
Live CD
Spécialité
Réseaux
R&T
IUT
BETHUNE
R&T

Notice du LiveCD
Spécialité Réseaux

Les Logiciels Réseaux

Ethereal :

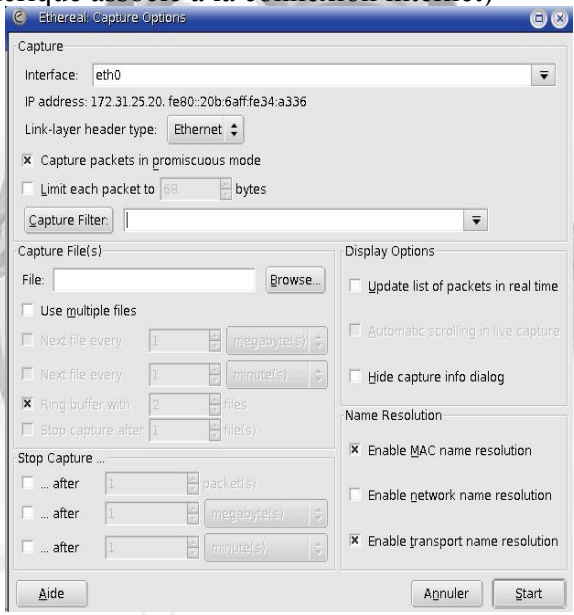
Ethereal est un sniffer de réseau, il capture les trames circulant sur le réseau, en permet l'analyse et sépare suivant l'encapsulation les différnetes données contenus dans ces trames.

Fonctionnement:
Pour lancer Ethereal il faut se connecter en root dans un terminal(commande su) puis lancer ethereal via la commande du même nom.
Une fois le logiciel lancé il faut choisir sur quelle interface capturer pour cela on va dans capture puis options ou par la raccourci clavier Ctrl+k.

Les Logiciels Réseaux

Ethereal :

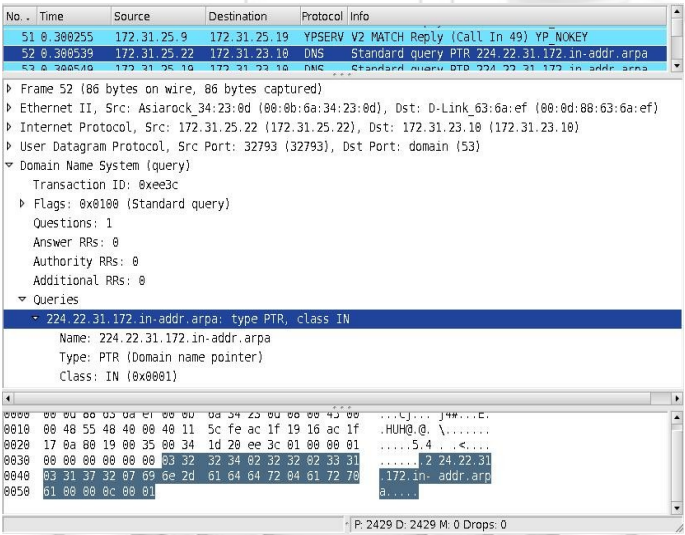
ethX est une carte réseau ethernet(où X est le numéro de la carte)
lo est la boucle locale
any capture sur toute les interfaces
pppX est le périphérique point à point(souvent le périphérique associé à la connexion internet)



Dans la ligne capture filter on peux rajouter des filtres sur les paquets à capturer tel que tcp ou udp pour filtrer suivant le protocole.Un clic sur le bouton start démarre la capture de trame et un clic sur arrêter dans la fenêtre qui s'ouvre termine la capture de trame.

Les Logiciels Réseaux

Ethereal :



Ex: avec cette capture de trame on voit ici que la machine 172.31.25.22(machine lr1-12 du laboratoire réseau) envoi une réquête de résolution inverse au serveur dns(172.31.23.10) pour obtenir le nom de la machine 172.31.22.224

Les Logiciels Réseaux

Annuaire LDAP(logiciel OpenLDAP) :

Un annuaire LDAP est un annuaire électronique pouvant être assimilée à une base de donnée permettant de stocker des données de façon hiérarchique donnant ainsi un accès facile aux données. OpenLDAP sert entre autre à :

constituer un carnet d'adresse
authentifier des utilisateurs (grâce à un mot de passe)
définir les droits de chaque utilisateur
recenser des informations sur un parc matériel (ordinateurs, serveurs, leurs adresses IP et adresses MAC...) décrire les applications disponibles.

