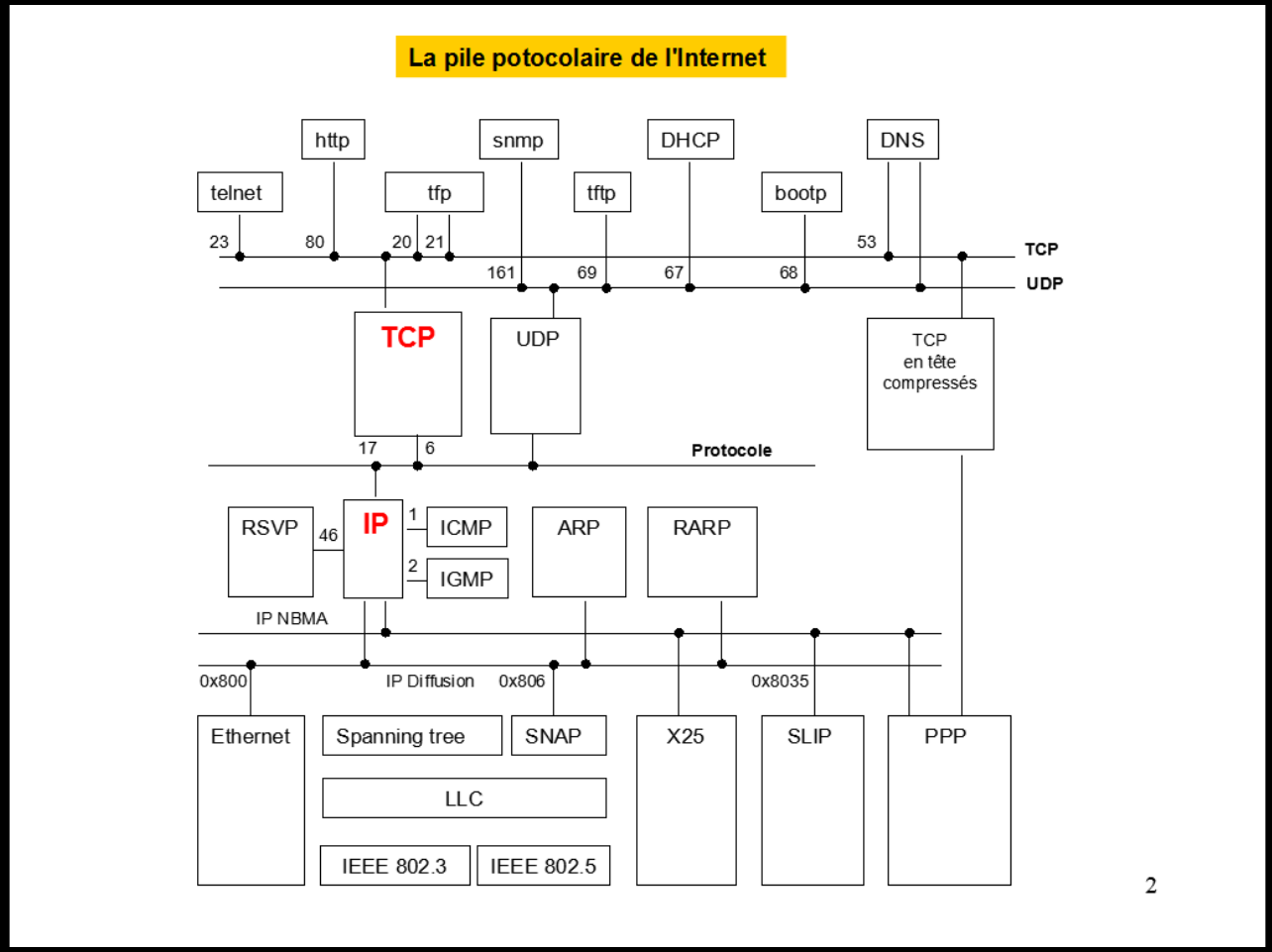
Université de M'sila
Faculté des Mathématiques et de l'Informatique
Département d'informatique
Spécialité: Master RTIC

Cours7:Attaques Informatique -2-

Université de M'sila
Département del'informatique :2021-2022
Niveau : master2
Préparé et présenté par: SAOUDI Lalia

