Adresse IP et Ports

1/- Protocoles :

1.1/ - Smtp

Le protocole SMTP (simple mail transfert protocol) sert a transférer des mails d'une machine a une autre.
Pour envoyer un mail il suffit de ce connecter sur le port TCP 25 d'un serveur, et moyennant quelques commandes envoyer ce mail.

1.2/ - Http

Le Protocole HTTP (hypertext transfert protocol) sert au dialogue entre votre navigateur Web et un serveur.
C'est un protocolebasé sur TCP, il suffit d'ouvrir une connexion TCP sur le port 80 du serveur, et d'envoyer une requête vers le serveur.
Il est très facile de faire des tests avec la commande: telnet www.site.com 80.

La requête à la forme suivante: GET http://www.site.com/index.html HTTP/1.1 (suivi de 2 retour chariots).

La réponse sera composée de deux parties, l'entète qui indique si la requête a reussie et le corps du message.

Remarques: en plus de la ligne GET ..., la requête peut contenir des champs supplémentaires sur les lignes suivantes, tel que Host qui est indispensable si l'on passe par un proxy. Cette information est utilisée dans le programme client.

1.3/ - Pop

POP (post office protocol) (la version standard est POP3, definie dans la RFC 1725) est la manière dont les clients mail récupère les emails sur les serveurs internet. Comme la plupart des protocoles internet, il est basé sur la ligne de commande, c'est à dire que toutes les operations sont faites a partir d'un texte de commandes qui est envoyé au serveur. Il est donc tres simple de simuler un client à partir d'une connection telnet sur le serveur (et le bon port), il est donc aussi facile d'écrire un client spécialisé à certaines taches basées sur la mail.

1.4/ - ICMP

Le protocole ICMP (Internet Control Message Protocol) gère les messages d'erreur et de contrôle qui sont transmis entre deux ordinateurs (ou hôte) ou durant le processus de transfert. Il leur permet de partager ces informations. ICMP est essentiel pour diagnostiquer les problèmes du réseau.

1.5/ -TCP

Le protocole TCP (Transmission Control Protocol) est l'un des principaux protocoles employés sur Internet.
Il facilite les tâches critiques telles que le transfert de fichiers et les sessions distantes.
Il accomplit ces opérations par l'intermédiaire d'une méthode de transfert fiable orientée connexion, fondée sur la transmission d'un flux. Ce flux garantit quel les données arriveront dans un ordre et un état identiques à ceux d'émission. A cet égard, il diffère des autres protocoles de la suite. Dans le cas d'une livraison non fiable, vous n'avez aucune garantie que les données arriveront dans un état parfait.

Le système TCP repose sur un "cheminement", appellé "Poignée de Main en trois temps", qui est établi entre la machine "cliente" et machine "hote".
Ce cheminement est expliqué ci-dessous

1) Demande de connexion par envoi de paquet SYN
2) Réponse du serveur par un paquet SYN/ACK
3) Le client envoie un paquet ACK pour ouvrir la connexion

Pour l'étape 2 le serveur peut aussi envoyer un paquet RST s'il refuse la connexion.

1.6/ -IP

L'IP est le protocole en-tête de base dans un paquet et se trouve toujours là, Il assure le format des paquets et la bonne transmission sur le réseau.

L'adresse IP est à la base de tout; elle est attribué par le fai à chaque connexion.
C'est en fait une sorte de numéro de série. Malheureusement grâce à cette adresse IP on peut vous tracer lors de vos connections mais aussi la piquer lors d'une connexion et se faire passer pour vous. Car L'ip est à la base de tout sur le net. Par exemple, vous avez l'IP d'un pc connecté et mal protégé, vous pouvez rentrez dessus très facilement. Cette IP est dynamique, elle change à chaque connexion.

IP v4

C'est la version du protocole ip actuellement en place sur le net, elle n'a pas changé depuis les années 70.
L'adresse ip v4 est codé sur 32 bits, il y a plus de 4 milliards de combinaisons différentes(4 228 250 627 combinaisons exactement).
Une adresse IP v4, c'est ça: 212.62.66.68 , dans chaque suite les nombre sont compris en 0 et 256

IP v6

Appelée aussi IPNext Génération, elle à été mise en place du fait de la saturation d'ip libres.
Une ip v6 ressemble à cela:

4A3F:AE67:F240:56C4:3409:AE52:440F:1403

Elle n'est pas encore 'en service' sur internet.

