

Séance 2 : Réseaux I - Outils de communication Web

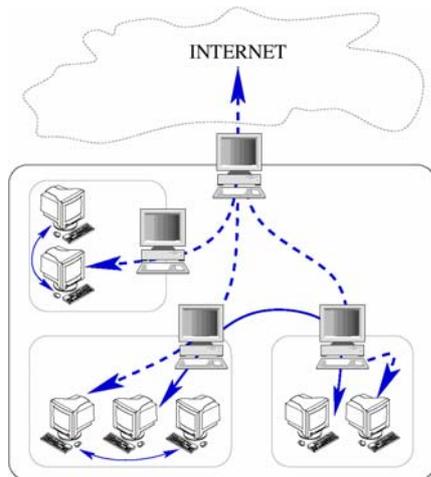
Remarques préliminaires

Les problèmes rencontrés et les oublis constatés dans ce support sont à signaler à clot@univ-lyon1.fr

L'objectif de ce support est de présenter les concepts de base nécessaires à une bonne compréhension de l'insertion d'une machine dans un réseau de machines reliées entre elles via les technologies usuelles du réseau. L'accent sera également mis sur les outils de navigation sur le Web.

Il est important de lire complètement le texte d'un item avant de tenter d'atteindre l'objectif visé. Il est fréquent que des indications soient fournies dans l'ensemble de phrases constituant l'item.

Aperçu global



Un réseau de machines est un ensemble de machines reliées entre elles. Internet peut être vu comme le réseau des réseaux, interconnectant les réseaux entre eux.

L'ensemble des machines est structuré en groupes et sous-groupes appelés réseaux et sous-réseaux. Au sein d'un sous-réseau, toutes les machines peuvent communiquer entre elles directement. En revanche, d'un (sous-)réseau à un autre, la communication est relayée par certaines machines jouant un rôle particulier : à cheval sur plusieurs (sous-)réseaux, elles permettent de transmettre l'information entre les (sous-)réseaux et sont capables de construire pas à pas le chemin emprunté par les données échangées.

Modèles en couches: OSI et TCP/IP

Les réflexions conduites dans le cadre de la mise au point de réseaux de machines communicantes ont conduit à la formalisation d'un modèle organisé en couches. Chaque couche rend un service et ne peut communiquer qu'avec les couches adjacentes. La façon dont elle rend le service n'est pas connue. L'exemple suivant illustre le principe de ce type de modèle:

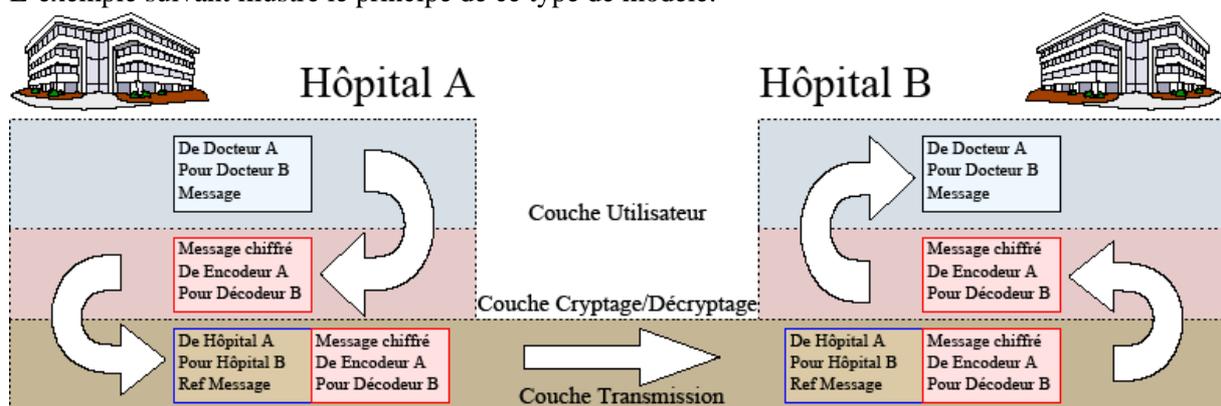


Figure 6 - exemple de communication par couches

Le modèle théorique faisant office de norme est le modèle OSI (Open Systems Interconnection). Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol), conçu parallèlement à OSI, est le modèle pratique déployé mondialement comme support pour les communications au sein des réseaux. Il comporte quelques imperfections par rapport à OSI...

La figure 7 présente une couche basse correspondant au support sur lequel les communications sont réalisées. Les couches supérieures sont remplies par divers protocoles de la famille de protocoles de TCP-IP. Un protocole particulier rend un service qui peut reposer lui-même sur les services rendus par les couches inférieures. C'est ce qui détermine sa position dans la pile.

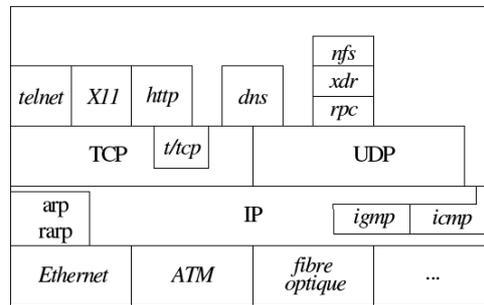


Figure 7 - Quelques protocoles de la pile TCP-IP

Détails du modèles TCP/IP

Correspondance entre adressages logique et matériel :

Chaque interface réseau dispose d'une adresse matérielle. Une interface sait que des informations lui sont destinées lorsque ces informations contiennent son adresse matérielle. Elle transmet alors au système les informations reçues. Les autres informations ne sont pas traitées. Cet adressage physique sert à identifier l'interface, mais ne permet pas d'organiser les machines en réseaux. L'adressage logique permet, lui, de définir cette organisation. Le système permet d'associer à une interface une adresse logique afin de définir sa place dans l'organisation des machines en réseaux.

