Sniffer

TP Sniffer

Introduction

Le rapport présenté ici est un compte-rendu des 10 séances de travaux pratiques réseaux et résume les principaux points abordés lors de ce stage. Les étudiants ont été mis dans une situation classique et courante dans toute entreprise : la réalisation d'un projet.

Un projet à réaliser, que ce soit en cours ou en entreprise, est toujours définit par un cahier des charges. Dans le cas d'une entreprise c'est le client qui le rédige. Il permet le dialogue entre le client et le technicien et reste l'un de seuls moyens pour que se comprennent le demandeur du produit et le concepteur.

Le projet que nous devions réaliser concernait le renifleur (sniffer) NetXRay, on nous a demandé de créer un TP qui permettrait de comprendre le principe du renifleur en une heure et demie ou trois heures (durée de la séance de travaux pratiques).

Nous allons tout d'abord parler des réseaux en général, le model OSI, les différents protocoles utilisés par Windows, les paquets et leur composition, les adresses des machines avant d'aborder le principe même du renifleur et d'expliquer le fonctionnement du logiciel NetXRay.

I) Les réseaux : quelques notions de base

1) Les couches réseau

Les tâches nécessaires à la communication en réseau sont réparties en une suite d'opérations assurées par des couches logicielles successives. Le modèle de référence OSI, développé par l'ISO, définit une description formelle de ces tâches en 7 couches

N°	couches	fonctions
1	physique	• **tout moyen de liaison entre les machines** • **appareillage mécanique, électrique** • **cartes, câblage, et "tuyauteries" diverses**
2	liaison	• **contrôle la couche physique** • **gère les erreurs de transmission physique**
3	réseau	• **routage physique des données** • **recherche du meilleur chemin reliant deux machines** • **choix en fonction de la topologie et de l'état du réseau**
4	transport	• **gère l'envoi des données** • **établit l'ordre et la priorité des envois**

		• **contrôle l'intégrité de la réception**
5	session	• **coordonne les communications entre les applications** • **maintient la synchronisation de leur connections** • **détecte les erreurs d'application** • **gère les interruptions temporaires**
6	présentation	• **conversion des données émises par l'application** • **plus de format de fichier, de caractères (ASCII, etc.) particuliers** • **format commun d'envoi indépendant de la machine** • **reconversion des données au format de l'application réceptrice**
7	application	• **interface utilisateur** • **émetteur - récepteur des données** • **exemple : Telnet, courrier, téléchargement, navigateur,...**

2) Les protocoles

Les protocoles informatiques définissent les règles de communication de chacune des couches, entre deux machines communicantes. Dans la pratique des réseaux Internet, la répartition a été simplifiée ; les protocoles utilisés se répartissent les tâches suivant l'architecture suivante, en 4 parties :

OSI	couches	protocoles
7 6 5	couches supérieures	DNS FTP NFS X TELNET SMTP KERBEROS et autres applications utilisateurs
4	Transport	TCP UDP
3	Réseau	IP ICMP
2 1	Physique	ETHERNET ATM PPP

Liste des protocoles dans C:\WINDOWS\PROTOCOL

Nom	Numéro	Allias	Commentaires
ip	0	IP	# Internet protocol
icmp	1	ICMP	# Internet control message protocol
ggp	3	GGP	# Gateway-gateway protocol
tcp	6	TCP	# Transmission control protocol
egp	8	EGP	# Exterior gateway protocol
pup	12	PUP	# PARC universal packet protocol
udp	17	UDP	# User datagram protocol
hmp	20	HMP	# Host monitoring protocol
xns-idp	22	XNS-IDP	# Xerox NS IDP

rdp	27	RDP	# "reliable datagram" protocol
rvd	66	RVD	# MIT remote virtual disk

3) Les paquets

- ENVOI :
  Les données transmises par l'application sont segmentées en paquets. Chaque couche ajoute son en-tête de protocole avant de transmettre le paquet à la couche inférieure : encapsulation des paquets.
- RECEPTION :
  chaque couche enlève l'en-tête qui lui est destiné et transmet les données à la couche supérieure.
- EXEMPLES : **Paquet IP**