Rappel sur le protocole TCP



Les Protocoles de transport

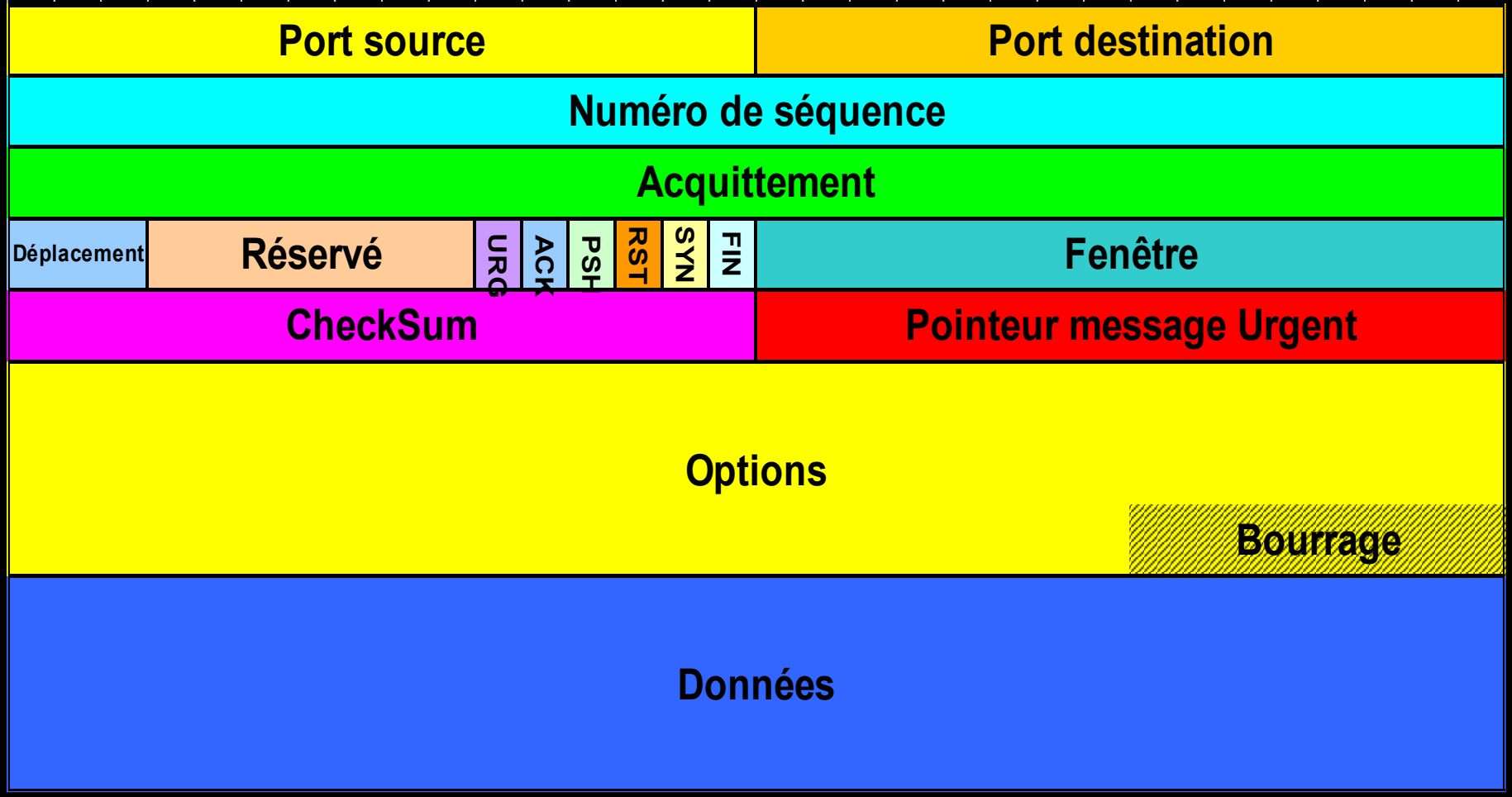
On trouve typiquement au dessus du protocole IP (couche réseau - 3), les protocoles de transport (couche 4) suivants :Couche transport

- UDP
  - Non connecté
  - Rapide
  - Aucune garantie
- TCP
  - Connecté
  - Messages remis dans le bon ordre
  - Aucun message perdu
  - Aucun message abîmé

Les Protocoles de transport

- Caractéristiques du protocole TCP
  - Un contrôle des données transférées (données endommagées, perdues et/ou dupliquées) et un reséquencement si la couche IP ne les délivre pas dans l'ordre.
  - Un niveau de priorité. Les données transmises dans un message peuvent être traitées avec plus ou moins de priorité.

LE MESSAGE TCP



LE MESSAGE TCP

- **Port Source - Port Destination**
- L'adresse IP, au niveau 3, permet de situer une machine.
- Une fois la machine trouvée, il faut pouvoir déterminer l'application qui doit traiter les données.
- L'application est désignée par un NUMERO DE PORT.
- Numéro sur 16 bits (0 - 65535)
- Deux classes de ports
  - 0 - 1023 : Ports réservés
    « well known ports» www.iana.org/assignments/port-numbers
  - 1024 - 65535 : Ports libres (ou presque)
    - Pas d'utilisation précise (quoique…)
    - Souvent alloués à la demande, par l'O.S.

LE MESSAGE TCP

Les Ports

TCP : ports standards

No port	Mot-clé	Description
20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
79	FINGER	Finger
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3
111	SUNRPC	SUN Remote Procedure Call

LE MESSAGE TCP

- Champ des bits de contrôle (Flag)

6 Bits pour définir la fonction des message et la validité de certains champs :

URG : Message urgent - Les données doivent être traitées sans attendre que le récepteur ait traité les octets envoyés dans le flux.

ACK : Indique la validité du champ acquittement.

PSH : Les données reçues doivent être immédiatement remises à la couche supérieure.

RST (Reset) : Réinitialisation de la connexion suite à une erreur irrécupérable.

SYN : Indique l'ouverture d'une connexion.

FIN : Fermeture normale d'une connexion

LA CONNEXION TCP

- Gestion d'une connexion TCP

  Les champs numéro de séquence, acquittement et flags sont utilisés par le protocole TCP à gérer la communication de bout en bout (couche 4)

LA CONNEXION TCP

Une application qui appelle le module

TCP utilise les appels systèmes suivants :

- OPEN pour ouvrir la connexion. On distingue :
  - OPEN PASSIF qui est un open type serveur. Il reste à l'écoute et accepte les requêtes qui lui arrive.
  - OPEN ACTIF qui est un open type client qui après une connexion sur un open passif enverra des données.
- CLOSE pour fermer la connexion
- SEND pour envoyer les données après un OPEN
- RECEIVE pour recevoir des données
- STATUS pour obtenir des informations sur la connexion.

Three Way handshake

- L'ouverture d'un connexion TCP se négocie en 3 temps à l'aide des flags SYN et ACK :