Le protocole ARP (Address Resolution Protocol) est utilisé pour connaître l'adresse matérielle associée à une adresse IP (l'adresse logique). Il permet à un hôte de questionner l'ensemble des machines du sous-réseau sur l'adresse matérielle du possesseur d'une adresse IP. Ce possesseur répond en indiquant son adresse matérielle.

Adressage IP – forme, structuration, adresses particulières :

Une adresse IP (IPv4) est un nombre défini sur 32 bits, noté sous la forme d'un quadruplet d'entiers dont les valeurs sont comprises entre 0 et 255(2⁸-1) en notation décimale. La notation binaire est rarement utilisée au profit de l'écriture décimale, mais elle est utile pour la compréhension des opérations de masquage dont les adresses sont l'objet.

Considérons par exemple l'adresse 134.214.100.141. Le dernier octet, 141, s'écrit 10001101 en notation binaire. Les passages entre les deux notations sont illustrés ci-après:

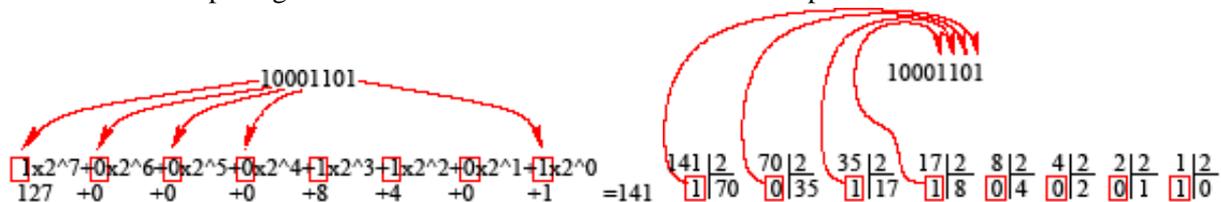


Figure 8 - passages entre les notations binaire et décimale

Une adresse IP est composée d'une partie correspondant à l'adresse du réseau et du restant servant à identifier l'hôte dans ce réseau. Il existe différentes classes de réseaux, ces classes correspondant au découpage suivant :

Classe A : 1^{er} bit du 1^{er} octet nul – le 1^{er} octet est l'adresse du réseau et les 3 octets suivants sont l'adresse de l'hôte dans ce réseau

Classe B : les 1^{ers} bits du 1^{er} octet sont 10 – les deux premiers octets forment l'adresse du réseau de classe B. Le reste sert à identifier l'hôte dans ce réseau.

Classe C : les 1^{ers} bits du 1^{er} octet sont 110 – les trois premiers octets forment l'adresse du réseau de classe C. Le reste sert à identifier l'hôte dans ce réseau.

? Calculez les valeurs possibles du **premier octet** pour les adresses de classe A, puis B et C.

Certaines adresses ne servent pas à désigner des hôtes :

- Lorsque la partie réservée à l'identification de l'hôte ne comporte que des zéros, on dit que l'adresse est l'adresse du réseau. Ainsi, 10 et 10.0.0.0 désignent le même réseau.
- Si ces mêmes bits sont positionnés à 1, on obtient l'adresse de diffusion (broadcast) sur le réseau.

Certaines adresses sont particulières:

- Les adresses du réseau 127 sont des adresses désignant la « boucle locale ».
- Les réseaux d'adresses 10, 172.16 à 172.31, et 192.168.0 à 192.168.255 forment des réseaux privés d'adresses, inaccessibles depuis l'internet et donc réutilisables à volonté.

? Déterminez la **notation binaire** pour l'adresse 134.214.102.141.

? A quelle **classe** appartient cette adresse ?

Résolution de noms

Un des premiers services rencontrés dans l'usage du Web est la résolution de noms. Un serveur de nom (serveur DNS) est une machine qui est chargée d'établir la correspondance entre un nom (www.univ-lyon1.fr ou www.google.fr) et une (ou plusieurs) adresse IP. L'émission de paquets à destination d'un hôte nécessite la connaissance de son adresse IP. Lorsqu'une machine ne connaît que le nom de l'hôte, elle sollicite un serveur de nom qui, en réponse, lui fournit une adresse IP correspondant au nom. Leur échange est défini par le protocole DNS (Domain Name System).

Ports

L'usage des adresses IP permet d'identifier les hôtes aux extrémités d'un canal de communication. Mais entre deux hôtes, plusieurs canaux de communication peuvent coexister. Le concept de port permet de démultiplier les possibilités d'adressage en permettant l'identification de nombreux canaux de communication au niveau d'un hôte. Un numéro de port est un entier codé sur 16 bits (valeurs comprises entre 0 et 65535 ($2^{16}-1$)). Ainsi, toute communication TCP ou UDP (User Datagram Protocol) fait intervenir une paire d'adresses IP et une paire de numéros de ports. Il est classique d'associer certains numéros à certains services: 22~ssh, 25~smtp, 80~web.