IP	IP@ source	IP@ destin.	longueur données	données : paquet TCP encapsulé	CRC

Trame Ethernet

Préambule Ethernet	MAC@ destination	MAC@ source	Type	Données : paquet IP encapsulé	CRC
64 bits	48 bits	48 bits	16 bits	46oct.< longueur <1500oct.	32 bits

Ping

L'application PING (**C:\WINDOWS\PING.EXE**) sert à tester le réseau. En utilisant le protocole ICMP, elle envoie des paquets quelconques à une machine distante, laquelle a pour mission de les renvoyer ("Ping-pong"). Toute erreur permet de diagnostiquer un disfonctionnement dans les couches physiques (carte Ethernet, câblage,..).

4) Les adresses

Deux sortes d'adresses pour identifier les machines sur le réseau :

ADRESSE PHYSIQUE :

Media Access Control address (MAC@),
appelée *Adresse Ethernet* car fixée sur la carte Ethernet ,
codée sur 6 octets par le constructeur et le vendeur.
Exemple : 8:0:20:ae:6:1f

ADRESSE RESEAU :

Adresse INTERNET (IP@) ,
fournie sur demande au NIC (Network Information Center)
codée sur 4 octets ,
classées hiérarchiquement.
Exemple : 146.19.13.5

- Le transport se fait en utilisant les MAC adresses.
- Les couches supérieures ignorent les Mac adresses.
- Le protocole ARP (Address Resolution Protocol) assure la conversion.

II) Renifleur (ou Sniffer)

1) Définition

Sorte de sonde que l'on place sur un réseau pour l'écouter, et en particulier récupérer à la volée des informations sensibles, comme des mots de passes sans que les utilisateurs ou les administrateurs du réseau ne s'en rendent forcément compte.

2) Principe simplifié

Un réseau informatique peut en quelque sorte être comparé à un réseau de canalisation d'eau. On parle d'ailleurs couramment de « tuyau ».

Imaginez donc un réseau de canalisations à l'intérieur duquel circulent vos informations. Envoyer un fichier, se connecter à Internet etc. revient à établir un dialogue donc à échanger des informations à travers les tuyaux. Imaginez maintenant que quelqu'un fasse quelque part un trou dans la canalisation juste pour regarder. Il verra tous les messages circulants dans le tuyau, il pourra ainsi connaître l'émetteur du message, le destinataire et … son contenu.

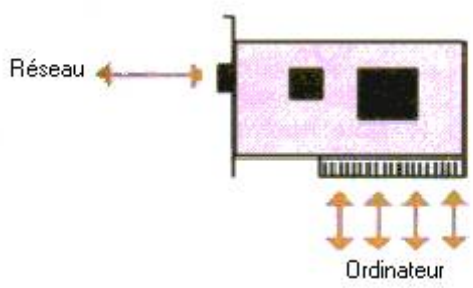
C'est en gros le principe du renifleur. C'est pourquoi on parle aussi de sonde ou d'écouteur.

3) Principe réel

Pour parler entre eux sur un réseau les ordinateurs sont dotés d'une carte d'extension, la carte Réseau. Du côté de l'ordinateur, la carte échange des paquets de données et du côté du réseau, elle module et démodule des trames.