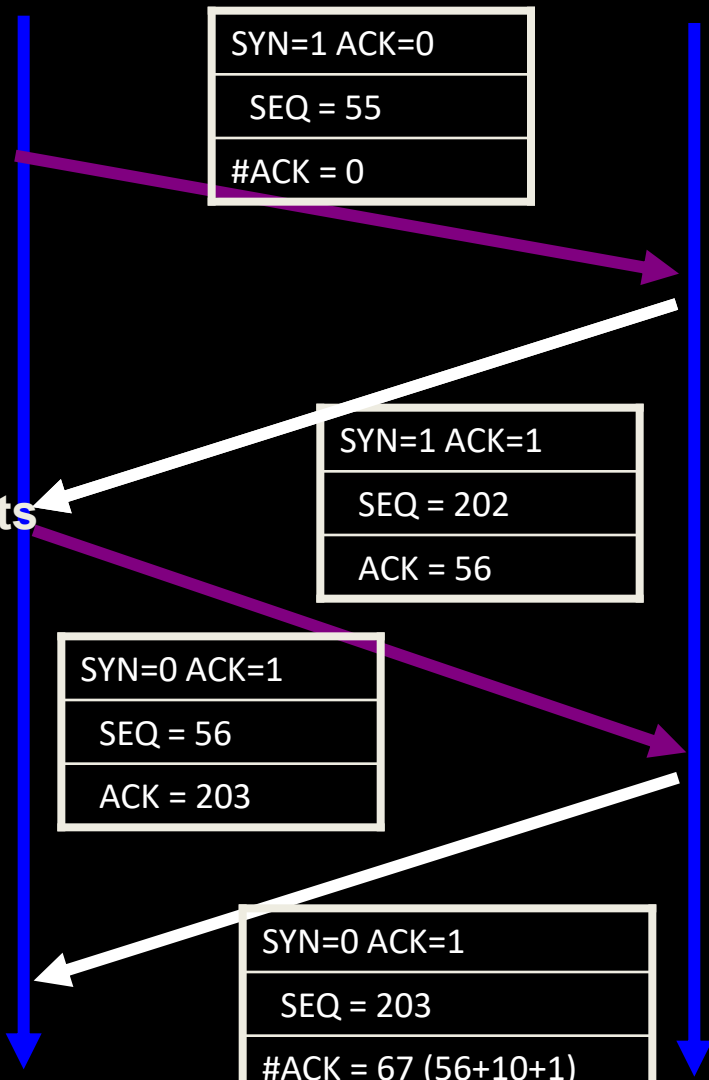
SYN = 1	ACK = 0	Demande d'ouverture
SYN = 1	ACK = 1	Acceptation de l'ouverture
SYN = 0	ACK = 1	Données

LA CONNEXION TCP

- Le contrôle de flux se fait à l'aide des champs numéro de séquence (noté #SEQ) et acquittement (noté #ACK). La valeur initiale de #SEQ est produite à partir d'une horloge et d'un compteur incrémenté toutes les 4 ms. Il permet de numéroter les octets de données.
- Avec ces éléments un schéma d'une connexion TCP sera le suivant :

LA CONNEXION TCP

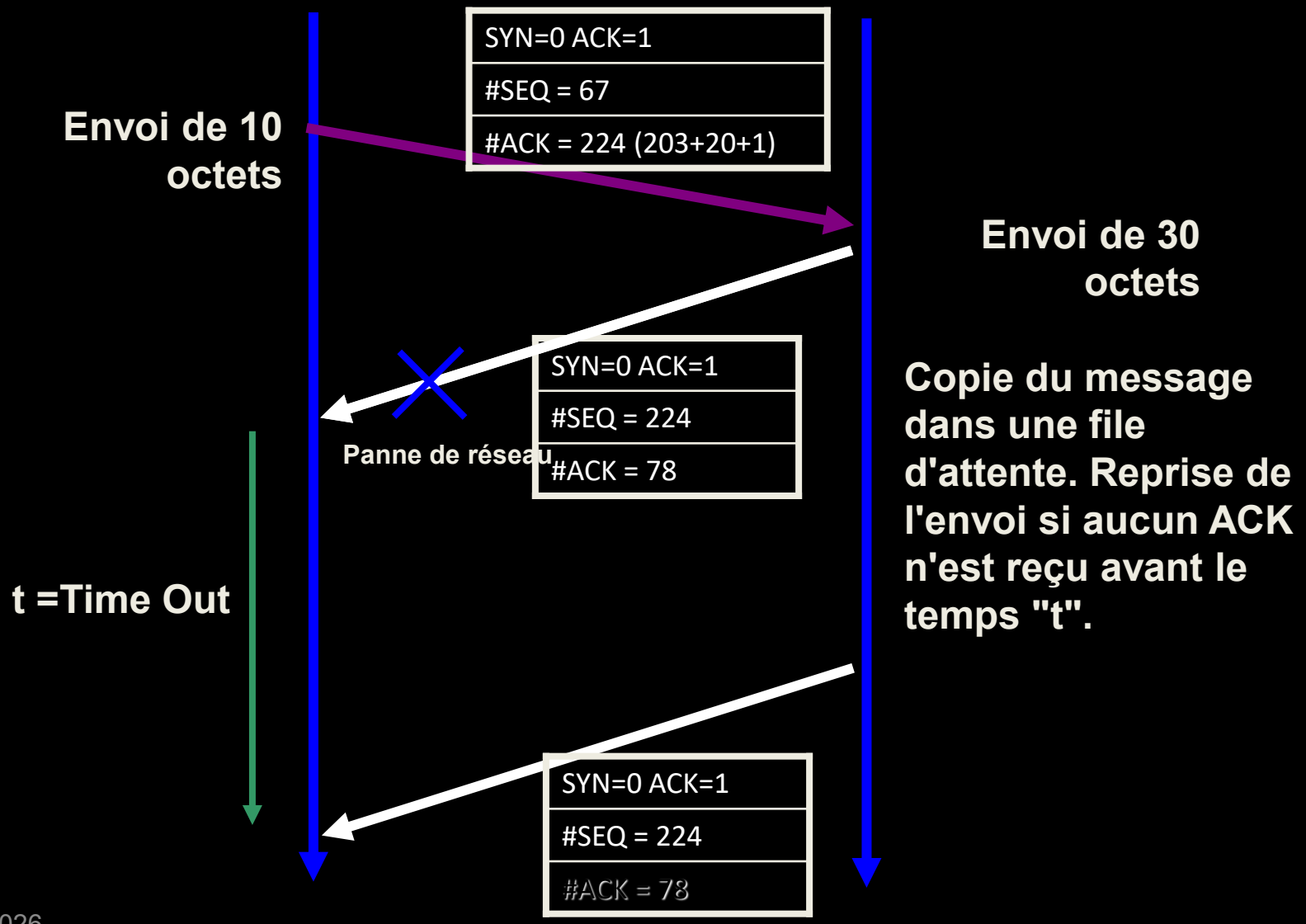
ACTIVE OPEN
Demande d'ouverture de connexion par le client