Les Logiciels Réseaux

IPTABLES :

Par défaut iptables utilise la table filter(autorise ou non les paquets à entrer/sortir de la machine) deux autres tables sont également disponibles : nat(translation d'adresse et de port) et mangle(marquage de paquets et qualité de service) Pour changer de tables il faut commencer sa commande par :
iptables –t <nom de la table> <commande iptables à executer>

TELNET :

Connexion sur une machine distante non sécurisée

telnet <adresse ip ou nom de machine> <port>

Telnet peut servir à se connecter à un serveur SMTP, FTP, IRC ou encore un routeur Cisco par exemple pour pouvoir le configurer à distance.

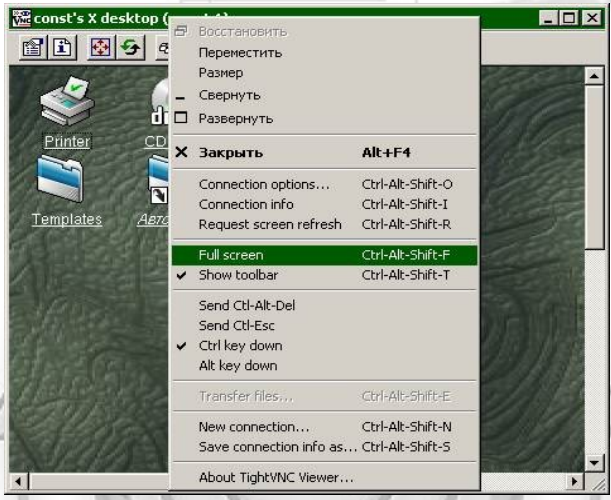
SSH :

Connexion sécurisée sur une machine distante

Une fois connecté vous devrez connaitre la syntaxe utilisée par le protocole du serveur sur lequel vous vous connectez.
Se connecter avec le nom d'utilisateur courant :
ssh <adresse ip ou nom de la machine distante>
Se connecter avec un nom d'utilisateur différent :
ssh –l <nom d'utilisateur> <adresse ip ou nom de la machine distante>

Les Logiciels Réseaux

TightVNC :



TightVNC permet de se connecter par le réseau(y compris par internet) sur le bureau d'une machine distante qu'elle que soit son système d'exploitation(à condition qu'un serveur TightVNC soit installer sur la machine sur laquelle on désire se connecter)

On peut voir ici sur l'exemple un utilisateur Windows se connecter sur une machine linux utilisant le gestionnaire de fenêtres KDE.

Les Logiciels Réseaux

Nessus :

Sécurité du réseau(logiciel nessus) :

Nessus *est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Il détecte les machines vivantes sur un réseau, balaie les ports ouverts, identifie les services actifs, leurs versions, puis tente diverses attaques.*

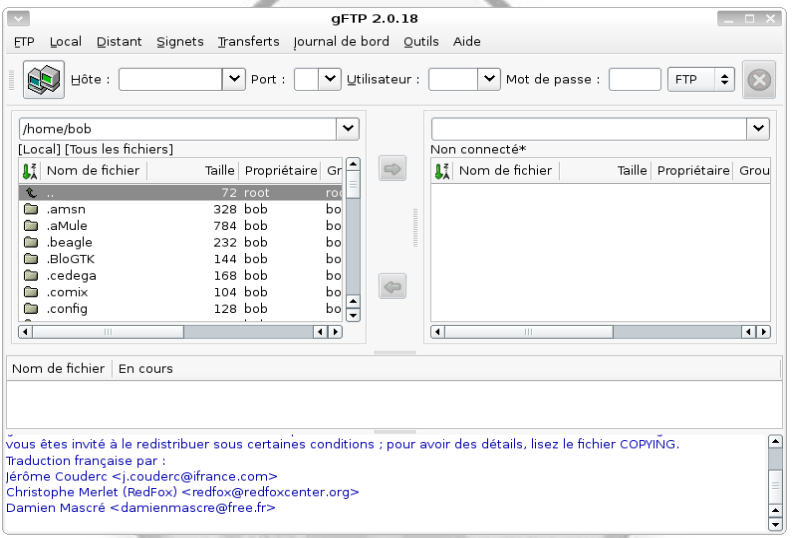
Nagios :

