TP : INFORMATIQUE INDUSTRIELLE N°11
MISE EN ŒUVRE ET ANALYSE DES PROTOCOLES INTERNET

MISE EN ŒUVRE ET ANALYSE DES PROTOCOLES INTERNET

1) But

Le but de ces travaux pratiques est d'étudier la mise en œuvre d'un réseau Ethernet mettant en œuvre les différents protocoles de l'Internet.

2) Objectifs

L'étudiant devra être capable :
- De décrire les differents protocoles utilisés pour acheminer l'information sur un réseau internet ou intranet
- De rechercher une éventuelle cause de disfonctionnement sur le réseau local et d'identifier l'élément en panne.

3) Présentation

On a vu lors du tp précédent les commandes simples MSDOS permettant de connaître la configuration d'un réseau et éventuellement déceler une panne. Cette méthode très statique ne permet pas de déterminer les différentes informations qui circulent sur le réseau. Un analyseur de trame réseau va nous permettre de déterminer au bit près les informations qui circulent sur le réseau. Ils existent des analyseurs de trame réseau matériel et d'autres logiciels qui sont couplés à une carte réseau. L'analyseur de protocoles SURVEYOR ou Wireshark sont des logiciels qui permettent d'analyser et "monitorer" les réseaux Ethernet 10/100 Mb/s. Pour l'utilisation de ce logiciel, on s'aidera de sa description simplifiée (voir fascicule en salle de TP) et des annexes de ce TP.

4) Questions

4.1) Configuration du réseau

Pour répondre à cette série de question se mettre en mode monitoring
pour lancer le monitoring cliquez sur le bouton lecture
4.1.1) double cliquez sur la fenètre du monitor
Analyser le flux des services IP en présence en cliquant sur le bouton Protocol distribution, notez les différents protocoles analysés sur le réseau.

4.1.2) Retrouver les adresses Ethernet des différentes machines connectées en cliquant sur le bouton Host Table.

4.1.3) Retrouver les adresses IP des différentes machines connectées en cliquant sur le bouton Network Layer Host Table. Notez ces différentes addresses IP du réseau

En utilisant une commande MSDOS faire le lien entre l'adresse IP de votre ordinateur et son nom NETBIOS.

4.2) Le protocole ARP

Lancer une capture et essayer d'obtenir une trame ARP d'un des ordinateurs du réseau, arrêter la capture.
Analyser le buffer de capture et décortiquer une trame ARP en la comparant à sa structure théorique donnée en annexe. Aux vues des trames capturées a-t-on dans la salle comme matériel des HUBs ou des switches, justifiez votre réponse.
Dans la trame ARP, Quelle est l'adresse Ethernet de broadcast qui est utilisée, retrouvez dans une des trames ARP, les adresses MAC IP source et destination?
Quel est le type de protocole utilisé dans une trame ARP.
Combien de trames type ARP sont envoyées sur le réseau, à partir de ces trames définir en quelques lignes comment s'effectue le dialogue sur le réseau entre les 2 ordinateurs

4.3) Le protocole ICMP

4.3.1) Lancer la capture. A partir d'une fenêtre MSDOS, faire un ping vers une machine du réseau. Arrêter la capture. On utilisera l'adresse IP de la machine pour le ping
Retrouver dans le buffer de capture les trames correspondant aux échanges ping.
Comparer la structure de la trame émise avec la structure théorique donnée en cours.
Quel est le type des trames ICMP émises, donnez leurs numéros ainsi que leurs appelations ?
A quoi correspond l'octet cheksum de la trame ICMP
Combien de trames sont échangées pour un ping ?

4.4) La couche application telnet

Analyse du flux telnet. Lancer la capture. Faire un telnet vers une cible OS9 (lors de la connexion, on prendra comme nom utilisateur super et comme mot de passe user). Arrêter la capture. Retrouver dans le buffer de capture les trames correspondant aux échanges telnet.
Quel est le protocole utilisé par les trames telnet?
Quel protocole de transport est utilisé ?
Déterminez la nature des 2 premiers segments TCP, Justifiez les 2 drapeaux trouvés.
Déterminez l'adresse IP de la cible OS9 ?
Préciser les numéros de port source et destination du protocole TCP.
Retrouver dans le flux de données la séquence d'échange username/passwd. Le mot de passe est-il crypté ?
Que peut-on dire sur la sécurité d'un réseau Internet ?