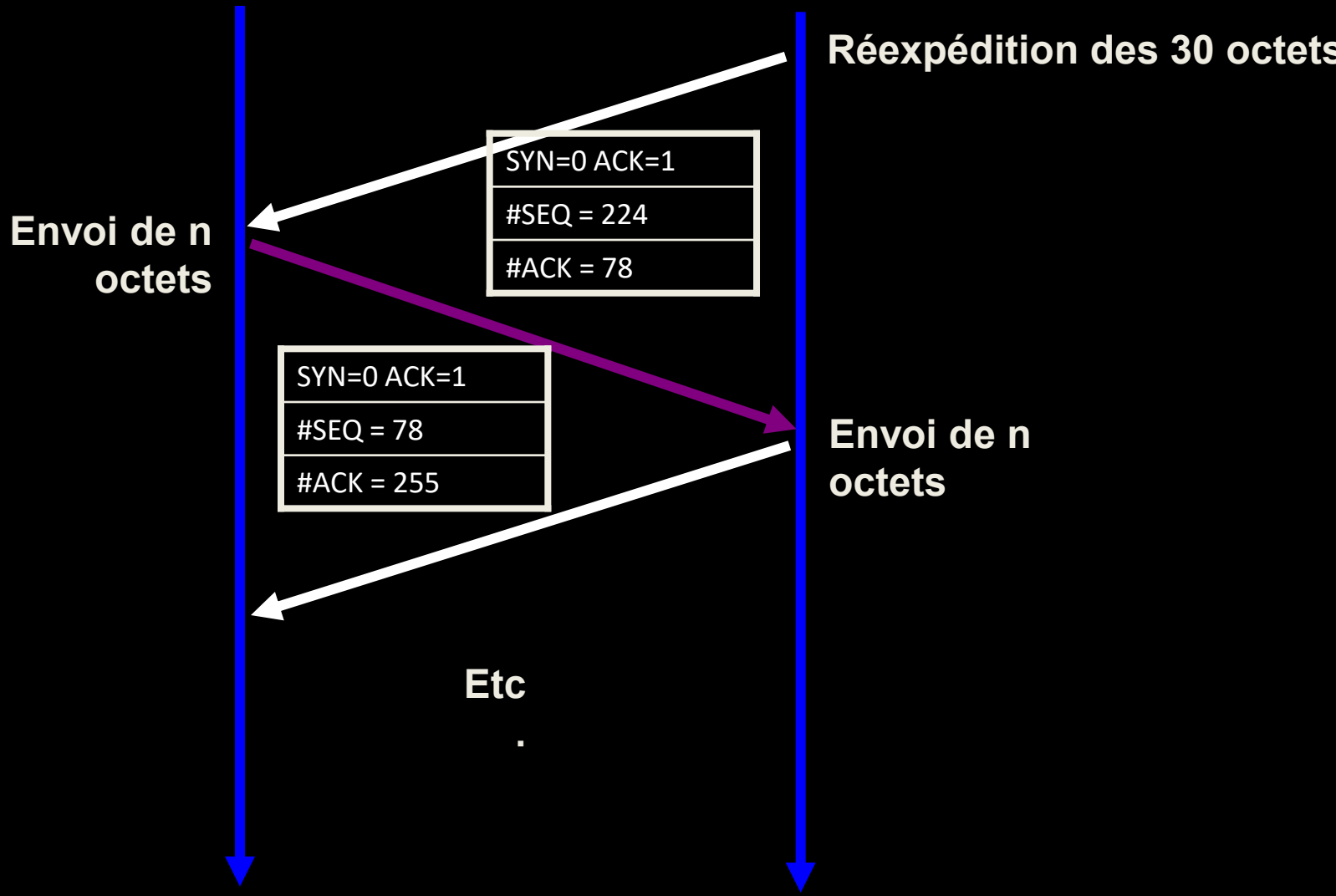
Quand SYN=0 et ACK=1 :

- **#SEQ reprend le #ACK reçu**
- **#ACK = #SEQ reçu + Nombre d'octets reçu + 1**
- **#ACK donne le numéro du prochain octet**

