

A qui peut-on parler sur un réseau

Ping, traceroute, scan de réseau, nmap

► BUT :

Manipuler des adresses IP, savoir qui est sur notre réseau, quelle est la limite de notre réseau privé. Savoir par où passent nos conversations et combien de temps elles mettent pour arriver au destinataire. (C'est un problème connu des utilisateurs de jeux vidéo, une latence trop grande peut vous coûter la vie, immatérielle certes, mais vous avez perdu la partie...)

► GLOSSAIRE :

Ping : C'est une petite application qui utilisant le protocole ICMP. Elle permet d'appeler quelqu'un et d'attendre sa réponse. En fonction de sa réponse on peut savoir si nous avons fait une erreur de branchement ou si le destinataire est absent.

Traceroute : Logiciel qui utilise aussi le protocole TCP qui permet de savoir par quels routeurs passent nos conversations internet.

scan : L'action de *scanner* (interdite en dehors de son réseau personnel) est le fait d'écouter et/ou de provoquer des réactions de périphériques afin de les faire sortir du bois (de les voir informatiquement).

nmap : Créé par Fyodor (Gordon Lyon) une star du Hacking (<https://insecure.org/fyodor/>) en 1998 et sans cesse amélioré. Cette application va parcourir votre réseau, l'interroger, et peut vous fournir les hôtes actifs sur votre réseau mais aussi les services qui fonctionnent sur ces machines, les versions de de ces services ainsi qu'éventuellement la nature du système d'exploitation de l'hôte (Rq : Win10 est vu comme XP et ça ne fonctionne pas pour un natel).

latence : temps de transmission de vos informations sur le réseau, en général on mesure en millisecondes (ms) cela paraît rapide mais un processeur moderne fait 150 millions d'instructions en 1ms (Core I7 150 000 MIPS - <https://fr.wikipedia.org/wiki/Microprocesseur>).

► La réponse à la question :

A l'école vous vous connectez, le plus souvent, au routeurs et aux switches avec le câble bleu clair (câble série). C'est le moyen le plus simple (à programmer) de se connecter sur un appareil informatique. Ce type de connexion n'est valable qu'en laboratoire, dès que le périphérique est chez le client de l'entreprise on ne peut le joindre qu'en Ssh.



► C'EST PARTI :

— Réponse de votre machine (PC fixe ou portable) —

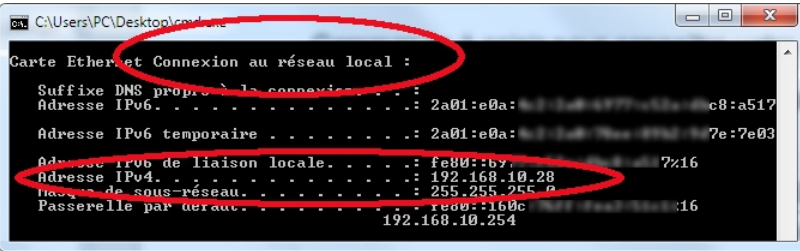
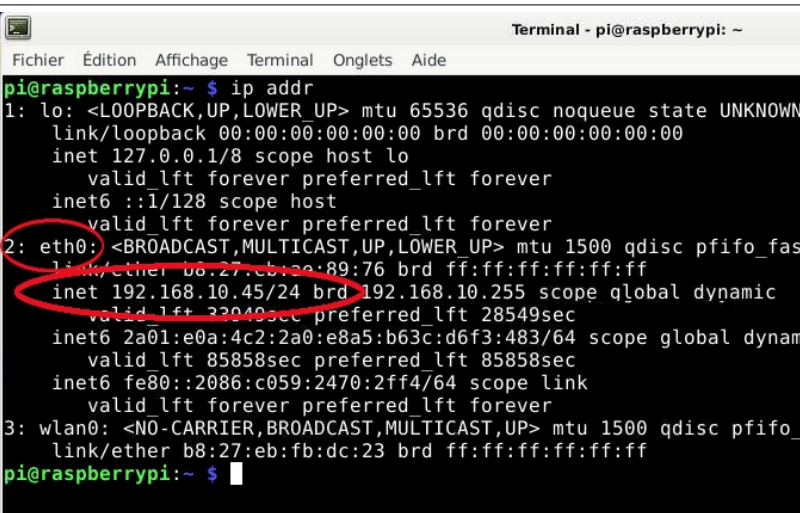
Le Raspberry Pi est sur votre box, votre ordinateur est sur le réseau filaire ou bien en Wifi peu importe.

