DÉMYSTIFICATION DE L'INTERNET

TP GYMNASIENS

EPFL Section Systèmes de Communication
Responsable: Jean-Yves Le Boudec

Mars 2005

But de ce TP

Le but de ce travail pratique (TP) est d'apprendre à utiliser quelques outils, disponibles sous tous les systèmes Windows, qui permettent d'explorer l'Internet.

1 Découvrir l'Internet

1.1 Démarrer

Appuyez simultanément sur les touches `Ctrl`, `Alt` et `Delete`. Si vous utilisez la machine numero 8 (le numero est inscrit sur l'ecran) alors votre login est `user8`. Le mot de passe est le même pour toutes les machines: `motdepasse`.

1.2 Utiliser des Commandes sous Windows

Les outils utilisés dans cette partie sont accessibles en tapant des commandes dans une fenêtre appelée "Command Prompt". Ouvrez cette fenêtre par `Start`→ `All Programs`→ `Accessories`→ `Command Prompt`. Pour taper une commande, vous entrez du texte et terminez par la touche `ENTER`. Ce faisant, vous donnez un ordre à l'ordinateur, qui l'exécute.

Vous pouvez utiliser les flèches vers la gauche ou la droite, avec les deux touches d'effacement, pour réparer des erreurs de frappe. La flèche vers le haut ou le bas permet de rappeler des commandes déjà entrées.

Quand vous avez tapé la touche ENTER, la commande est lancée et ne peut pas être modifiée. Par contre, on peut la stopper si nécessaire en entrant CTRL-c.

Entrer la commande `ver`. Que produit-elle ?

En général, on peut obtenir le mode d'emploi d'une commande en tapant le nom de la commande suivie d'un espace puis de `/?`

La commande `color` permet de changer la couleur du texte et du fond d'écran à l'intérieur de la fenêtre de commande que vous utilisez. Lisez le mode d'emploi de cette commande.

Changez les couleurs pour que le texte soit jaune sur fond bleu. Revenez à la couleur de départ.

1.3 ping

La commande `ping` envoie un message de test à une machine. La plupart des machines y répondent. Cela permet de tester si une machine (serveur, routeur) est atteignable. C'est notre premier outil de diagnostic.

Tapez la commande `ping 128.178.151.1`. Qu'obtenez vous ? Quel est le temps d'aller et retour entre votre PC et la machine répondant à l'adresse 128.178.151.1 ?

Testez si les machines suivantes sont atteignables depuis votre PC: `lcawww.epfl.ch`, `www.zurich.ibm.com`, `www.uchile.cl`, `oceano.uem.mz`, `www.nzherald.co.nz`, `www.newzealand.com`.

On peut modifier le comportement d'une commande en donnant une ou plusieurs options. Par exemple, la commande `ping -n 10 128.178.151.1` envoie 10 messages de test au lieu de 3 par défaut. (Terminologie: on dit que `128.178.151.1` est l'argument de la commande, `-n 10` est l'option.)

Les messages sont composés d'une suite de caractères, que l'on nomme `octet` en jargon informatique (voir section suivante pour une définition plus rigoureuse du terme `octet`). L'option `-l 10` fait que le message de test envoyé par `ping` contient 10 octets de données au lieu de 32 par défaut. Comparez le temps d'aller et retour vers la machine `www.newzealand.com` obtenu avec les longueurs de message suivantes: 0,100,1000,5000,10000.