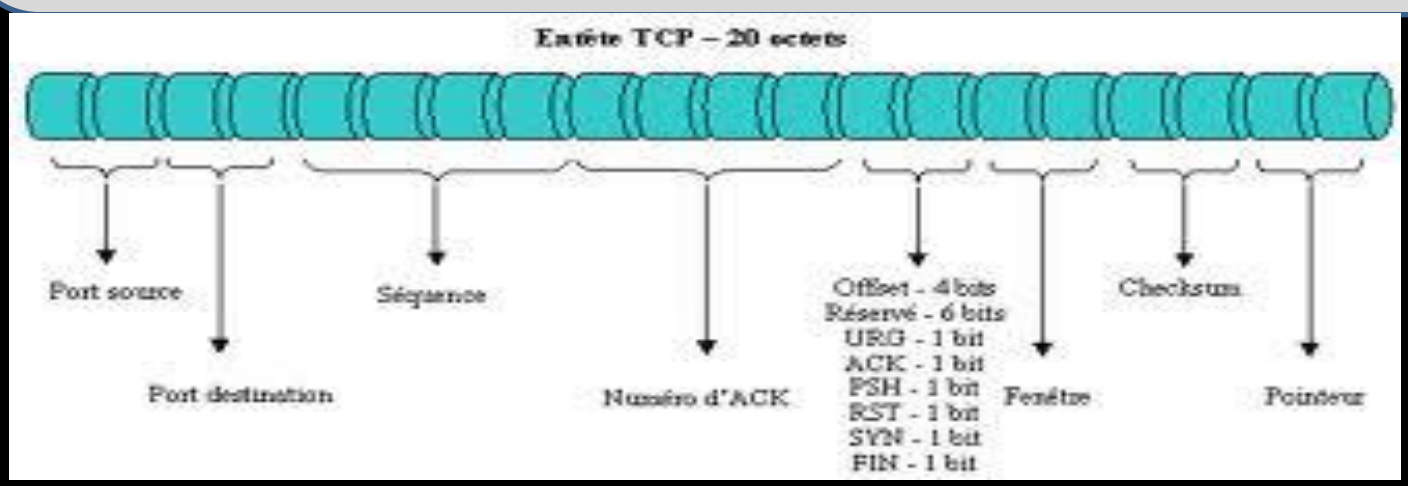
LA CONNEXION TCP

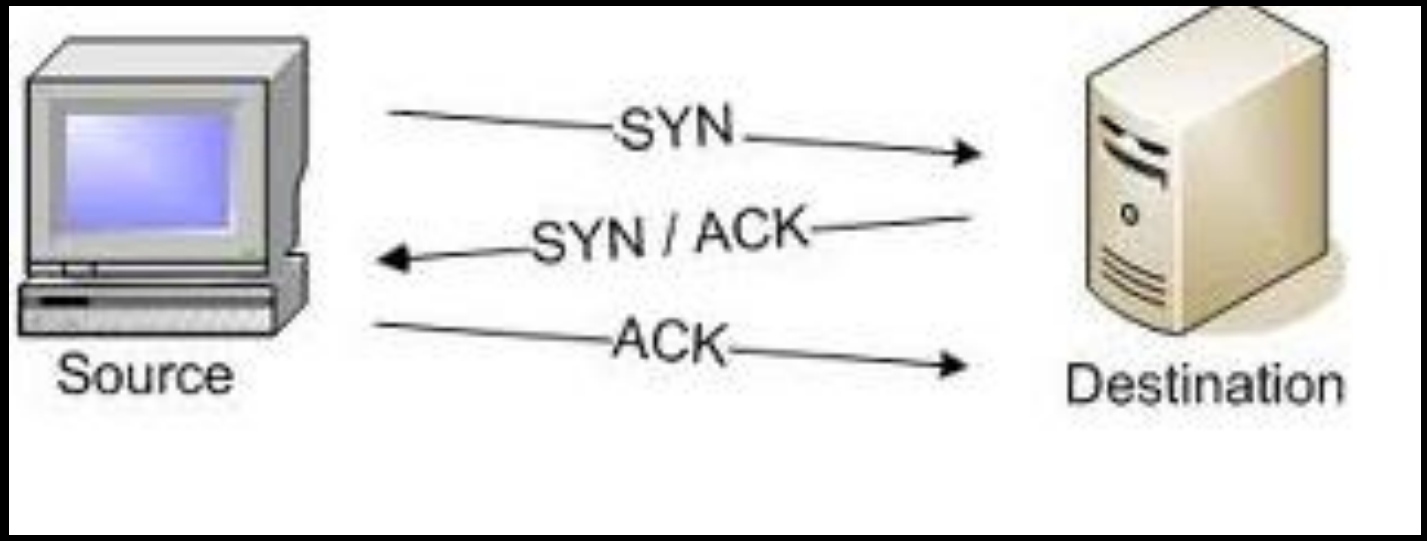


LA CONNEXION TCP



session TCP


Entête TCP – 20 octets
Port source
Port destination
Séquence
Numéro d'ACK
Offset - 4 bits
Réservé - 6 bits
URG - 1 bit
ACK - 1 bit
PSH - 1 bit
RST - 1 bit
SYN - 1 bit
FIN - 1 bit
Fenêtre
Checksum
Pointeur


SYN
SYN / ACK
ACK
Source
Destination

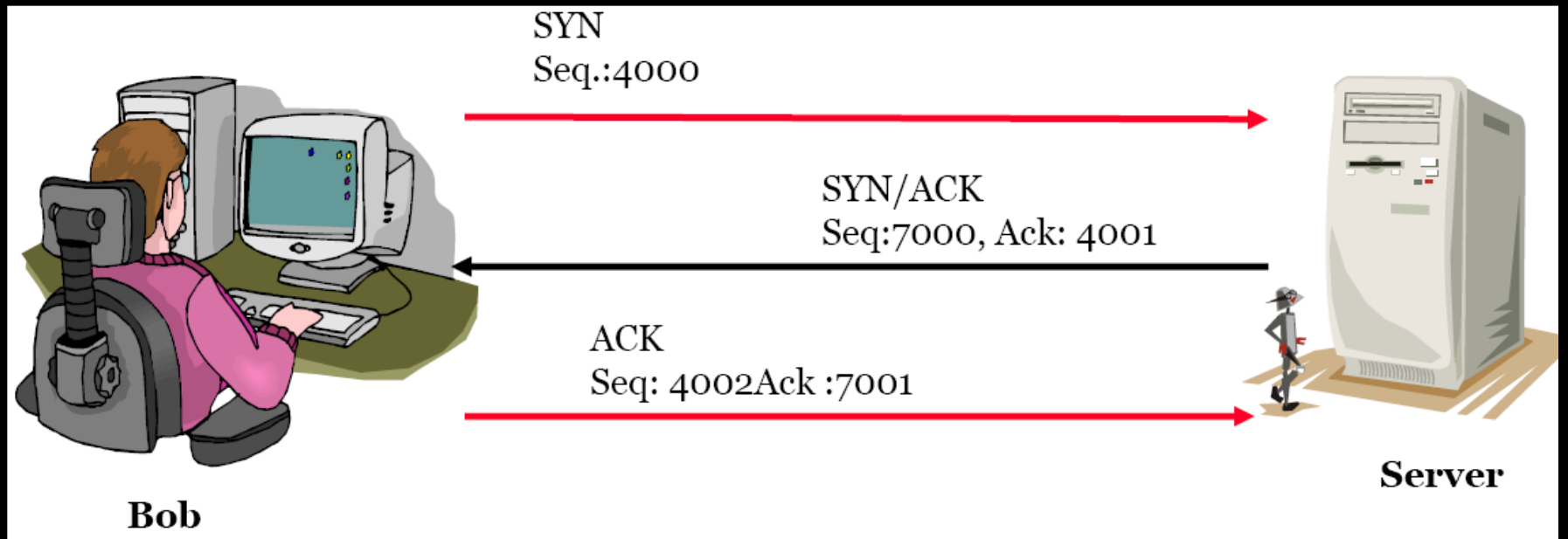
I. Le vol de session (TCP)