Sur votre ordinateur connectez vous en Ssh (ou en VNC) sur le Raspberry Pi, mais nous n'aurons pas besoin du graphique. Ouvrez aussi une fenêtre de terminal (cmd.exe, powershell pour Windows ou ⌘ N pour Mac).

Pour pouvoir aller sur internet vous avez besoin d'une adresse unique sur votre réseau privé (chez vous) sinon l'une des personnes de votre domicile pourra recevoir des messages qui vous seraient destinés.

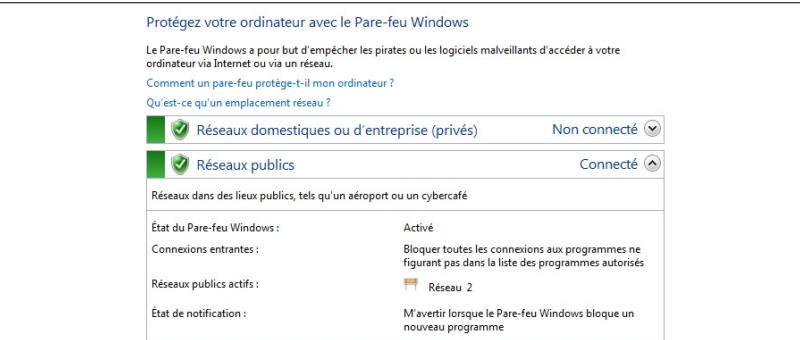
Pour être sûr que cette adresse est unique on utilise un serveur (encore un) DHCPd qui a le rôle de vous donner un adresse IP unique et de la mémoriser pour une autre fois.

Commande à saisir pour connaître votre adresse IP :

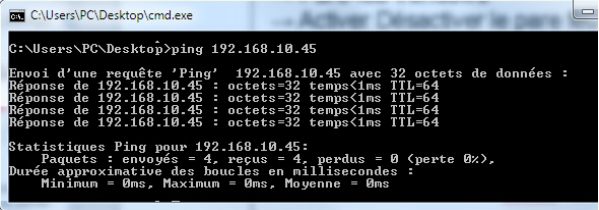
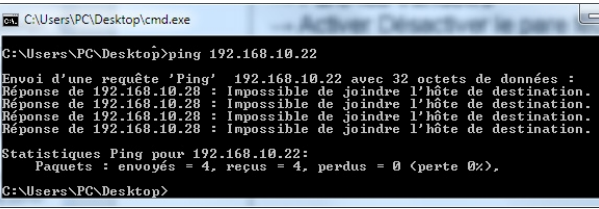
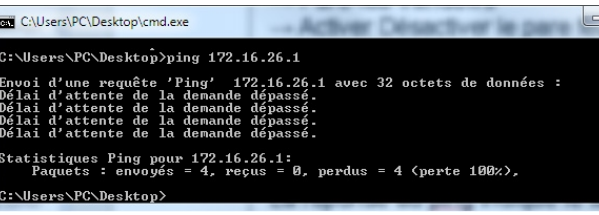
<p>Windows :</p> <p style="text-align: center;">ipconfig</p>	
<p>Mac, Raspberry Pi ou Linux :</p> <p style="text-align: center;">ifconfig</p> <p style="text-align: center;">ou</p> <p style="text-align: center;">ip addr</p>	

Dans tout les cas on utilise la commande ping adresse_IP pour demander au périphérique d'adresse_IP s'il est présent. Si on est sûr qu'il est vivant, il devrait vous répondre.

Un cas particulier se présente si le firewall d'un des deux (ou les deux) bloque les pings. Dans ce cas il faut enlever temporairement le firewall.