(Aide: pour éviter de passer trop de temps à taper des commandes, utilisez la flèche vers le haut qui permet de rappeler la dernière commande, puis éditez la avec les flèches gauche/droite et les touches d'effacement)

Le temps d'aller retour que vous avez trouvé est variable; il dépend de la charge sur le réseau. Avec un message de 0 octet, le temps n'est pas 0ms. Cela est dû à plusieurs faits:

- Même pour un message de test vide, le paquet créé sur le réseau mesure environ une cinquantaine d'octets (Il contient une en-tête avec par exemple des informations sur les adresses source et destination, un code qui permet de savoir que c'est un message ping et pas un message pour un serveur web, etc.)
- Le temps d'aller et retour est égal à la somme de trois composantes:
    1. le temps de transmission: c'est le temps qu'il faut pour enfiler les bits les uns derrière les autres. Il dépend du *débit* des lignes (communément appelé "vitesse"). Sur une ligne ADSL à 1 Mb/s, on transmet 10^6 bits en une seconde, donc le temps de transmission d'1 bit est 10^{-6}s. Un octet est 8 bits donc pour transmettre 100 octets il faut $100 \times 8 \times 10^{-6}$s =0.8 ms.

Quel est le temps de transmission de 100 octets sur une ligne Ethernet à 100 Mb/s ?

Le temps de transmission est à multiplier par le nombre de fois qu'il faut retransmettre le paquet. Si on traverse 30 routeurs pour aller à la destination, il faut le multiplier par 30.

2. le temps de traitement dans toutes les machines du chemin. Ce temps est variable; si une machine est très chargée à un instant donné, il peut y avoir une attente longue.
3. le temps de propagation: c'est la vitesse de la lumière dans les cables du réseau. Cette vitesse de propagation est : 3.0×10^8m/s dans l'air (liaisons radios), 2.3×10^8m/s dans le cuivre (cables Ethernet) et 2.0×10^8m/s dans le verre (cables transocéaniques).

Calculer le temps de propagation aller et retour pour aller à l'autre bout de la terre. (Indication: la distance d'aller et retour est de 40'000 km $=4 \times 10^7$m. Prendre comme vitesse de propagation de la lumière $c = 2 \times 10^8$m/s).

Comparer les temps d'aller retour avec les machines `www.nzherald.co.nz` et `www.newzealand.com`. Laquelle des deux pourrait être en Nouvelle-Zélande ?

1.4 Les Adresses IP

Les machines sont identifiées par des adresses IP, comme par exemple `128.178.50.137`. C'est l'équivalent pour l'internet du numéro de téléphone. Chaque interface de communication (d'un PC, d'un serveur web, d'un routeur) possède sa propre adresse IP.

Une adresse IP est en fait un nombre entier, qui peut être écrit en machine sur 32 bits. Toutes les machines représentent les entiers en base 2; par exemple, le nombre 2159161993 se représente en base 2 par

$$10000000101100100011001010001001$$

Si on appelle $b_{31} = 1, b_{30} = 0, ..., b_3 = 1, b_2 = 0, b_1 = 0, b_0 = 1$ la suite de ces 32 bits (i.e. chiffres égaux à 0 ou 1), cela veut dire que

$$2159161993 = 2^{31}b_{31} + 2^{30}b_{30} + 2^{29}b_{29} + 2^{28}b_{28} + ... + 2^3b_3 + 2^2b_2 + 2b_1 + b_0 \quad (1)$$

Comme il n'est pas très agréable pour nous autres humains de manipuler de telles suites de bits, on utilise la convention suivante pour écrire les adresses IP. On groupe les bits par paquets de 8 (i.e. par octet, en anglais "byte", abbréviation B)

$$10000000 \qquad 10110010 \qquad 00110010 \qquad 10001001$$

et on représente chaque paquet de 8 bits par son écriture décimale habituelle. Ainsi le dernier octet 10001001 est le nombre

$$2^7 \times 1 + 2^6 \times 0 + 2^5 \times 0 + 2^4 \times 0 + 2^3 \times 1 + 2^2 \times 0 + 2^1 \times 0 + 2^0 \times 1 = 137$$

ce qu'on écrit

$$b10001001 = 137$$

(le symbole b – “binary” – signifie que le nombre est représenté en base 2). De la même façon on trouve

$$\begin{aligned} b10000000 &= 128 \\ b10110010 &= 178 \\ b00110010 &= 50 \\ b10001001 &= 137 \end{aligned}$$

On représente alors l'adresse IP par

$$128.178.50.137$$

qu'on appelle *notation décimale pointée* (“dotted decimal notation”). Puisque chacun des paquets de bits vaut au maximum $b11111111 = 255$, la notation décimale pointée comporte quatre nombres entiers entre 0 et 255.