L'attaque se déroule de la façon suivante :

1. Le pirate essaye de prévoir le numéro de séquence des paquets du serveur cible envoyant plusieurs paquets et en analysant l'algorithme d'incrémentation de ce numéro.
2. Le pirate rend inopérante la machine A autorisée à accéder au serveur cible, de façon à s'assurer qu'elle ne répond pas au serveur cible.
3. Le pirate falsifie son adresse IP en la remplaçant par celle de la machine invalidée et envoie une demande de connexion au serveur cible.
4. Le serveur envoie une trame SYN|ACK à la machine qu'il pense être l'émettrice.
5. Celle-ci ne pouvant répondre, le pirate acquitte cette connexion par une trame ACK, avec le numéro de séquence prévu. Il établit de la sorte en toute impunité la connexion avec le serveur cible.

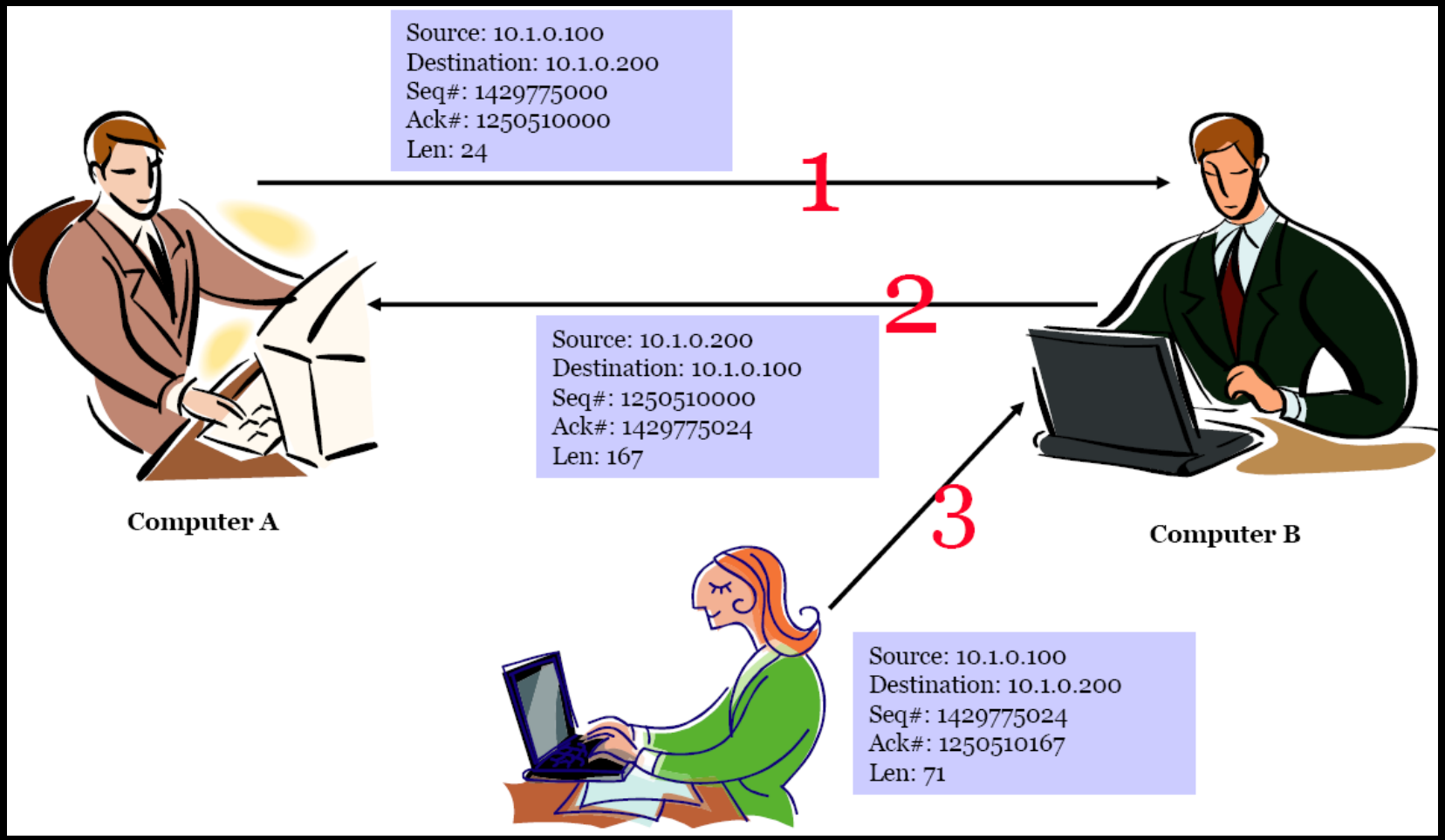
Remarque: L'IP spoofing est une menace moins importante aujourd'hui en raison des patches de sécurité appliqués

1.Le vol de session (TCP)



If the attacker can anticipate the next SEQ/ACK number Bob will send, he will spoof Bob's address and start a communication with the server

1.Le vol de session (TCP)



1.Le vol de session (TCP)

Cas1:
Cas où le pirate est sur le même réseau que la station de confiance

1. Pirate intercepte les paquets échangés
2. Pirate rend la station de confiance inopérante pour qu'elle ne réponde pas au Serveur
3. Pirate => Serveur: ACK (IP Confiance)

1.Le vol de session (TCP)

Cas2:

Cas où le pirate n'est pas sur le même réseau que la station de confiance

1. Le pirate ne pourra pas écouter les paquets ne pourra donc pas connaître l'ISN envoyé par le .serveur.

2. Le pirate cherche à deviner le prochain ISN du serveur et répondre avec ACK avec le bon numéro : le pirate ouvre quelques connexions légitimes. Pour déduire l'algorithme de génération de ISN ,Si l'algorithme est simple, il pourra deviner le prochain ISN.