<p>Win7ou Win10 :</p> <p>→ panneau de configuration → Pare-feu Windows → Activer Désactiver le pare feu (à gauche)</p> <p style="text-align: center;">Tout doit être au vert</p>	
<p>Raspberry Pi :</p> <p>Il n'y a pas de firewall en fonctionnement. S'il y avait iptables (firewall classique pour Raspberry Pi ou Linux) faire la commande</p> <p style="text-align: center;">sudo service iptables stop</p>	

Différentes réponses, essayez les valeurs d'exemples

<p>La réponse au ping indique le temps de latence, il est très faible dans son propre réseau</p>	
<p>La réponse au ping si l'hôte n'existe pas ou si le câble ethernet est débranché</p>	
<p>La réponse au ping si le réseau n'existe pas</p>	

— Qui est sur le réseau ? —

Sur le Raspberry Pi on va lancer la commande nmap avec la détermination de services afin de scanner notre réseau.

Si vous voulez-vous amuser connectez votre natel au wifi (si ce n'est pas déjà fait).

Sans préjuger du résultat vous devriez au moins avoir 4 périphériques (votre PC, le Raspberry Pi, le natel, votre box) mais on peut aussi trouver d'autres PC, la console de jeux, la box TV, une imprimante réseau, ...

nmap -sP 192.168.10.0/24 pour le réseau d'appartenance (voir ifconfig)

Une fois ce test effectué, vous pouvez tester la reconnaissance de l'OS par nmap pour une adresse IP particulière car cette reconnaissance est un peu longue

sudo nmap -O 192.168.10.45

Si on fait exécuter nmap avec des droits d'administrateur (sudo) on bénéficie de tests complémentaires (ceux qui demandent d'être exécutés en « root ». Un aperçu des différents paramètres possible même si je vous encourage à lire le manuel (man nmap ou « paramètres nmap » sur google).

-sP (scan Ping), -PT (Ping Tcp), -PU (Port Udp), -sU (scan ports Udp), -sS (scan SYN), -O (OS), -sV (service Verbose liste des services), ...

Vous pouvez remarquer que les adresses IP de votre réseau commencent toutes de la même façon. De plus vous n'en avez pas besoin de millier. Pour limiter le nombre d'adresses de votre réseau on utilise la notion de masque (255.255.255.0 ou /24) qui indique le nombre de machines pour votre réseau. Vous verrez en cours la manière de calculer ce nombre de machines possibles en fonction de ce masque.

Le *masque* permet par exemple à nmap de scanner une certaine plage on commence à l'adresse passée en paramètre et de terminer à une adresse donnée (sinon il peut aller très loin en ajoutant 1 à chaque boucle du test). Vous avez vu (ou verrez) en cours que les adresses que vous trouvez chez vous son des adresses IP privées (c'est normal c'est chez vous).

— Par où passe-t-on pour joindre une adresse IP de destination et où se trouve-t-elle? —

On va déjà localiser l'IP de destination (où se trouve géographiquement 209.212.98.29 ?)

On recherche la localisation en utilisant les serveurs webs suivants (ou en cherchant sur google des « site de géolocalisation d'IP »)

<https://gsuite.tools/ip-location>

<https://fr.geopipview.com/>

Chercher la localisation des adresse IP suivantes :