4.5) La couche application SSH

Analyse du flux telnet. Lancer la capture. Créez une session SSH vers une cible OS9 (lors de la connexion, on prendra comme nom utilisateur root et comme mot de passe root). Arrêter la capture. Retrouver dans le buffer de capture les trames correspondant aux échanges SSH.
Quel protocole de transport est utilisé ?
Préciser les numéros de port source et destination du protocole TCP.
Vérifiez les échanges de clés sous le protocole SSH?
Que peut-on dire sur la sécurité SSH ?

4.6) Le protocole FTP

4.5.1) Dans quelle couche du modèle OSI se trouve le protocole FTP ?
4.5.2) Lancez la capture se connecter dans un premier temps sur la cible OS9 grâce à l'utilitaire WSFTP32.). Arrêter la capture et Retrouver dans le buffer de capture les trames correspondant aux échanges ftp.
Quel protocole de la couche application du modèle OSI retrouve t'on dans le dialogue cible OS9 PC ?
Quel est le port destination et source dans la trame ftp ?
La valeur du port source est elle normale (voir cours) ?
Donnez le nom ainsi que le mot de passe utilisés lors de la connexion ?
Donnez dans les trames ftp (fenètre, file transport protocol control de surveyor) les différentes requêtes ftp échangé entre le pc et la cible OS9. Sous quel format sont envoyés les requêtes valeurs hexadécimals ou ASCII.
4.5.3) lancez la capture et envoyé un fichier texte assez conséquent vers la cible OS9. Arrêter la capture et Retrouver dans le buffer de capture les trames correspondant aux échanges ftp.
Comment sont appelées par surveyor web demo les trames ftp qui vont permettre de transférer le fichier ?
Quelle est la taille maximale d'une trame ftp ?

4.7) Le protocole HTTP

Un serveur HTTP noté (PIC SERVEUR WEB) connecté au réseau local de la salle permet de fournir des informations sous forme de page WEB. L'adresse IP de ce serveur est **192.9.200.xxx,** un simple navigateur (internet exploreur) sur le PC nous permet de récupérer ces pages WEBs. Utilisez un filtrage de trame du type bidirectionnel entre l'adresse IP de votre PC et l'adresse IP du serveur (voir dossier annexe)

4.7.1) Lancement de la capture

lancez la capture
Ouvrir internet explorer et dans la zone de navigation tapez l'adresse suivante: http://192.9.200.221 et appuyez sur entrée, arrêter la capture
Observez les 3 premières trames TCP capturées et en analysant l'adresse IP source, l'adresse IP de destination, le champ flag de la couche transport décrire le rôle des ces 3 premières

trames.
En analysant la première trame HTTP reçu et notamment le champ de données quel est le rôle de cette première trame ? Quel est le port source et de destination?
En analysant la deuxième trame HTTP reçu et notamment le champ de données quel est le rôle de cette deuxième trame,
Faites le lien entre la page WEB que vous observez sur internet explorer et le champ de données de cette deuxième trame. Comment s'appelle le langage utilisé pour formater les pages WEB ?

4.7.2) Navigation

Amenez le curseur de la souris sur la rubrique analogique et observez en bas d'internet exploreur le nom de la page qui doit s'ouvrir, Quelle est ce nom?
Lancez la capture et cliquez sur analogique dans la page WEB, arrêtez la capture.
Observez sur SURVEYOR la trame HTTP qui envoie une requête au serveur permettant de rapatrier cette page WEB.
Observez la réponse du serveur WEB. Sur internet exploreur amenez le curseur de la souris sur la rubrique analogique cliquez droit et faites ouvrir dans une nouvelle fenêtre puis allez dans le menu affichage source, le code obtenu est il identique à celui qui circule sur les tramesHTTP ?

4.7.3) Interaction

lancez une capture et cliquez sous internet exploreur sur l'image de l'interrupteur de gauche arrêtez la capture vérifiez sur la carte du pic web serveur que le LED LD a changé d'état (en cliquant sur le bouton votre PC, (le client) demande au serveur de rapatrier la page WEB digout.htm). Observez la réponse du serveur dans les trames capturées, comment s'appelle l'image de l'interrupteur baissé et l'image de la LED allumée.