Supervision (logiciel Nagios) :

Nagios est un logiciel qui permet de superviser un système d'information complet. Entre autres ses capacités sont :
Superviser des services réseaux : (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP , etc.)
Superviser les ressources des serveurs (charge du processeur, occupation du disque dur, utilisation de la mémoire paginée) et ceci sur les systèmes d'exploitations les plus répandus.
Interface avec le protocole SNMP.
La supervision à distance peut utiliser SSH ou un tunnel SSL.
Possibilité de définir une hiérarchie dans le réseau pour pouvoir faire la différence entre un serveur en panne et un serveur injoignable.
La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins (alerte par email, SMS, etc...).

Les Logiciels Réseaux

gFTP :



Hôte : serveur auquel vous voulez vous connecter
Port : le port utilisé par le serveur
La liste des fichiers à gauche correspond à votre disque dur et celle de droite aux fichiers sur le serveur.

Les Logiciels Réseaux

IProute :

Outils réseau (logiciel iproute) :

Iproute est une suite d'utilitaires réseau incluant la commande ip qui permet la configuration de cartes réseau, créer des routes manuelles pour accéder à une machine et faire de la QoS à l'aide de la commande tc.

Supervision et administration du réseau(logiciel Net-Snmp) :
Net-SNMP est une suite d'applications permettant d'implémenter le protocole SNMP (Simple Network Management Protocol. Net-Snmp contient un agent extensible, une bibliothèque SNMP, des outils de requête et de modification d'informations à partir d'agents SNMP.

Net-SNMP :

Supervision et administration du réseau(logiciel Net-Snmp) :
Net-SNMP est une suite d'applications permettant d'implémenter le protocole SNMP (Simple Network Management Protocol. Net-Snmp contient un agent extensible, une bibliothèque SNMP, des outils de requête et de modification d'informations à partir d'agents SNMP.

Les Logiciels Réseaux

MINICOM :

Minicom permet la communication avec un équipement(modem, routeur, switch…) via le port COM(équivalent de l'HyperTerminal sous windows)

Il faut donc configurer minicom pour notre port série. Pour connaitre le port série il faut regarder dans les informations système :
dmesg | grep tty

ensuite lancez minicom à l'aide de la commande :
minicom –s

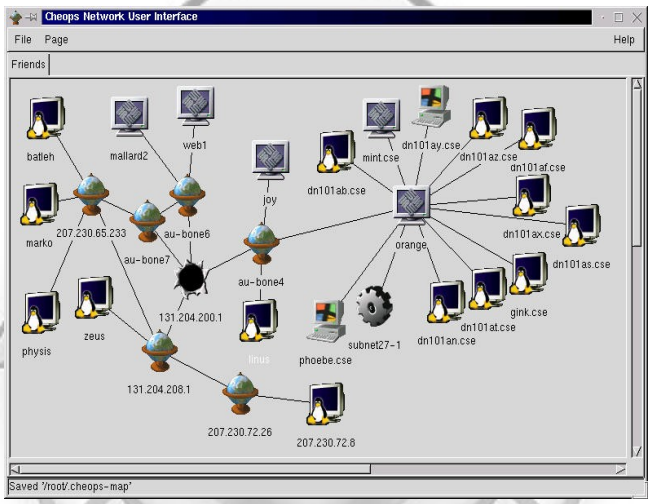
les principales options à configurer sont :

A- Port Serie
E- Débit/Parité/Bits
F- Controle de flux matériel

Celles-ci dépendent de votre ordinateur et de l'équipement auquel vous voulez vous connecter..