La représentation 2159161993 est appelée *notation décimale*. Elle est peu utilisée, car la notation décimale pointée est plus pratique, comme nous verrons dans la section 1.6. On peut passer de la notation décimale pointée $d_3.d_2.d_1.d_0$ à la notation décimale d en utilisant la formule suivante, dérivée de l'équation (1):

$$\begin{aligned} d &= d_3 \times 2^{24} + d_2 \times 2^{16} + d_1 \times 2^8 + d_0 \times 2^0 \\ &= 16777216d_3 + 65536d_2 + 256d_1 + d_0 \end{aligned}$$

Ainsi on peut vérifier que l'adresse 128.178.50.137 vaut, en décimal:

$$2159161993 = 128 \times 16777216 + 178 \times 65536 + 50 \times 256 + 137 \quad (2)$$

Quelle est la notation décimale de 128.178.151.121 ?

Vérifiez en allant sur le site web dont l'URL est `http://www.allredroster.com/iptodec.htm`. Pour cela, ouvrez une fenêtre Internet Explorer et entrez cet URL dans le champs d'adresse.

La commande ping effectue automatiquement la conversion de la notation décimale à la notation décimale pointée. Entrez la commande `ping 2159161993` et déduisez-en la notation décimale pointée de cette adresse.

L'adresse `333.222.111.000` est-elle valide ?

1.5 nslookup

En plus des adresses IP, les machines ont des *noms de domaine* (“DNS names”; DNS = Domain Name System). Par exemple, `lcawww.epfl.ch` est le nom de domaine de la machine répondant à l'adresse `128.178.151.121`. On dit souvent simplement *nom* au lieu de *nom de domaine*.

Tapez `ping ssc.epfl.ch` et déduisez-en l'adresse IP de ce serveur

Pourquoi utilise-t-on des noms de domaine au lieu des adresses IP ? La raison est que les adresses IP sont en général associées statiquement à des machines. Si demain matin, pour une raison de maintenance, le serveur web `ssc.epfl.ch` était déplacé d'une machine à une autre, l'adresse IP changerait, mais on peut s'arranger pour que le nom reste le même. Les noms de domaine permettent d'avoir des noms permanents pour les serveurs.

Quand vous tapez `ping ssc.epfl.ch`, la première chose que fait la commande `ping` est de trouver l'adresse IP correspondante. Pour cela, elle envoie un message de résolution d'adresse à un *serveur de nom* ("Name Server"). Chaque PC est configuré avec l'adresse IP d'un serveur de nom.

Vous pouvez aussi directement accéder au serveur de nom par la commande `nslookup`

Tapez `nslookup`. La réponse vous donne le nom et l'adresse IP du serveur de nom qu'utilise votre machine. Quels sont-ils ?

La commande `nslookup` attend maintenant que vous entriez du texte. Tapez `ssc.epfl.ch`; la réponse vous donne l'adresse IP, mais aussi un autre nom. Une machine peut en effet avoir plusieurs noms. Tapez le deuxième nom et vérifiez que l'adresse IP obtenue est bien la même.

Quittez la commande `nslookup` en tapant `CTRL-c` ou `exit`

Pour contacter un serveur web, on utilise d'habitude son nom plutôt que son adresse, mais on peut tout aussi bien utiliser l'adresse IP, en notation décimale pointée ou décimale.

Ouvrez une fenêtre Internet Explorer et tapez dans le champs adresse `http:\\2159187833`. Quel serveur web avez vous atteint ?

Trouvez la notation décimale et la notation décimale pointée de l'adresse IP du serveur `www.epfl.ch`.

Entrez `http:\\` suivi des chiffres de la notation décimale trouvée; arrivez-vous sur le même serveur que `www.epfl.ch` ? Même question si vous faites suivre `http:\\` de la notation décimale pointée.