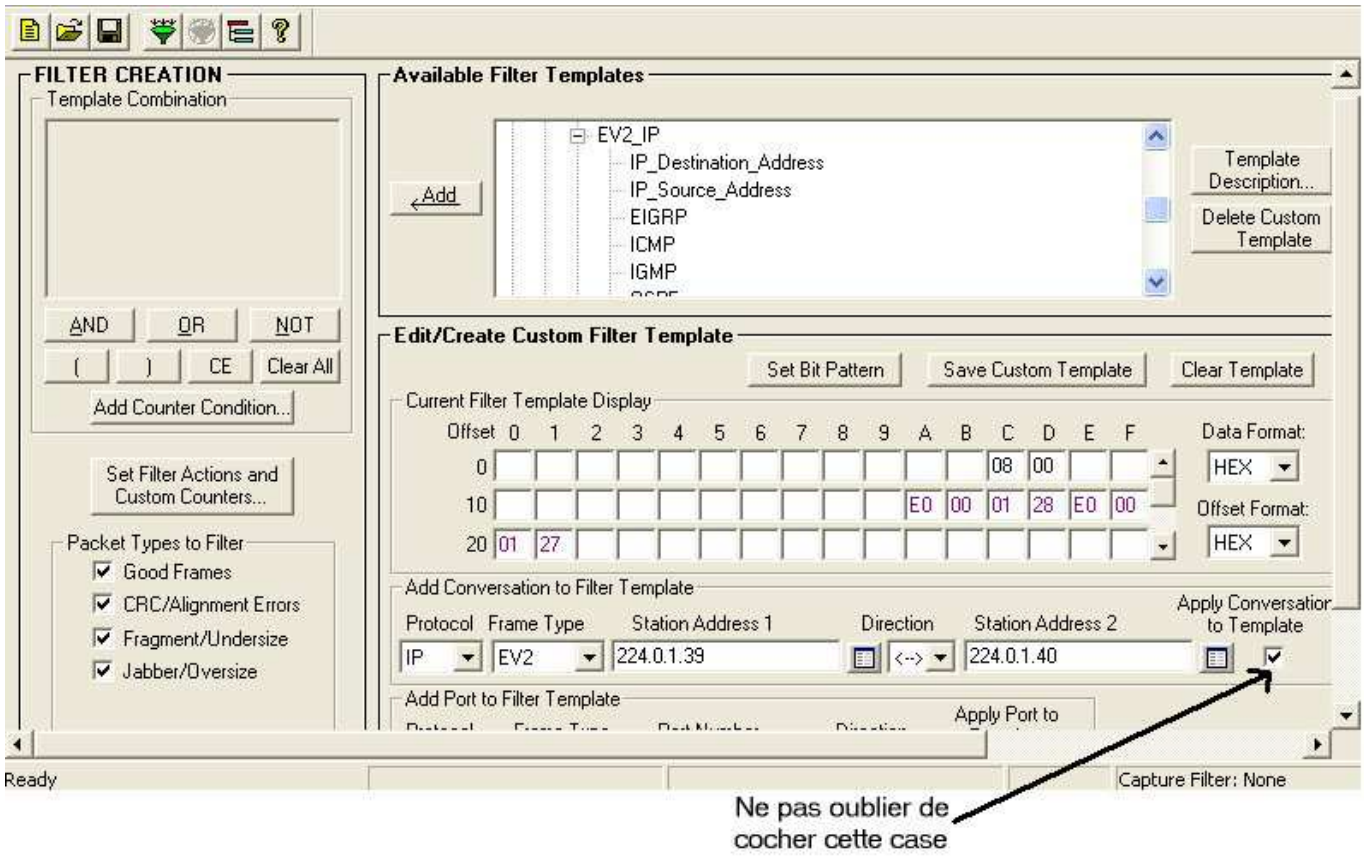
Annexe : Filtrage d'une trame réseau

1) Introduction

Il est souvent nécessaire de capturer les trames qui nous intèresse sur le réseau. En effet avec un trafic très dense sur le réseau ,beaucoup d'informations circulent. On doit alors filtrer les trames reçues ou envoyées par notre ordinateur.