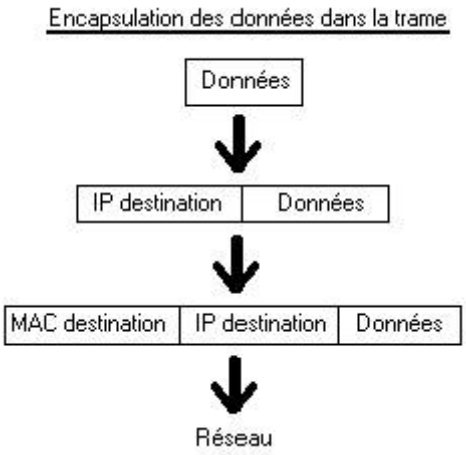
Les données que deux ordinateurs s'échangent doivent passer par la carte Réseau du premier, y être transformées en une trame, transiter par le câble, et passer par la carte Réseau du second. La trame ne transporte pas que les données mais aussi l'adresse de l'ordinateur de destination, et même celle de sa carte Réseau. Cela suppose une séquence d'opérations, au cours de laquelle les données seront « enveloppées » de ces informations nécessaires à leur routage.

Chaque carte Réseau est estampillée, en usine, d'un numéro unique que l'on appelle « l'adresse MAC » (aucun rapport avec l'ordinateur à la pomme). D'autre part, toute machine reliée à un réseau possède sa propre adresse IP,



affectée par l'administrateur système. Pourquoi deux adresses ? Entre autres, cela permet de ne pas avoir trop d'ennuis si on change d'ordinateur, car l'adresse MAC change alors forcément.

Pour faire la correspondance entre les adresses IP et les adresses MAC, un protocole, l'ARP (Adress Resolution Protocol) est utilisé. Cela maintient simplement une table en mémoire. Ainsi lors de la dernière étape de l'encapsulation, l'enveloppe contenant la bonne adresse MAC est ajoutée après consultation de la table suivante.



La trame

Lorsqu'une carte voit passer une trame, elle la « goûte » en examinant son enveloppe externe. La carte va comparer l'adresse MAC de destination à la sienne propre. Il existe un mode de fonctionnement spécial des cartes Réseau : le mode « mêlé » (« promiscuous mode »), dans lequel celles-ci vont sans discernement recopier toutes les trames et les trames et les transmettre à l'ordinateur, sans les faire disparaître du réseau. C'est aussi ce mode qui permet le reniflage, puisqu'il suffit de programmer l'ordinateur pour analyser les trames que lui envoie la carte. Utiliser un ordinateur pour renifler les trames qui transitent ne modifie pas les caractéristiques du réseau, et ne permet donc pas de détecter l'indiscret.

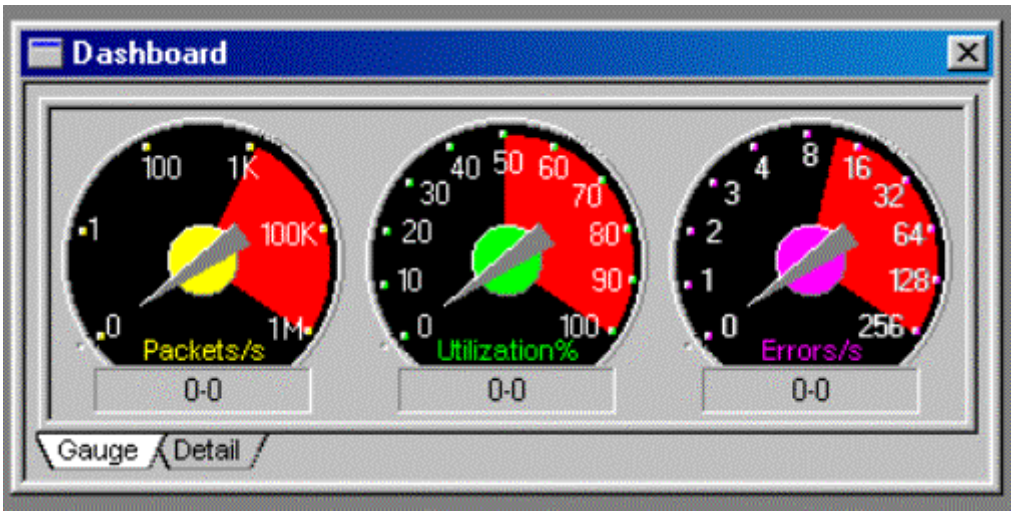
III) Fonctionnement du logiciel NetXRay

1) Les fonctions des boutons de la « Tool Bar »