Votre PC doit connaître l'adresse IP du serveur de nom qu'il utilise. Normalement, cela se configure automatiquement lorsque votre PC démarre, à l'aide d'un serveur de configuration appelé serveur "DHCP" (Dynamic Host Configuration Protocol"). Il est possible cependant de spécifier le - ou les - serveurs à utiliser explicitement, comme c'est le cas sur les machines que vous utilisez dans le cadre de ce TP (voir ci-dessous). On peut alors modifier manuellement cette configuration:

Double-cliquez sur l'icône montrant un petit ordinateur qui communique, puis cliquez sur le bouton `Properties`. Dans le menu déroulant qui apparaît à l'écran, sélectionnez `Internet Protocol (TCP/IP)` puis cliquez sur `Properties` (Figure 1). Sélectionnez l'onglet `General`.

Normalement, la case `Obtain DNS server address automatically` doit être cochée (Figure 2) [1]

Cochez maintenant la case `Use the following DNS server addresses`. Dans le champ `Preferred DNS Server`, inscrivez une adresses IP que vous choisissez au hasard. Cliquez OK autant

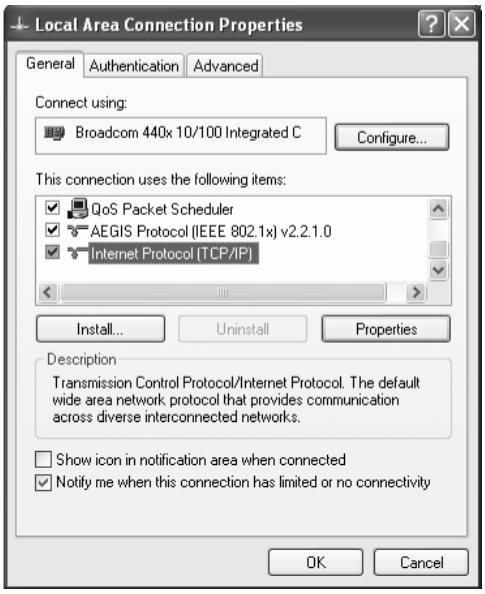

Figure 1: Sélection des propriétés du protocole TCP/IP

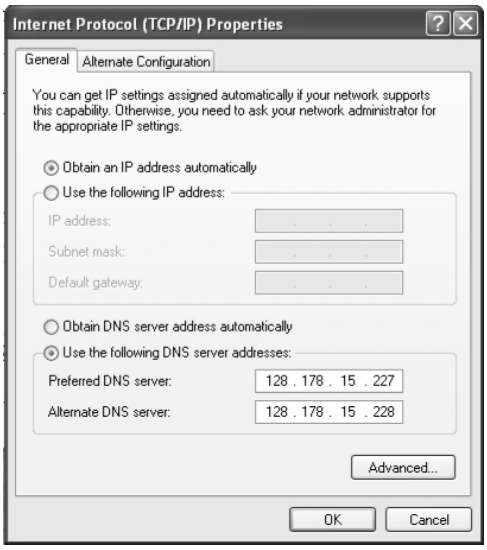

Figure 2: Configuration explicite des serveurs de nom du PC

de fois que nécessaire. Vous venez de dire à votre machine d'utiliser comme serveur de nom une adresses qui, très probablement, n'est pas celle d'un serveur de nom.

Revenez dans une fenêtre de commande et tapez `ping lcawww.epfl.ch` puis `ping 128.178.151.1` (vous pouvez interrompre une commande qui est "plantée" avec `CTRL-c`). Interprétez ce qui se passe.

Maintenant, suivez la même procédure que ci-dessus et instruisez votre PC d'utiliser DHCP pour obtenir l'adresse du serveur de nom (cochez la case `Obtain DNS server address automatically` à l'endroit adéquat). Vérifiez que tout marche comme prévu en tapant `ping lcawww.epfl.ch`.