2) Méthodes

sélectionnez dans le menu module → capture filter → create modify/capture filter
Choisir dans la fenètre avaible filter template les options suivantes:
Ethernet → EV2 → EV2_IP (pour filtrer les trames avec un protocole TCP-IP sur un réseau du type ethernet).
Ethernet → EV2 → MAC →ARP (pour filtrer les trames ARP sur un réseau du type ethernet).
Rentrez dans la case station adress 1 l'adresse IP de votre ordinateur.
Rentrez dans la case station adress 2 l'adresse IP de l'ordinateur distant qui communique avec votre ordinateur.
N'oubliez pas de cochez apply conversation template.



Cliquez sur save custom template choisir un nom pour ce type de filtrage. Le template apparaît alors dans la fenêtre avaible filtre template



Choisir le template puis cliquez sur ADD
Pour activer ce nouveau filtre cliquez sur l'icône suivante.



Lancez la capture et analyser les trames que vous avez filtré.

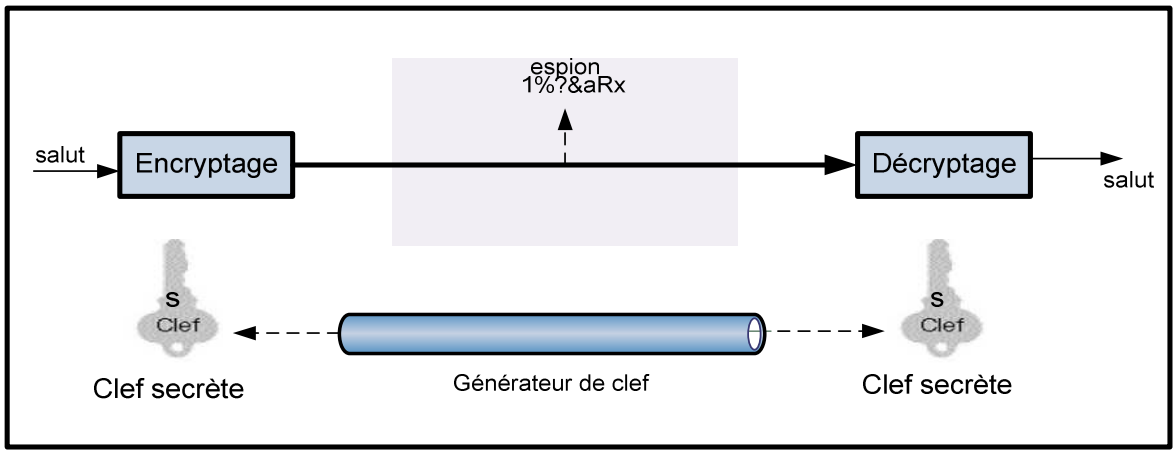
Rappel : Le cryptage de l'information

Le cryptage permet d'assurer :

- La **Confidentialité** des informations
- L'**Intégrité** des données en s'assurant que l'information n'a pas subi de modification et **l'authentification** afin de vérifier que le message correspond bien à l'expéditeur.

1) Cryptographie à clé secrète (chiffrement symétrique)