209.212.98.29
154.54.61.21

129.232.249.216
185.148.112.9

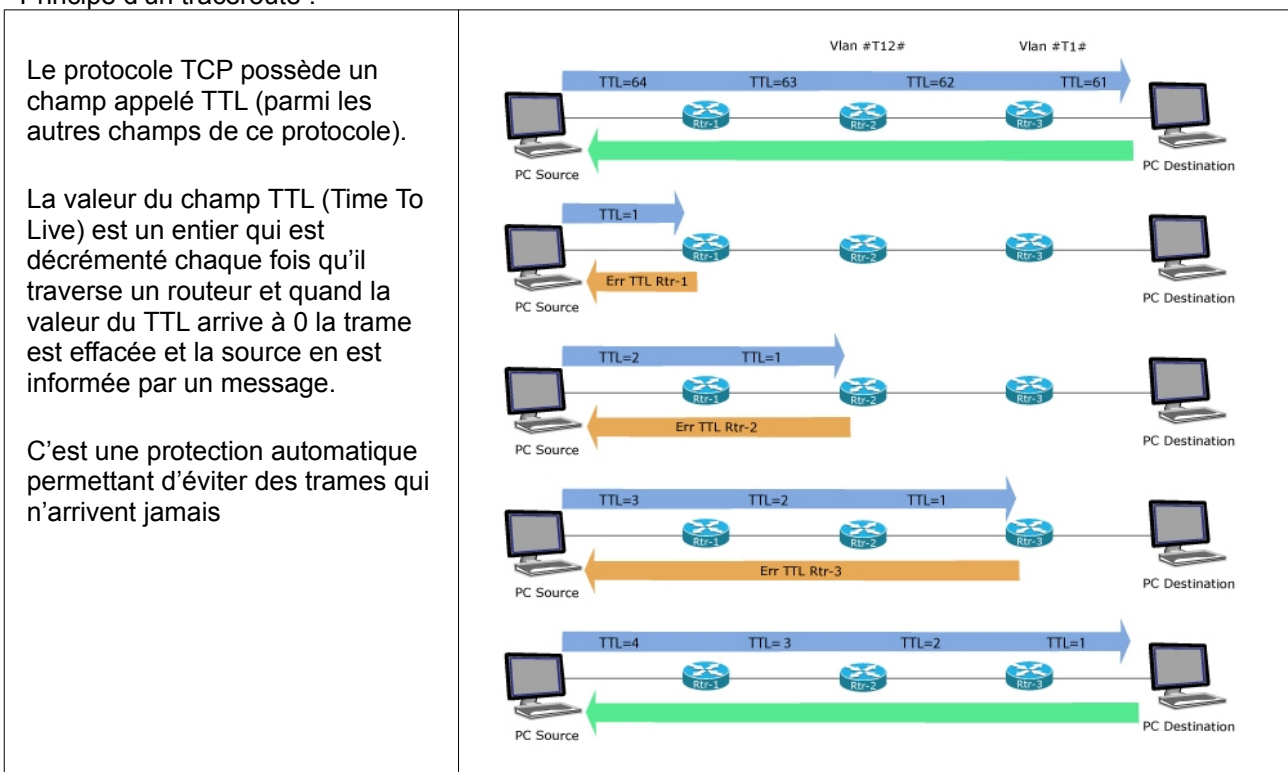
105.16.9.89
65.155.248.179

149.29.1.218

Par où passe-t-on pour aller là-bas ?

On va rechercher tous les routeurs traversés entre l'adresse IP source et la destination. On utilise l'application traceroute (Linux/Mac) ou tracert (Windows) selon le système. traceroute apparaît plus rapide que tracert.

Principe d'un traceroute :



Faites un traceroute sur les adresses IP suivantes, noter les temps (cumulés ou pas) au cours du voyage. Utilisez l'url suivante pour avoir un trace route graphique : <https://gsuite.tools/traceroute>, le plus souvent le traceroute ne fonctionne que dans un terminal (Linux, Mac ou Windows).

209.212.98.29
154.54.61.21
185.148.112.9

129.232.249.216
149.29.1.218

105.16.9.89
65.155.248.179

Comment expliquer la différence de latence entre certaines adresses qui vont à l'extrémité de l'Afrique par rapport à la majorité d'adresses situées aux États-Unis ? (la réponse sera donnée au prochain TPA)

— Petit complément pour clôturer ce TPA —

On a appris, depuis un terminal, à charger un fichier à partir d'une adresse web. Depuis un terminal du Raspberry Pi exécuter la commande suivante : `wget https://www.idreso.org/TPA/p2`
Il faut rendre le fichier exécutable : `chmod +x ./p2`

▶  :

Afin de nous donner un petit signe d'approbation de ce TPA, vous pouvez vous signaler en exécutant ce programme (`./p2`).

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