le message de fin d'écriture



Allez chercher dans le dossier /boot de la carte SD le fichier prop.txt (s'il le faut enlever le support de la carte et réinsérer le).

Utiliser le paragraphe précédent pour mettre vos initiales à la place de celles présentes.

Attention au sens de la carte SD, bien la glisser dans son connecteur (nul besoin de démonter le boîtier l'image n'est là que pour vous montrer le connecteur de la carte SD)