Les Logiciels Réseaux

Cheops :

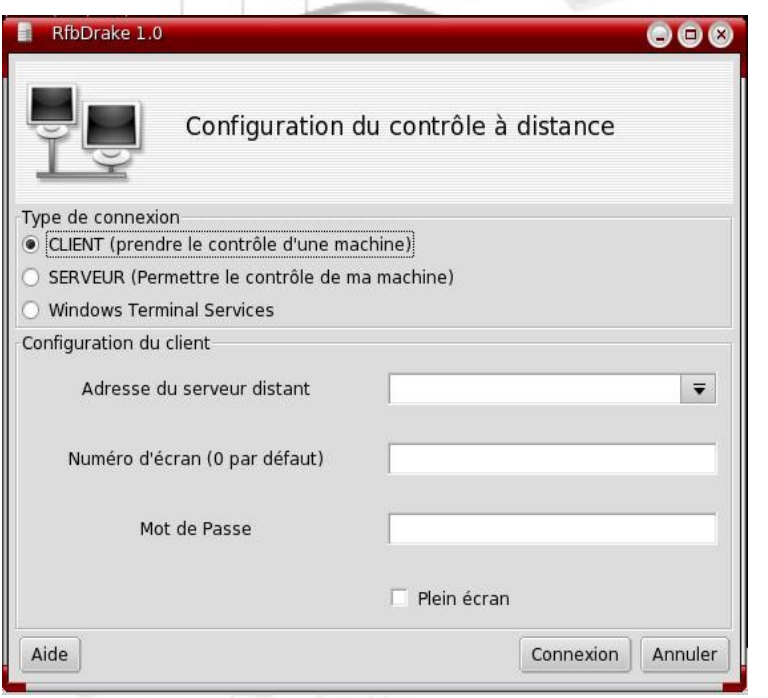


Cheops parcourt votre réseau pour y recenser toutes les machines, routeurs, passerelles…

Grâce à lui vous obtenez une « toile » de votre réseau vous indiquant l'OS des machines détectées, les routes pour accéder à une machine. Dans le menu contextuel vous obtenez accès aux services usuels tel que : ping, traceroute, secure shell, telnet. Cheops contient aussi un scanner de port ainsi qu'un client SNMP.

Les Logiciels Réseaux

RfbDrake :



Les Logiciels Réseaux

Bind :

Bind sert à associer une adresse ip à son nom de machine/nom de domaine ou à faire de la résolution inverse c'est-à-dire trouver l'adresse ip à partir du nom de domaine. Chaque serveur DNS s'occupe d'une zone et peut consulter un autre serveur DNS pour faire la résolution d'une autre zone.

AWK

Récupération de champs

Awk est un langage de traitement de lignes. Il agit comme un filtre qui prend une série de lignes en entrée (un fichier ou du texte écrit en argument de la ligne de commande) et affiche le résultat après traitement ou l'enregistre dans un fichier Awk lit l'entrée ligne par ligne, puis sélectionne les lignes à l'aide d'expressions rationnelles .Si la ligne correspond à l'expression rationelle celle ci est découpée en champs selon un séparateur d'entrée (qui par défaut correspond au caractère espace ou tabulation). Puis on récupére les différents champs dans des variables $1 (premier champ), $2 (deuxième champ), $3 (troisième champ), ..., $NF (dernier champ).

Les Logiciels Réseaux

La qualité de Service sous linux :

tc permet de mettre en place des filtres suivant des algorithmes, le débit, le protocole le port ou encore le type de traffic._

bench permet de tester les répartitions, des flux en période de congestion. Pour obtenir la liste des options. Tapez la commande

benchd.linux –help

mgen est un générateur de traffic entièrement configurable associé avec trpr qui analyse les fichiers de log de mgen. Gnuplot pourra tracer des graphiques des limitations de débit.

Exemple de génération de trafic: Pour générer 2 secondes après le démarrage, un flux nommé 1 en UDP avec comme IP de destination 192.168.9.24 sur le port 5000 un flux PERIODIC qui envoit 10 paquets de 1024 octets par seconde. 6 secondes après le démarrage, un flux nommé 2 en UDP avec comme IP de destination 192.168.9.24 sur le port 5001 un flux POISSON qui envoit 100 paquets de 8192 octets par seconde. Ce flux s'arrête au temps 11.0. Vous mettez les ligne suivantes dans le fichier source.mgn :

2.0 ON 1 UDP DST 192.168.9.24/5000 PERIODIC [10.0 1024]

6.0 ON 2 UDP DST 192.168.9.24/5001 POISSON [100.0 8192]

11.0 OFF 2

Pour lancer la génération : mgen input source.mgn

Credits

Rédaction de la Notice :
Sylvain Delattre

Design et Mise en page de la Notice :
David Daubresse

http://projet.livecd.free.fr

UNIVERSITÉ D'ARTOIS

i.u.t. BETHUNE