Masque de sous-réseaux

Une adresse IP permet d'identifier un réseau et l'adresse de l'hôte dans ce réseau. Le fort développement des réseaux a rendu ce découpage inadapté et insuffisant pour faire face à la demande. Afin de rendre ce système plus souple, un niveau de découpage a été ajouté avec le concept de sous-réseau : chaque réseau peut être organisé en sous-réseaux, le découpage étant défini par un « masque de réseau ». Ce masque a la forme d'une adresse IP dont les x premiers bits sont positionnés à 1. Le masque 255.255.252.0 (11111111.11111111.11111100.00000000) se note aussi 22 car ses 22 bits de poids forts sont à 1.

Chaque hôte associe un masque à son adresse IP, ce qui lui permet de déterminer les hôtes avec lesquels il partage le sous-réseau. Pour cela, il réalise un ET logique bit à bit. Supposons que l'adresse

134.214.102.141 est associée au masque 255.255.252.0. L'adresse du sous-réseau s'obtient en réalisant un ET logique avec l'adresse IP de l'hôte et son masque:

$$\begin{array}{r} 10000110.11010110.01100110.10001101 \\ 11111111.11111111.11111100.00000000 \\ \hline 10000110.11010110.01100100.00000000 \end{array} \text{ ET , i.e. } 134.214.100.0$$

L'adresse de broadcast d'un sous-réseau s'obtient en positionnant à 1 les bits servant à identifier l'hôte dans le sous-réseau. Elle s'obtient en prenant le complémentaire du masque et en réalisant un OU logique bit à bit avec l'adresse IP:

$$\begin{array}{r} 10000110.11010110.01100110.10001101 \\ 00000000.00000000.00000011.11111111 \\ \hline 10000110.11010110.01100111.11111111 \end{array} \text{ OU , i.e. } 134.214.143.255$$

- ? Considérez l'adresse 134.214.91.133 associée au **masque** 22. A quelle classe d'adresse appartient cette adresse ? Déterminez l'adresse du réseau auquel appartient cette adresse.
- ? D'après le masque associé, à quel **sous-réseau** appartient cette adresse? Déterminez l'adresse de **broadcast** sur ce sous-réseau.
- ? Avec ce masque, combien de **bits** ont été ajoutés (à ceux utilisés pour identifier le réseau) pour identifier le sous-réseau ? Combien de sous-réseaux cela permet-il de définir sur ce réseau?

Routage

Le routage est le mécanisme qui gère le cheminement des informations échangées dans le réseau. Chaque hôte dispose d'une « table de routage » qui lui permet de choisir le prochain hôte vers lequel envoyer directement les données en fonction de l'adresse IP de destination: lorsque des paquets sont à destination d'un hôte situé sur le même sous-réseau, les paquets lui sont transmis directement, sans intervention d'une tierce partie, mais lorsqu'ils sont à destination d'un hôte sur un autre sous-réseau (éventuellement situé dans un autre réseau), les paquets sont transmis à un routeur (ou passerelle) qui décidera à son tour de la prochaine destination pour ces paquets, le prochain destinataire étant la cible finale ou un autre routeur. Le routage est l'affaire du protocole IP.

Exemple de communication illustrant l'ensemble des mécanismes mis en jeu

Supposons que vous souhaitiez consulter le moteur de recherche google. Dans votre navigateur, vous saisissez l'url <http://www.google.fr> . Nous supposons que vous réalisez cette opération à partir d'une machine du campus. Les étapes suivantes ont alors lieu :

Le mécanisme de résolution de nom est sollicité. Le serveur de nom (dont l'adresse IP est connue) va être interrogé. L'adresse de son sous-réseau est déterminée avec le masque et comme il n'appartient pas au même sous-réseau, les paquets vont être transmis au routeur. Si l'adresse matérielle du routeur n'est pas connue, une requête ARP sera émise afin d'obtenir en réponse l'adresse matérielle du routeur. Une fois cette adresse obtenue, la requête DNS peut être émise avec l'adresse matérielle du routeur comme destination et l'adresse IP du DNS en destination.

Une fois une adresse IP de google obtenue, l'adresse est masquée avec le masque de sous-réseau afin de déterminer l'adresse du sous-réseau de google et le système la compare au sous-réseau de votre hôte. Comme ils diffèrent, les paquets seront transmis au routeur dont l'adresse matérielle devrait toujours être en mémoire. Un numéro de port est obtenu auprès du système pour identifier le canal de communication depuis l'extérieur. Le numéro de port sur utilisé pour communiquer sur google sera implicitement le port 80, numéro classiquement utilisé pour les serveurs Web.

Dans la construction et l'émission des paquets d'autres mécanismes interviennent : découpage des données à transmettre en paquets, calcul et contrôle de sommes de contrôles, suivis des paquets et retransmission en cas de non-réception ou mauvaise réception. Les détails associés sortent du cadre de cette initiation.

Paramètres utiles à la configuration de mon hôte

Le fonctionnement des mécanismes présentés repose sur un ensemble de paramètres que nous allons observer à présent.