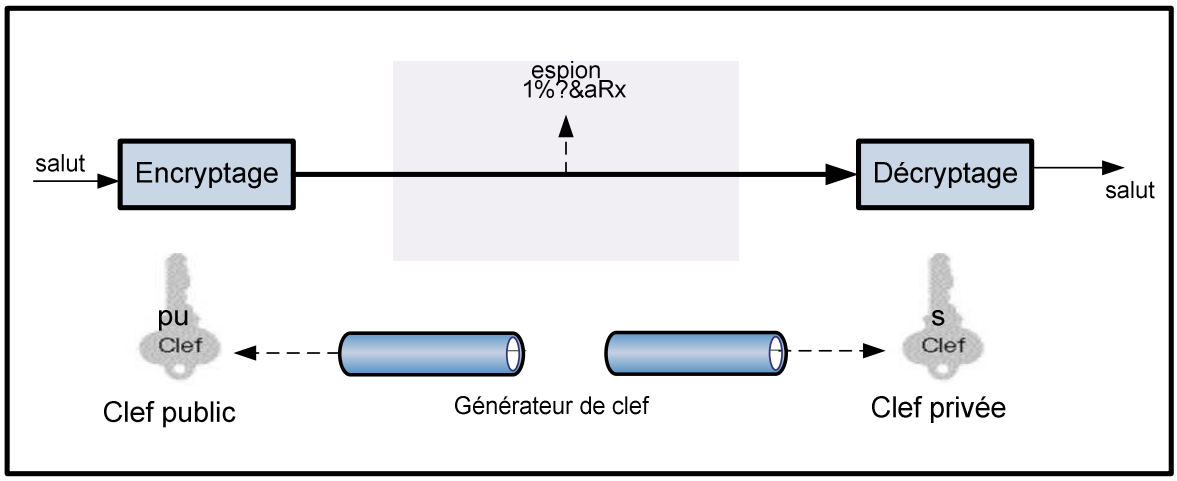
On utilise une clef secrète commune aux 2 systèmes qui veulent communiquer ensemble. Les algorithmes symétriques actuels sont nettement plus rapides que les algorithmes asymétriques. Une clef symétrique est toutefois potentiellement peu sûre. Il suffit qu'un individu nuisible se procure la clé secrète et il n'y a plus d'information protégée. La clef symétrique doit donc être transmise au correspondant sans être interceptée.



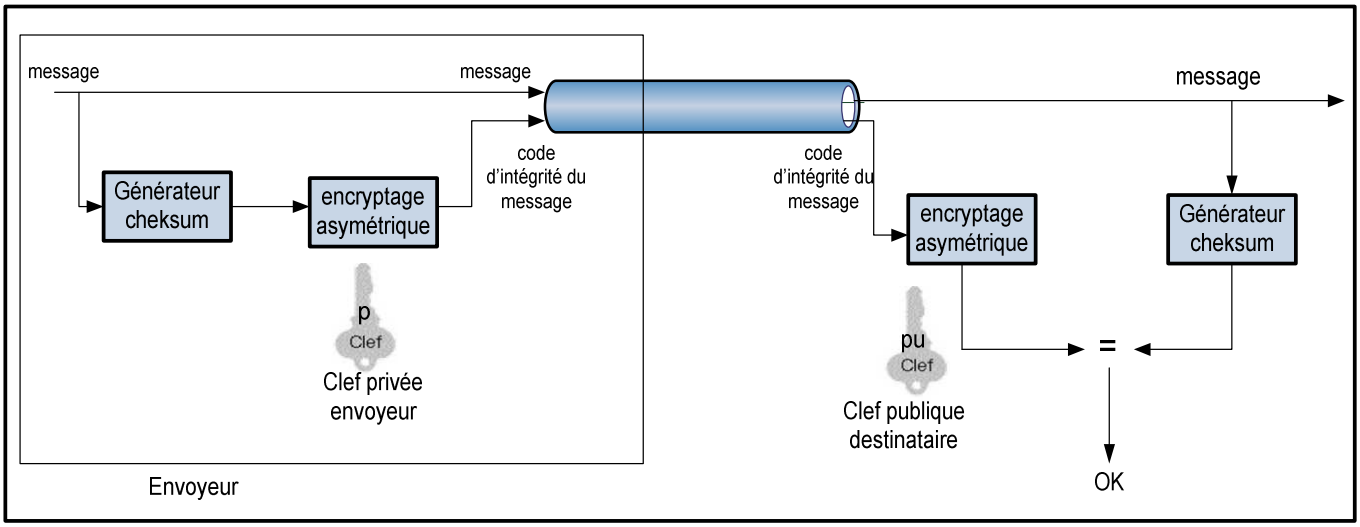
Les algorithmes de cryptage symétriques les plus répandus sont le **DES et le 3DES**

2) Cryptographie à clé publique (chiffrement asymétrique)

Le chiffrement à base de clef publique garantit qu'une donnée chiffrée par une clef, **publique ou privée**, ne peut être déchiffrée que par la clef associée. Les clefs sont de même nature et leurs rôles peuvent être inversés : ce que l'une chiffre est déchiffrable par l'autre. La paire de clef repose sur des nombres premiers.
L'astuce consiste à conserver une clef secrète (la clef privée) et à distribuer l'autre clef (la clef publique) à tout le monde. N'importe qui peut vous envoyer un message chiffré mais personne d'autre que vous ne peut le déchiffrer tant que vous êtes le seul à conserver un des deux membres de la paire de clefs.