Boutons	Fonctions
	Permet d'ouvrir un fichier sauvegardé
	Sauvegarde le document actif
	Ouvre les parametres de l'impression
	Arrête le document en cours d'impression
	Retourne au premier paquet
	Retourne au paquet précedent
	Va au paquet suivant
	Va au dernier paquet
	Permet d'ouvrir ou fermer le "Dashboard"
	Permet d'ouvrir ou fermer le "Packet Capture"
	Permet d'ouvrir ou fermer le "Packet Generator"
	Démarre la "Host Table"
	Démarre la "Matrix Statistics"
	Ouvre l' "History Folder"
	Démarre le "Protocol Distribution"

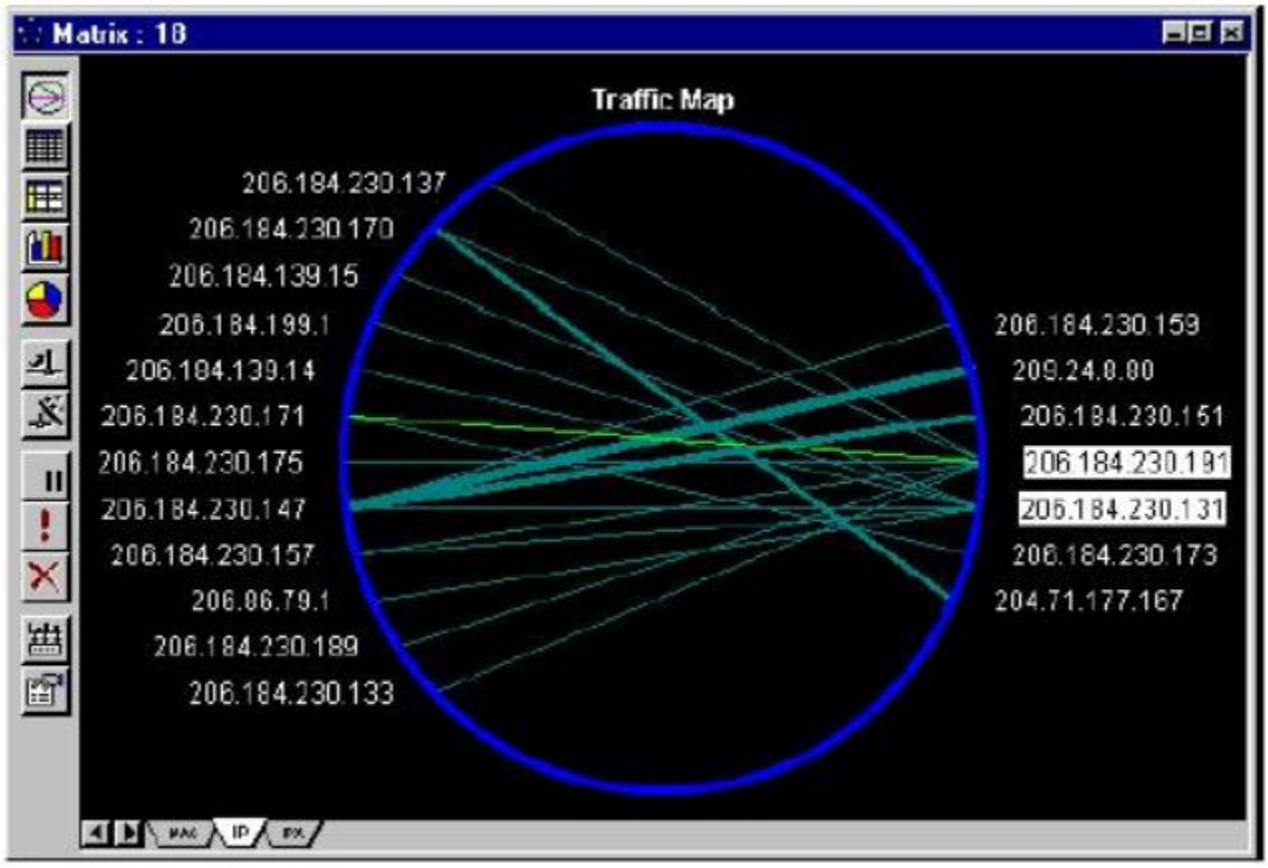
2) Le Dashboard

Le trafique du réseau : paquets par seconde, utilisation en pourcentage et erreurs par seconde sont visibles sur ce tableau de bord.