- ? Utilisez le raccourci Win+r pour ouvrir la fenêtre exécuter et exécuter la commande **cmd**.
- ? Maximisez la fenêtre de l'interpréteur de commande qui s'ouvre, et exécutez **ipconfig /?** afin d'obtenir l'aide de la commande ipconfig. Quelle option permet d'obtenir toutes les informations de configuration ?
- ? Utilisez cette option avec la commande ipconfig afin d'affichez toutes ces informations. Dans la sortie produite repérez les éléments suivants pour la Carte Ethernet Connexion au réseau local:
 - o **Adresse physique** de l'interface
 - o **Adresse IP**
 - o **Masque** de sous-réseau
 - o **Passerelle** par défaut
 - o Adresse IP du ou des serveurs de noms (**DNS**)
- ? Les machines des salles du nautibus ne disposent pas d'une passerelle par défaut en raison de la politique d'accès à Internet définie par les administrateurs. L'accès à Internet par le navigateur est toutefois possible après un ajustement décrit plus loin. Quelles sont les machines avec lesquelles votre hôte (du nautibus) peut communiquer malgré cette restriction?
- ? A quel **réseau** et **sous-réseau** appartient votre hôte ?
- ? La commande **ping** permet d'envoyer des paquets à un hôte auxquels il répond s'il les reçoit. Ceci permet notamment de tester la présence d'un hôte sur le réseau. Que représentent les adresses du réseau 127 ? Choisissez deux adresses de ce réseau et utilisez-les comme dans la commande ping 127.0.0.1. Dans la sortie produite, combien de paquet émis ont obtenu de réponse ? Que pouvez-vous déduire de vos commandes ?
- ? Exécutez les commandes ping 134.214.88.10 puis ping bat710.univ-lyon1.fr. Quel **mécanisme** supplémentaire met en jeu la seconde commande ?
- ? A partir de l'aide de la commande ping, déterminez l'option permettant d'obtenir le **nom** associé à une adresse IP.
- ? L'hôte précédent est-il sur le même sous-réseau que votre hôte ? La **passerelle** est-elle intervenue dans les échanges précédents ?
- ? Cette manipulation n'est pas possible des salles de TP du nautibus, mais il serait intéressant de la réaliser d'ailleurs. La commande **tracert** permet de déterminer la route empruntée par les paquets émis vers une destination. Exécutez la commande **tracert** www.univ-lyon1.fr. Combien de routeurs ont relayé les paquets vers la destination finale ? Quels réseaux ont été traversés par les paquets ? Mêmes questions pour www.google.fr.

Ces diverses manipulations avaient pour objet d'accéder au paramétrage du réseau de votre hôte, de le tester et de mettre en jeu les différents mécanismes exposés. Cependant, il est rare d'utiliser l'interpréteur de commande pour utiliser des outils de navigation sur internet. L'usage quotidien repose en général sur un navigateur graphique (Internet Explorer ou Mozilla Firefox) pour la navigation et un client de messagerie pour la gestion du courrier électronique.

Utilisation du navigateur

Un navigateur permet d'accéder à des ressources que l'utilisateur doit désigner. Le format d'adressage de ressources en vigueur repose sur les URLs, (Uniform Resource Locator) présentées ci-après.

URLs

Une url est un format de nommage universel pour désigner une ressource sur internet. Une url est structurée comme suit, les parties entre crochets étant optionnelles:

Protocole://[Nom d'utilisateur[:Mot de passe]@]Nom du serveur[: Port][/ Chemin]

Les navigateurs permettent à l'utilisateur de spécifier une url pour l'obtention de la ressource pointée. En fonction des protocoles pris en charge par le navigateur, les modèles suivants d'urls peuvent être utilisés :

http://istil.univ-lyon1.fr/french_index.htm - utilisation du protocole http (HyperText Transfert Protocol) à destination du serveur istil.univ-lyon1.fr sur lequel le chemin à la ressource sollicitée est french_index.htm

ftp://ftp.free.fr/pub/Distributions_Linux/ - utilisation du protocole ftp (File Transfert Protocol) sur un site ne nécessitant pas d'authentification.

<ftp://user:password@privateftp.keepout.net/> - utilisation du protocole ftp sur un serveur nécessitant une étape d'identification/authentification. Notez qu'en l'absence des paramètres user et password dans l'url, une interface d'authentification sera présentée à l'utilisateur afin qu'il s'identifie. Par ailleurs, il n'est pas recommandé d'utiliser cette syntaxe faisant apparaître les paramètres de connexion étant donné le mécanisme d'historique existant sur la plupart des navigateurs.

<file://localhost/C:/Documents%20and%20Settings/> - utilisation du protocole file sur le poste. Ce protocole permet d'utiliser le navigateur comme un explorateur de document.

Pratique de la navigation

Par le biais du navigateur

- ? Lancez une instance d'**Internet Explorer** (souvent dénommé **IE**) en double-cliquant sur son icône (si elle existe) ou à partir du menu démarrer.
- ? Les machines des salles du Nautibus nécessitent un ajustement de configuration supplémentaire pour pouvoir accéder à Internet. En effet, ces machines ne peuvent accéder directement à Internet mais peuvent utiliser un intermédiaire qui assure les échanges : un serveur proxy. Ce proxy doit être déclaré auprès du navigateur utilisé pour pouvoir accéder à Internet. L'adresse de ce proxy est **proxy710.univ-lyon1.fr** et le port vers lequel les requêtes doivent être transmises est le port **8080**. Dans IE, ces paramètres trouvent leur place dans le menu Outils, Options Internet, onglet Connexions, bouton paramètres réseau puis rubrique Serveur Proxy. Si vous utilisez une machine du bâtiment Nautibus, effectuez ce paramétrage.
- ? Dans la **barre d'adresse**, saisissez l'adresse du portail étudiant etu.univ-lyon1.fr puis validez. Remarquez que le navigateur a préfixé l'adresse par la partie manquante dans l'URL : celle décrivant le protocole.