II.Attaques permettant de mettre le réseau en déni de service

- Le déni de service, ou DoS (Denial of Service), est une attaque qui vise à rendre indisponible un service, un système ou un réseau.
- Il y a trois catégories de DOS :
  - **Attaque de vulnérabilité** : Cela implique l'envoi de quelques messages bien conçus à une application ou à un système d'exploitation vulnérable pour arrêter le service ciblé ou, pire, l'hôte peut tomber en panne.
  - **Inondation de bande passante** : cette attaque est basée sur l'envoi massif de paquets de bande passante élevée, ou sur d'autres flux répétitifs de paquets., empêchant les paquets légitimes d'atteindre le serveur.
  - **Inondation de connexion TCP**: l'attaquant établit un grand nombre de connexions TCP semi-ouvertes ou entièrement ouvertes sur l'hôte cible, Les adresses source et les ports TCP source des paquets de demande de connexion sont randomisés. L'objectif est de forcer l'hôte cible à conserver les informations d'état pour de nombreuses connexions qui ne sont jamais terminées.

II.1.Attaque par inondation

- **principe de fonctionnement :**
- Une ou plusieurs machines inondent le réseau avec des paquets réseau afin de saturer la bande passante de celui-ci.
- Une fois que toute la bande est occupée, les autres machines ne peuvent plus travailler, ce qui génère une situation de déni de service.
- La plupart du temps, le protocole utilisé pour inonder un système ou un réseau est ICMP.

Pourquoi ICMP.

- contrairement aux protocoles TCP et UDP par exemple, un équipement branché sur le réseau doit toujours analyser les paquets ICMP car ceux-ci demandent souvent une réponse particulière de sa part.
- Afin de tester le comportement d'un lien saturé, les systèmes d'exploitation disposent d'une commande ping avec l'option d'inondation .
- Inonder une victime semble donc techniquement très simple, surtout si le pirate dispose de plus de bande passante que sa victime. Mais sinon, d'autres moyens existent.
- ping iphere -l 65000 –t
- -t :Pings the specified host until stopped.
- -l sizeSend buffer size.

II.2.Attaques smurf et fraggle par amplification de l'inondation

- Les attaques smurf et fraggle sont des variantes de la précédente qui s'appuient sur une faiblesse de configuration des routeurs.
- Ces techniques consistent à inonder le réseau avec des ping qui n'utilisent que des adresses de broadcast.
- Pour un paquet envoyé, toutes les machines d'un réseau répondent, ce qui augmente la saturation du réseau.
- Du fait de l'envoi des paquets ICMP avec une fausse adresse source vers une adresse de broadcast, chaque machine appartenant au réseau couvert par le broadcast répond aux systèmes victimes ou aux systèmes fictifs.
- La différence entre l'attaque smurf et l'attaque fraggle est que cette dernière utilise le protocole UDP.

II.2.Attaques smurf et fraggle par amplification de l'inondation

- **Parades à Smurf:**
- **la fonctionnalité de diffusion ciblée doit être désactivée au niveau du routeur frontière. Avec les routeurs Cisco, entrez la commande suivante : no ip directed-broadcast**
- **À partir de la version 12 de Cisco IOS, cette fonctionnalité est activée par défaut.**

II.3.Attaque par inondation SYN

- La technique d'inondation SYN est identique à celle du balayage SYN, à la différence près qu'elle est utilisée à des fins de déni de service.
- le principe du balayage semi-ouvert consistait à ce que le client ne termine pas la session TCP .
- Dans cet état, le serveur doit réserver des ressources (réseau, mémoire,CPU, etc.) pour le traitement de la session TCP et attendre la fin du handshake.
- Tous les serveurs supportent un nombre maximal de sessions TCP en cours.
  - Lorsqu'une session est terminée, les ressources associées à la session sont remises à disposition du système d'exploitation.
  - Lorsque la session n'est pas encore établie, le système prend la peine de faire patienter les paquets manquants, estimant qu'ils sont simplement retardés par le réseau. Ce délai d'attente pour passer les différents états de libération de la session est paramétrable mais prend généralement une bonne minute.
- L'envoi de paquets SYN par un pirate vers un serveur, une opération très rapide puisque le pirate n'attend pas de réponse de celui-ci, engendre une saturation des ressources réseau de la victime, laquelle ne peut plus dès lors assurer sa mission.
- Cette attaque est furtive : les pirates falsifient l'adresse source du paquet SYN, ce qui complique singulièrement l'identification du coupable.

II.3.Parades aux inondations SYN

- **Pour déterminer si vous faites l'objet d'une telle attaque, utilisez la commande netstat -na si elle est acceptée par votre système d'exploitation. Si vous trouvez un grand nombre de connexions dans l'état SYN_RECV, une attaque SYN est probablement en cours.**
- **Nous vous proposons ci-dessous quatre solutions de base contre les attaques par inondation SYN.**
  - Allongement de la longueur de la file d'attente des connexions .
  - Réduction de la durée de temporisation d'établissement d'une connexion ,
  - Application de correctifs logiciels fournis par les éditeurs pour détecter et contrecarrer d'éventuelles attaques par inondation SYN
  - Utilisation d'un IDS de réseau .

II.4.Attaques sur les bogues des piles IP/TCP

- Les principales attaques qui s'appuient sur les erreurs de programmation associées aux piles TCP/IP sont:
  - le ping de la mort, le baiser de la mort, le win nuke, l'attaque land et l'attaque teardrop.

.le ping de la r[illegible]t- Ping of death

- Un ping a normalement une longueur maximale de 65535 ((2 exp 16) - 1) octets, incluant une entête de 20 octets. Un ping of death c'est un ping qui a une longueur de données supérieure à la taille maximale. Lors de son envoi, le ping of death est fragmenté en packets plus petits. L'ordinateur victime qui reçoit ces packets doit alors les reconstruirent. Certains systèmes ne gèrent pas cette fragmentation, et se bloquent, ou crashent complètement. D'où le nom de cette attaque.
- Comment s'en protéger ?