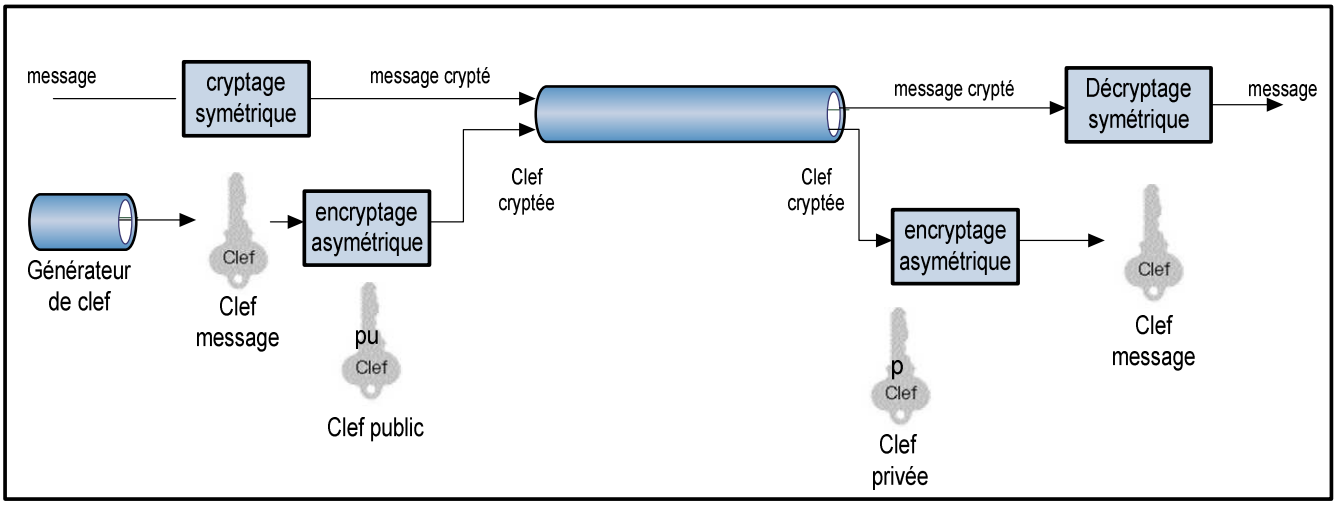


La signature d'un message consiste à associer une identité à son contenu. L'identité du message est représentée par une suite binaire que l'on appelle le checksum. On applique le message à l'entrée d'une fonction de hachage qui fournit en sortie un résultat appelé checksum. Le checksum est ensuite cryptée par la clef privée. Le destinataire de l'ensemble (message + code d'intégrité) recalcule le haché ou le checksum et le compare au résultat du déchiffrement de la signature ou code d'intégrité avec la clef publique.



3) La solution mixte (SSL)

On utilise un système asymétrique (comme **RSA** ou **Diffie-Hellman**) pour crypter les clés de Message. Ces clés de message permettront de chiffrer le message grâce à un chiffrement symétrique (DES, 3DES, IDEA, RC4…).



Rappel:

Netbeui/netbios : créé par microsoft, c'est un protocole de bas niveau de performances, il permet un bon fonctionnement au niveau des réseaux locaux. Il ne permet pas le routage et ne sait gérer que le nom des ordinateurs ainsi que les ressources partagés.
IPX/SPX créé par netware pour les réseaux novell, il représente une protocole intéressant puisqu'il permet l'interconnexion d'un réseau mondiale sous la forme d'une base de donnée unique appelée NDS, mais lil ne garantit pas l'homogénéité qu'offre TCPIP
TCP-IP: née en 1980 et crée par la défense américaine, TCPIP représente la particularité d'avoir une architecture en 3 couches transport, routage liaison. Son protocole n'est pas conforme au norme recommandé par l'OSI mais les fonctionnalités sont proches. En fait il se su

Format d'une trame ARP :