- ? Déplacez la souris sur les éléments de la page et remarquez les changements d'apparence du pointeur en fonction des éléments survolés. Lorsque la souris passe sur un lien, remarquez l'adresse indiquée dans la **barre d'état**. Vers quel lien pointe le logo de l'université en haut à gauche de la page ?

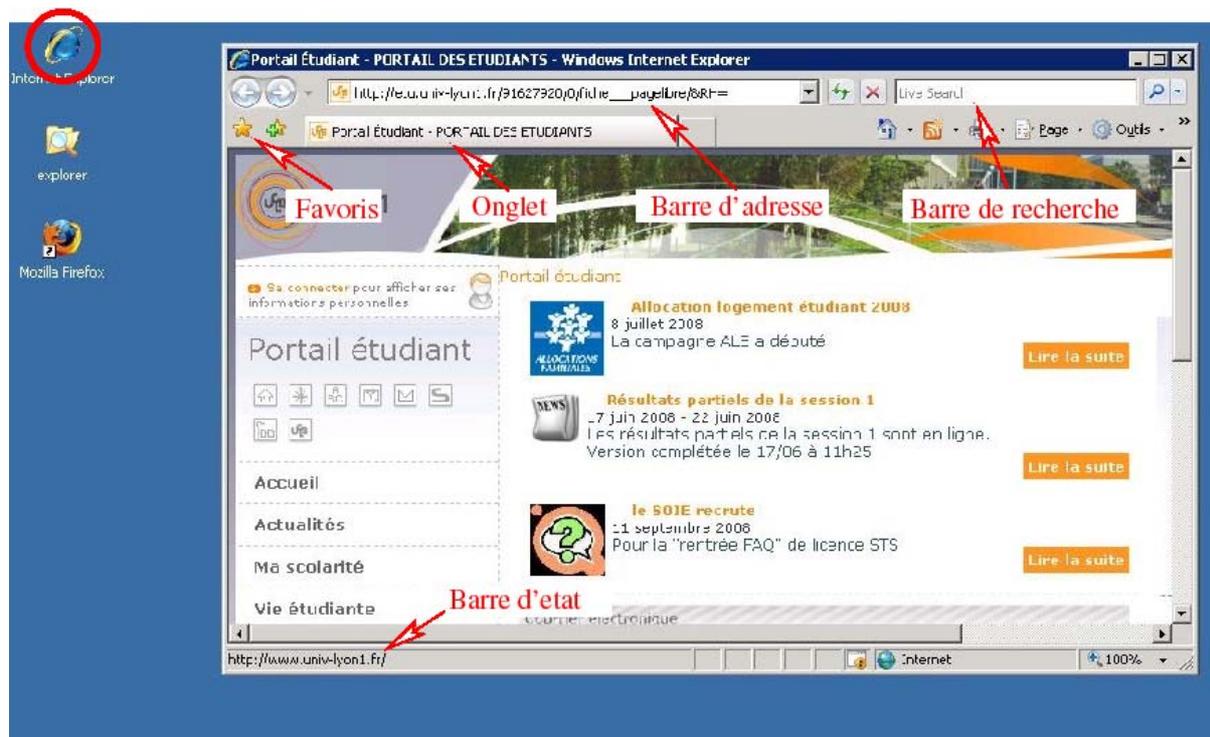


Figure 9 - Interface d'Internet Explorer

- ? Suivez le lien vers lequel pointe le logo de l'Université. La page de l'Université s'affiche. Le navigateur est capable de gérer un historique des pages visitées. Revenez à la **page précédente** en cliquant sur la flèche gauche sur la barre d'adresse. Suivez à nouveau le lien, mais en cliquant à l'aide de la molette de la souris et non le bouton gauche: la page s'ouvre dans un nouvel onglet.
- ? Il est possible d'afficher plusieurs pages dans le navigateur à l'aide des onglets et de basculer facilement entre ces onglets. Utilisez la combinaison **Ctrl+Tab** pour changer d'onglet affiché.
- ? L'affichage d'une nouvelle page peut se faire dans un nouvel onglet ou dans une nouvelle fenêtre. Utilisez la combinaison **Ctrl+t** pour ouvrir un nouvel onglet. Dans la barre d'adresse, le champ de saisie de l'adresse est activé et vous pouvez directement saisir l'url vers la nouvelle ressource. Entrez l'adresse du moteur de recherche google : <http://www.google.fr>.
- ? Ouvrez trois nouveaux onglets puis utilisez la combinaison Ctrl+Tab pour naviguer entre les différents onglets ouverts. Finalement, repositionnez-vous sur les nouveaux onglets et utilisez la combinaison **Ctrl+w** pour refermer ces onglets.
- ? Il est possible de mémoriser les pages visitées afin de les retrouver facilement par la suite. Dans l'interface d'Internet Explorer, les adresses enregistrées constituent les « Favoris ». Dans Firefox, il s'agit des Marque-pages (Bookmarks). Placez le portail étudiant dans vos **favoris**. Pour cela, affichez l'onglet contenant la page du portail étudiant puis cliquez sur le bouton dédié, situé à côté de celui donnant accès aux favoris.
- ? Utilisez la combinaison **Ctrl+n** pour ouvrir une nouvelle fenêtre. Vous pouvez saisir directement l'url de la ressource à afficher. Saisissez l'adresse de l'ISTIL et affichez la version française puis ajoutez-la à vos favoris une fois la page affichée. Faites de même avec la page d'accueil de Wiki-