3) Matrix statistic

Elle nous permet de détecter le trafic du réseau, les adresses IP et MAC.

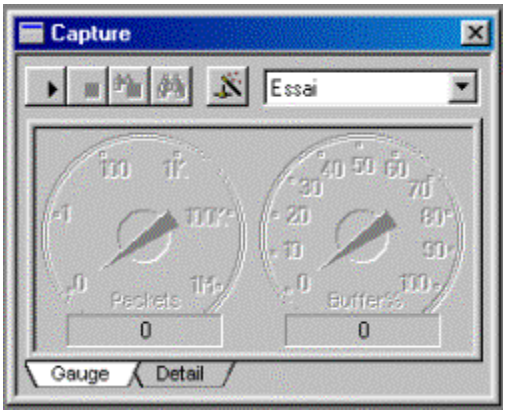


4) Capture des paquets

a) Pour capturer des paquets de type IPX (par exemple) :

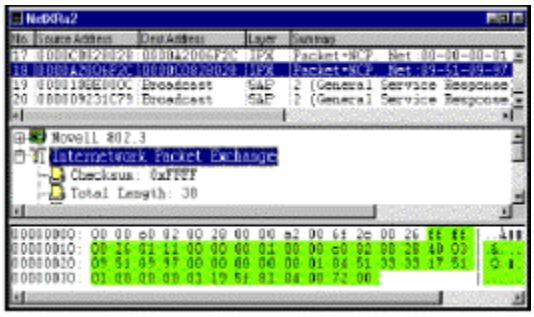
Il faut aller dans le menu Tools et sélectionner Capture ou appuyer sur le bouton  .

L’écran suivant apparaît :



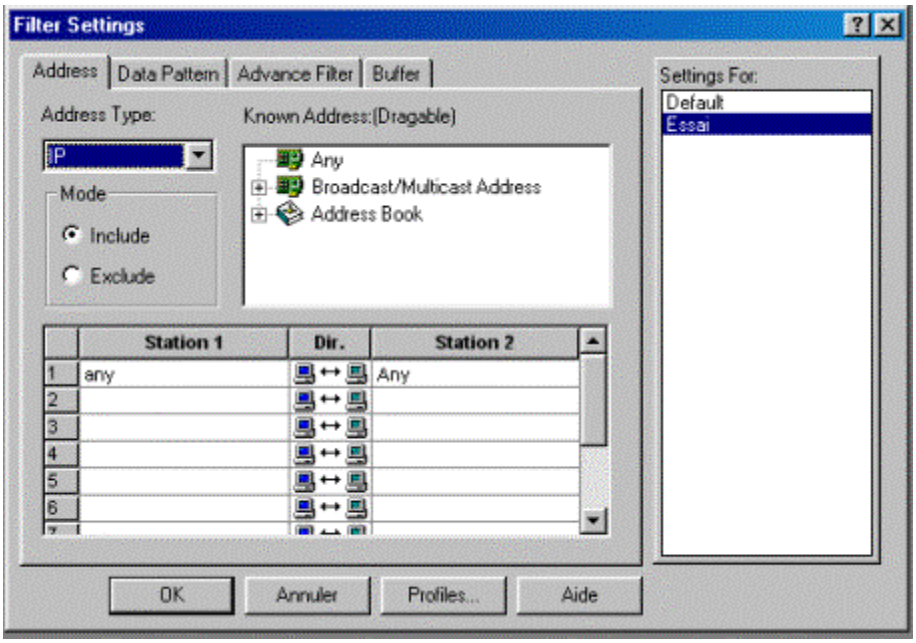
Pour régler les paramètres de la capture cliquez sur l’icône de la baguette magique  en haut à droite, puis sur Profiles et sur New et entrez un nom (exemple : Wagga IPX). Ensuite accédez au menu Advance Filter , faites dérouler la liste des filtres et sélectionner IPX.