1.6 ipconfig

La commande `ipconfig` vous permet de connaître la ou les adresses IP utilisées de votre PC.

Trouvez l'adresse IP de la machine sur laquelle vous travaillez.

Le `defaut gateway` signifie le routeur par défaut ("gateway" est un mot ancien; aujourd'hui en anglais on dit "router"). C'est l'adresse IP du routeur où sont envoyés tous les paquets pour des destinations qui ne sont pas sur le réseau dans cette salle.

Quel est l'adresse du `defaut gateway` ?

La commande `ipconfig /all` donne, (parmi de nombreuses choses) l'adresse du ou des serveurs de nom utilisé par ce PC.

Quelle est l'adresse du serveur de nom utilisé par votre PC ? Est-ce le même que celui qui est apparu par la commande `nslookup` ?

1.7 tracert

La commande `tracert` permet de trouver la liste de tous les routeurs entre ce PC et une destination. Elle permet de diagnostiquer un problème réseau.

Tapez `tracert 128.178.50.137` et observez les réponses. Combien de routeurs y a-t-il entre votre PC et cette destination ? Le premier routeur est-il le même que le routeur par défaut que vous avez découvert avec `ipconfig` ?

Combien y a-t-il de routeurs entre votre PC et les machines suivantes: `lcawww.epfl.ch`, `www.uchile.cl`, `oceano.uem.mz` ?

SWITCH est le réseau qui relie entre elles et à l'extérieur toutes les hautes écoles de Suisse. Combien y a-t-il de routeurs entre votre PC et SWITCH ?

Combien y a-t-il de routeurs entre votre PC et `www.zurich.ibm.com` ?

Observez les chemins pour `www.nzherald.co.nz` et `www.newzealand.com`: Pouvez vous confirmer lequel des deux n'est certainement pas en Nouvelle Zélande ?

Le logiciel VisualRoute vous permet de visualiser les résultats obtenus par `tracert`. Pour l'utiliser, cliquez sur son icône sur votre écran.

Afin de afficher visuellement la route menant de votre machine à `www.nzherald.co.nz`, entrez ce nom dans la fenêtre en haut à gauche et tapez la touche ENTER. La liste des routeurs utilisés sur le chemin est affichée au bas de la fenêtre. Vous pouvez aussi suivre l'itinéraire emprunté par le paquet sur la carte du monde (agrandissez la carte en cliquant sur un point de celle-ci avec le bouton gauche de la souris, revenez en arrière en utilisant le bouton droit). La route affichée est-elle la même que celle trouvée avec la commande `tracert`?

2 Un étrange message

L'internet aujourd'hui est le théâtre de toutes sortes de manipulations. Certaines utilisent les mécanismes de noms et d'adresses que nous avons introduits dans la section précédente.

L'exemple décrit ci-dessous est réel. Il utilise le scénario suivant: Utilisateur occasionnel du site de ventes aux enchères eBay (`www.ebay.ch`), vous avez reçu un message email qui vous invite à aller sur un site web afin de mettre à jour vos informations personnelles (ouvrez ce message sur votre ordinateur en cliquant sur l'icône intitulée `eBayMsg.html`, puis cliquez sur le lien). Comme vous pouvez le constater, vous êtes invité à entrer votre numéro de carte de crédit pour vérifier votre identité, et même de donner le code secret pour bancomat ("Credit Card ATM Pin"). Ce message vous paraît-il crédible ?

En utilisant les outils présentés dans la section précédente (ping, nslookup, tracert), localisez géographiquement le serveur auquel on se connecte quand on clique sur le lien contenu dans le message email. Comparez avec le résultat obtenu pour `www.ebay.com`. Qu'en déduisez-vous?

3 Et Maintenant...

Bravo, vous avez terminé ce TP ! Demandez un corrigé et comparez vos réponses avec notre solution.

Donnez-nous aussi votre feedback en remplissant le formulaire anonyme.

S'il vous reste au moins 30 minutes avant la fin de la séance, vous pouvez demander à faire le deuxième TP.