pedia. Pour trouver l'url, recherchez dans le moteur de recherche google le mot clé wikipedia. Suivez le lien approprié puis ajoutez-le à vos favoris.

- ? Cliquez sur le bouton des favoris afin de consulter la liste des sites figurant dans vos favoris. Sélectionnez l'un d'eux: la page s'affiche dans l'onglet en cours. Il est possible d'agrandir ou réduire la taille des éléments d'une page affichée. Maintenez la touche Ctrl enfoncée en tournant la molette de la souris. Inversez le sens de rotation pour inverser le **zoom**. Pour revenir à la taille originale, vous pouvez cliquer sur la petite loupe située en bas à droite de la fenêtre d'IE.
- ? Fermez la ou les instances d'IE (par la combinaison Alt+F4 par exemple) en confirmant la fermeture de tous les onglets si nécessaire, puis lancez à nouveau IE. Dans le premier onglet, affichez la page d'accueil de l'ISTIL et dans un second onglet, ouvrez le portail étudiant. Repérez sur la même ligne que les onglets le bouton figurant une maison et cliquez sur la flèche orientée vers le bas pour accéder au menu de gestion des pages de démarrage. Dans le menu qui se déroule, choisissez Ajouter ou modifier une **page de démarrage**, puis dans la boîte de dialogue sélectionnez Utilisez l'ensemble d'onglets actuel comme page de démarrage.
- ? Fermez l'instance d'IE puis relancez-le. Au **démarrage**, les pages enregistrées précédemment doivent être chargées automatiquement.
- ? Testez les adresses <http://www.nowhere.nada/> et <http://www710.univ-lyon1.fr/~noone>. Qu'est-ce qui différencie les **erreurs** signalées?

Confidentialité des données échangées

Lors des échanges

Lorsqu'un utilisateur navigue sur Internet, il émet des requêtes via le navigateur et le navigateur gère les réponses, notamment en affichant une page à l'aide des éléments qu'il reçoit. Les échanges d'informations se basent sur l'ensemble de protocoles utilisés dans la pile TCP-IP. La plupart de ces protocoles se base sur des échanges qu'il est facile de suivre et comprendre. Seuls quelques protocoles tentent d'apporter une réponse à la protection des données échangées en cryptant les échanges.

Nous allons considérer des captures de trafic réalisées dans différentes situations afin d'observer les mécanismes présentés ici ainsi que les protocoles courants de la couche application et les flux qu'ils engendrent. Les captures ont été réalisées à partir d'une machine d'une salle de TP du Nautibus. Son adresse IP est 134.214.90.82 et son adresse matérielle est 00:13:72:97:cc:47 (ou Dell_97:cc:47 après identification du constructeur de l'interface). Il est important de signaler que lors d'une capture, tout le trafic est enregistré, i.e. celui que l'on pense observer auquel s'ajoutent de nombreuses communications que le système et l'environnement produisent.

- ? Sur la page <http://bat710.univ-lyon1.fr/~dclot/ISTILL3.html>, **téléchargez** les trois fichiers de capture de trafic.
- ? Ouvrez le fichier nommé IE_Sans_Proxy.pcap. L'application associée aux fichiers d'extension pcap est **ethereal** (renommée wireshark dans les versions les plus récentes). Les données capturées sont présentées sous trois formes: une liste des paquets, la structure, au sens des protocoles, du paquet sélectionné dans la liste et les données de ce paquet sous forme « brute ». Maximisez l'interface d'ethereal et ajustez les trois panneaux présentant ces informations si besoin.
- ? La capture a été réalisée alors que le proxy n'était pas configuré dans IE. Lors de l'ouverture, IE a tenté d'ouvrir la (ou les) page de démarrage, ici <http://go.microsoft.com/fwlink/?LinkId=74005> . Dans l'interface de l'outil, les lignes numérotées représentent les paquets d'information échangés. A quel protocole correspondent les **paquets** de numéro 2 et 3 ? Quelles informations contiennent-

ils ? Vous pouvez sélectionner ces paquets dans la liste puis utiliser le panneau dessous pour observer plus en détail son contenu. Quelle est l'adresse IP du serveur go.microsoft.com ?