Comment obtenir une IP:

1/ - Pour obtenir l'adresse Ip d'un site vous faite un ping sur le site en tapant sous dos: ping -a lesite.com

2/ - Pour voir votre IP, allez dans "Démarrer", "Exécuter" puis "Winipcfg" ou alors sous Dos tapez "ipconfig"

3/ - Pour avoir l'ip de quelqun dont vous avez son mail, arrangez-vous pour qu'i vous envoie un mail et vous pouvez récupérer ainsi son ip, en regardant sa source vous apercevrez un texte ressemblant à ceci:

Return-Path: <toto@yahoo.fr>
Received: from minitel.net (193.252.91.16) by mailsmtp3.ftmms (5.1.053)
id 3ADC4EF2000D9C57 for trauma@mailme.org; Tue, 24 Apr 2001 14:11:12 +0200
From toto@yahoo.fr Tue Apr 24 14:11:10 2001
Received: from web11406.mail.yahoo.com (web11406.mail.yahoo.com [216.136.131.236])
by smtp1.minitel.net (Postfix) with SMTP id 1B14D41EBF
for <trauma@mailme.org>; Tue, 24 Apr 2001 14:11:10 +0200 (MET DST)
Message-ID: <20010756891109.48426.qmail@web11406.mail.yahoo.com>
Received: from [175.42.3.112] by web11506.mail.yahoo.com; Tue, 24 Apr 2001 14:11:09 CEST
Date: Tue, 24 Apr 2001 14:11:09 +0200 (CEST)
From: =?iso-8859-1?q?hean=20dupond?= <toto@yahoo.fr>
Subject: Coucou
To: Trauma <trauma@mailme.org>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="0-1017306873-988114269=:47269"
Content-Transfer-Encoding: 8bit

--0-1017306873-988114269=:47269
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
Content-Disposition: inline

Pour obtenir l' en-tête d'un mail sous Outlook, allez dans "Fichier" => "Propriétés" puis "détails".
Pour obtenir l'en-tête d'un ip sous netscape Messenger , allez dans "Affichage" => En-têtes => Tous. A chaque fois que vous lirez un mail, l'en-tête s'affichera.

4/ - Sous ICQ, en lançant un programme spécifique, en lui indiquant l'UIN, vous pouvez récupérer l'ip (voir dans les downloads pour récupérer ce prog)
Pour obtenir l'ip de quelqun sur l'irc tapez /dns login ou /whois login et l'ip de la personne concernée s'affiche.

2/- Les Ports :

Les ports sont utilisés quand on se connecte par exemple à un serveur.

Lorsque vous ouvrez votre navigateur, vous allez taper par exemple http://www.lesite.com/ et magie une page html va s'ouvrir, c'est comme si vous aviez tapé http://www.lesite.com:80/ en fait, vous vous passez par le port 80 pour vous connecter en http.

lorsque vous vous connectez sur un site ftp ou uploadez des données, vous passez par le port 21 (ftp) donc par un autre protocole.

Voici une liste des ports les plus utilisés :

Port :	Protocole:	Description:
7		Echo
15		netstat
21	Tcp	FTP
23	Tcp	Telnet
25		SMTP
79		Finger
80	Tcp	Http
110		POP3
119		nntp
139	Tcp	NetBIOS
143		IMAP
6346		Utilisé par GNUtella
8080		Http

6/- Ping/Pong :

Le ping (Packet InterNet Groper) est un outil permettant de tester les machines d'un réseau ou de vérifier qu'un hôte est disponible et de calculer un temps de transition en milli-secondes avec cette machine, en envoyant un paquet (ping) et en attendant la réponse (pong).
le paquet de données envoyé lors d'un ping s'appelle Icmp Echo Request.
Le pong renvoyé en réponse s'appelle Icmp Echo Reply.

Le protocole Icmp est un complément du protocole Ip, Il contient des messages d'information, d'erreur et de configuration permettant d'améliorer le réseau.
Chaque paquet Icmp (ping ou pong) à une durée de vie (TTL) choisie lors de l'envoi.

On peut envoyer cette commande sous MsDos par exemple par la commande ping ou via des utilitaires .

7/- Trace-route :

Le Trace-Route utilise le PING pour essayer de définir la "route" que parcourent les paquets vers une machine.
Cette route est en fait l'ensemble des routeurs qui traiteront le paquet permettant de le faire arriver à destination.

Pour effectuer un trace-route, tapez la commande tracert www.site.com