Cliquez maintenant sur le bouton enregistrement  de la barre de Capture. Lorsque le nombre de paquets enregistrés vous parait suffisant cliquez sur le bouton Arrêt et Jumelles  , vous pouvez désormais visualiser les trames enregistrées.

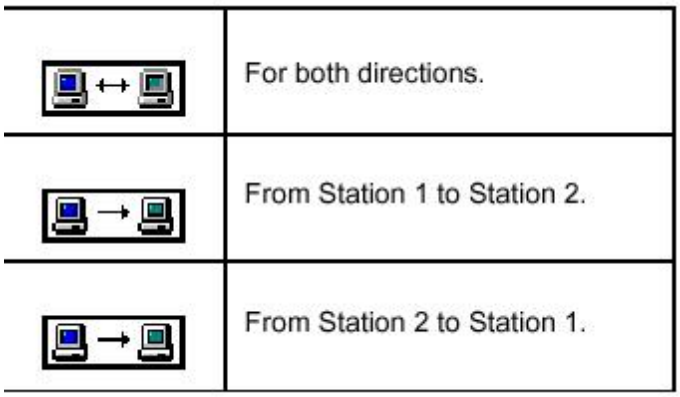


b) Capturer des paquets à l’aide des adresses IP :

Accéder aux paramètres de la capture et sélectionner Adress .



Entrez les adresses IP que vous désirez renifler, par exemple 192.48.53.2 sous Station 1 et 192.48.53.3 sous Station 2. Sélectionnez la direction dans laquelle vous souhaitez voir les trames, enregistrez les puis visionnez les.



.

Conclusion technique :

Pour réaliser ce projet nous avons commencé par des recherches sur les réseaux, les trames, les paquets, les adresses IP et MAC et bien d'autres choses … Puis nous avons installé le réseau sur deux ordinateurs, et le logiciel NetXRay. Le réseau ne fonctionnant pas correctement dans un premier temps nous avons cherché les causes de ce disfonctionnement.

Nous avons ensuite étudié la documentation du logiciel NetXRay et effectué des tests de capture de trames sur internet puis sur le réseau de l'IUT. Au fil des séances nous avons compris que le renifleur (sniffer) était bien plus qu'un logiciel servant au « Hacker » (pirate informatique) , effectivement le renifleur est avant tout un logiciel permettant le calibrage et la maintenance d'un réseau .

TP Sniffer

But du TP :

Le but de ce TP est de mieux comprendre les réseaux et ses protocoles, ainsi que d'analyser des trames à l'aide d'un renifleur (sniffer). Pour cela vous utiliserez deux ordinateurs en réseau munis du logiciel NetXRay et connectés à internet.

1) Pour commencer assurez-vous que le réseau fonctionne correctement, l'idéal est de le faire avec l'application Ping.

2) Rechercher les adresses IP des ordinateurs que vous utilisez (l'utilisation de la Matrix Statistic est recommandée).

3) Faites une capture de trames à l'aide des adresses IP, pour cela vous utiliserez le programme WinPopup (qui se trouve dans la racine de Windows) pour vous envoyer des messages.

4) Créer un compte messagerie sur Internet (Caramail, Hotmail …) vous pouvez également utiliser le votre.

Sélectionner un filtre TCP / IP / HTTP et « sniffez » votre login et un mot de passe.

5) Interprétez la trame ainsi filtrée.