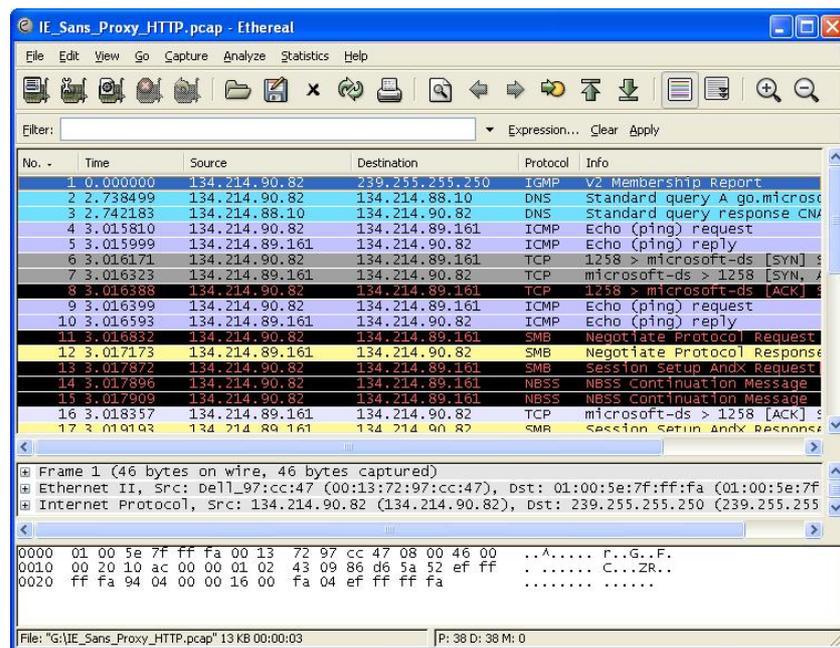


Figure 10 - Interface d'ethereal

- ? Pouvez-vous trouver les paquets correspondant à la requête **http** qu'il faudrait émettre pour obtenir la page de démarrage ? Pourquoi ?
- ? Ouvrez le fichier nommé IE_Config_Proxy_DNS_Page_demarrage.pcap. La capture a été réalisée avec IE alors que le proxy venait d'être configuré. La page de démarrage a pu être affichée dans ce cas. A quel **protocole** correspondent les paquets 3 et 4 ?
- ? A quel protocole correspondent les paquets 5 et 6 ? Quelles **informations** transportent-ils ?
- ? Le paquet 10 est la requête http visant à obtenir la page de démarrage. Vers quel hôte est dirigée cette requête i.e. quelle est la destination immédiate du paquet dans le processus de **routing**?
- ? Aucune requête **DNS** n'a été émise par notre hôte pour obtenir l'adresse IP du serveur go.microsoft.com. Selon vous, où le mécanisme de résolution de nom a-t-il eu lieu?
- ? Ouvrez le fichier nommé IE_Avec_Proxy_HTTP.pcap. Cette capture a été réalisée dans les mêmes conditions que précédemment. Le navigateur a été utilisé pour afficher la page <http://bat710.univ-lyon1.fr/~dclot/ISTILL3.html> .
- ? Dans les paquets, repérez le paquet correspondant à la requête http initiale. Sélectionnez ce paquet puis faites un clic droit sur la ligne correspondante et choisissez dans le menu contextuel **Follow TCP stream**. Dans la fenêtre qui s'ouvre, la totalité de l'échange engendré par la requête est reconstitué. Les parties sur fond rose correspondent aux requêtes émises par le navigateur et celles sur fond bleu correspondent aux réponses. Combien de fichiers sont échangés?
- ? Sélectionnez la ligne 57 correspondant à la réception de l'image au format png présente dans la page. Dans le bandeau présentant la structure, sélectionnez la ligne Portable Network Graphics. Ceci met en évidence le contenu du fichier transféré dans le panneau inférieur. Utilisez la combinaison **Ctrl+H** pour enregistrer les données correspondant au fichier transféré. Vous nommerez le fichier test.png et le placerez sur le bureau. Une fois enregistré, double-cliquez dessus pour

l'afficher. Vous devez observer une image de la page <http://bat710.univ-lyon1.fr/~dclot/ISTILL3.html>.

Ces manipulations ont pour objectif de montrer la grande transparence du protocole http lors des échanges. Une machine présente sur le trajet des données peut être le lieu d'une grande indiscretion ! Le protocole https est la version sécurisée du protocole http. Il permet un encryptage des données échangées entre le navigateur et le serveur.

- ? Lancez une instance d'IE et ouvrez le portail étudiant <http://etu.univ-lyon1.fr> et cliquez en haut à gauche sur le lien se connecter.
- ? Quel est le protocole utilisé pour l'ouverture de l'interface d'authentification? Observez le cadenas en bas à droite de la fenêtre de navigation. Un site utilisant le chiffrement dans ses connexions afin d'empêcher d'autres utilisateurs malveillants d'Internet de voir les données transmises est signalé par la présence d'un cadenas à cet endroit accompagné du nom de domaine du site avec lequel l'échange est réalisé.

Les protocoles http et https sont essentiellement réservés à la consultation passive d'information. Le protocole ftp est un protocole dédié aux transferts de fichiers dans les deux sens entre le serveur et le client. IE permet l'utilisation du protocole ftp. Il est également courant d'utiliser la ligne de commande.



Le filtrage du trafic réalisé dans les salles de TP du nautibus empêche l'usage du protocole ftp de manière générale. En l'absence de mise en place d'une solution officielle lors de l'impression du sujet, les questions ci-dessous sont définies sans prendre en considération le filtrage du nautibus. Une adaptation des questions ci-dessous pour les salles du nautibus devrait être publiée sur <http://bat710.univ-lyon1.fr/~dclot/ISTILL3.html>.

- ? Ouvrez l'url <ftp://istil-ftp.univ-lyon1.fr>. Une fenêtre de dialogue demande les paramètres de connexion au serveur ftp. Utilisez le login testmiag et le mot de passe Iw5iseix puis validez.
- ? Dans l'interface IE, dans le menu Page, choisissez Ouvrez le site FTP dans l'Explorateur Windows. L'apparition de la fenêtre de l'explorateur est suivie de celle des paramètres de connexion. Saisissez-les à nouveau.
- ? Dans l'arborescence de fichier présente sur le serveur, faites glisser un fichier sur le bureau. Le fichier présent sur le serveur est copié vers votre poste. Visionnez le contenu de ce fichier.
- ? Renommez ce fichier en incorporant votre nom dans le nouveau nom puis faites glisser le fichier vers la fenêtre de l'explorateur présentant l'arborescence du serveur. Le fichier est copié vers le serveur.

Notez que le protocole ftp transporte lui aussi l'information en clair sur le réseau, dont le login et le mot de passe au serveur. Son usage doit être évité en milieu étranger i.e. dans un contexte réseau mal maîtrisé.

Traces de navigation

La gestion de l'**historique** et l'utilisation d'un **cache** sont des fonctionnalités très répandues parmi les navigateurs. L'historique de navigation permet de retrouver les urls visitées et les dates de visite. Le cache est un espace utilisé pour stocker les pages web visitées et tous les éléments qui les constituent pour limiter un trafic inutile (notamment les ressources communes à plusieurs pages comme les feuilles de style).

Ces fonctionnalités entraînent un stockage d'informations relatives à la navigation des utilisateurs au beau milieu de leurs données personnelles. Ce fait, parfois méconnu, met en péril la confidentialité autour des informations affichées par les utilisateurs. Un utilisateur averti doit maîtriser la gestion de ces mécanismes. Il est important de noter que chaque navigateur gère de façon indépendante son historique et son cache.

- ? Lancez une instance d'IE. Utilisez la combinaison **Ctrl+Maj+H** afin de basculer entre affichage et masquage du panneau de l'historique.
- ? A l'aide du menu déroulant du bouton Historique, affichez l'historique **par site**, puis **par date**.
- ? Il est possible de retirer des éléments de l'historique : affichez l'historique par site, puis faites un clic droit sur une ligne des éléments affichés. Dans le menu contextuel qui s'affiche, choisissez **supprimer** pour retirer de l'historique toutes les pages visitées sur ce site. L'autre choix du menu contextuel permet d'afficher le détail des pages visitées sur un site.
- ? Il est possible de supprimer tout l'historique ainsi que d'autres éléments relatifs à la navigation. Cliquez sur le bouton Outils présent sur la même ligne que les onglets. Dans le menu, choisissez **Supprimer l'historique de navigation...** puis dans la fenêtre correspondante, cliquez sur le bouton Supprimer l'historique... et confirmez votre choix. Dans le panneau de l'historique, tous les éléments disparaissent. Notez que cette action n'a aucune incidence sur l'historique de Mozilla Firefox.
- ? La fenêtre affichée permet également de supprimer les Fichiers internet temporaires (i.e. le contenu du cache du navigateur), les Cookies, les données utilisées dans les champs de saisie de formulaires et les mots de passe. Afin d'accéder à plus de détails sur les paramètres de gestion du cache, fermez cette fenêtre puis cliquez sur le bouton Outils et choisissez la dernière entrée du menu déroulant **Options Internet**.
- ? Dans l'onglet Général, cliquez sur Paramètres dans la partie relative à l'historique de navigation. Quel est l'espace réservé pour le cache ? Relevez le **chemin** du dossier utilisé par IE pour organiser son cache puis fermez cette fenêtre.
- ? Ouvrez un interpréteur de commande et faites un clic droit sur la barre de titre de la console. Dans le menu contextuel, choisissez Propriétés, puis l'onglet configuration. Donnez une largeur de **115 colonnes** à la taille de la fenêtre puis validez.
- ? Dans la console, placez-vous dans le dossier relevé précédemment. Que contient ce dossier ? Vous utiliserez les options de la commande **dir** permettant de lister les répertoires cachés. Placez-vous dans le répertoire dont le nom termine par IE5.
- ? Supprimez les Fichiers internet temporaires. Avec IE, ouvrez la page d'accueil de l'ISTIL. Le cache reçoit alors les éléments de la page affichée. A l'aide de la commande dir, déterminez l'ensemble des images d'extension gif présentes dans le cache. Vous pourrez consulter les exemples de la commande dir dans le **Centre d'aide et de support**.
- ? Vous allez réaliser un **copier/coller** du chemin d'un dossier contenant les images dont le nom débute par logo. Pour cela, ouvrez le menu contextuel de la console, puis choisissez Modifier puis Sélectionner. A l'aide de la souris, mettez en surbrillance le chemin complet du dossier (en maintenant le bouton gauche enfoncé) puis validez avec la touche entrée. Ouvrez alors une instance de l'explorateur et dans la barre d'adresse, copiez (Ctrl+V) le chemin. Retrouvez-vous les images affichées dans le navigateur ?