  Mettre à jour l'OS.

  Effectuer un test avant que quelqu'un d'autre le fasse à votre place. Si le système réagit correctement, il n'y a pas de problème.

II.5.L’attaque de type land

- L’attaque de type land demande une ouverture de session TCP avec l’adresse source du paquet égale à l’adresse destination et le port source égal au port destinataire.
- Cette attaque utilise principalement le port 139 TCP (NetBIOS Session) afin de viser le système d’exploitation Windows. L’impact de l’attaque peut provoquer des comportements indésirables du système cible.

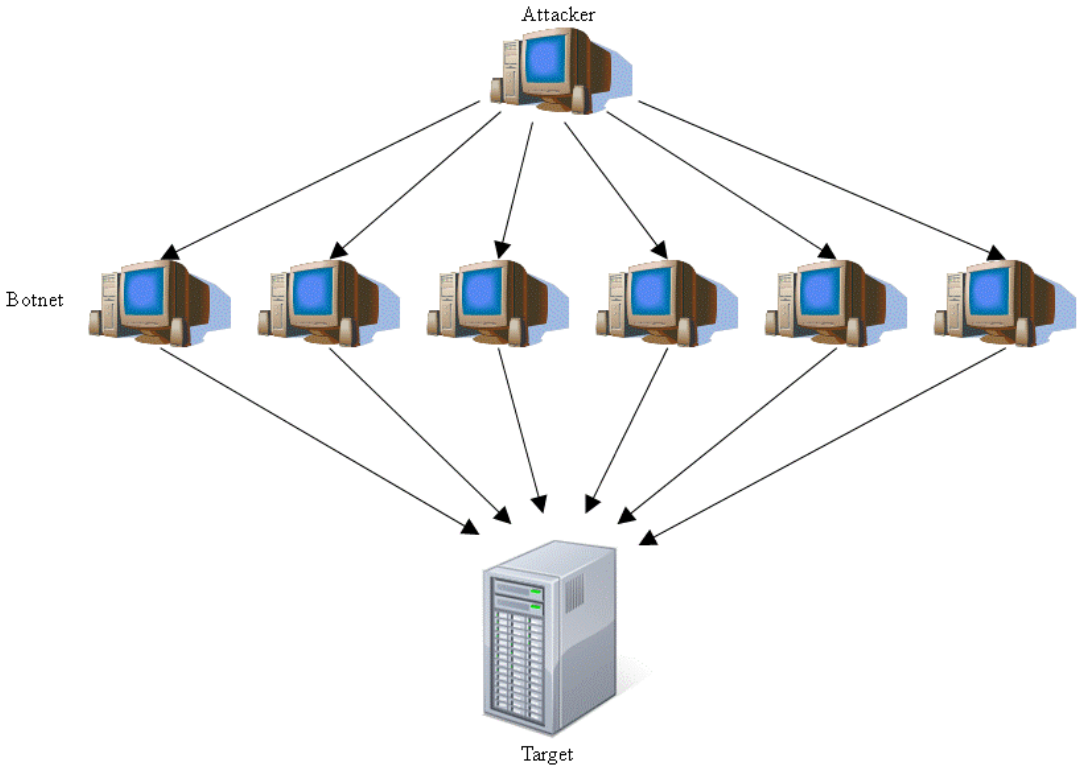
III.Attaques par déni de service distribué (DDoS)

Le principe du DDoS consiste donc à s'appuyer sur des réseaux ou plates-formes présents sur Internet afin de disposer d'un maximum de ressources (en général de la bande passante ou de la capacité à générer des sessions) à exploiter face à une victime.

- Les attaques de type DDOS visent à rendre un service présent sur Internet (site web par exemple) indisponible en le bombardant de requêtes jusqu'à saturation. Pour ce faire, l'attaquant utilise généralement la puissance cumulée d'un grand nombre d'ordinateurs sous son contrôle (également dénommées « zombies »), pour constituer ce que l'on appelle un « botnet ».

Attaques par déni de service distribué (DDoS)

Figure 1 DDoS attack



Attacker sends command to botnet, botnet floods server with messages

III. Attaques par déni de service distribué (DDoS)

- Les attaques DDOS sont particulièrement pernicieuses pour les raisons suivantes :
- Facilité de mise en œuvre .
- Difficulté à contrer l'attaque : Lorsqu'elle est touchée par une telle attaque, une organisation se doit de bloquer le trafic malveillant tout en essayant de maintenir un accès au service pour ses utilisateurs légitimes. Si l'attaque est bien ficelée, la distinction est très difficile à opérer.
- Évolution de l'attaque : Lorsque l'organisation victime met en œuvre une contremesure, l'attaquant adapte en général très rapidement sa stratégie pour maintenir la pression. La migration des services visés vers d'autres plages d'adresses IP constitue, à ce titre, une solution illusoire.

III.1 Attaques distribuées des attaques smurf et fraggle

- les attaques smurf et fraggle peuvent être utilisées de manière distribuée pour attaquer des sites à très forte capacité réseau ou nuire à un ensemble de réseaux.
- Il suffit pour cela d'utiliser comme adresse source une adresse de broadcast d'un des réseaux auquel le pirate veut nuire et de viser quantité de réseaux, lesquels amplifient l'attaque.
- **Exemple**:
- Imaginons qu'un pirate ne dispose que de 512 Kbit/s de bande passante montante. Il peut envoyer environ 960 paquets ICMP de 68 octets par seconde. Ces paquets étant destinés à des réseaux différents, ces derniers renvoient un total de 9 600 réponses, soit une moyenne de dix réponses par réseau.

Chaque réponse est en elle-même une attaque smurf, qui engendre une réponse de la part du réseau dont l'adresse de broadcast source a été usurpée. Si ce réseau dispose, par exemple, de dix machines, il renvoie 96 000 paquets en réponse, soit une bande passante d'environ 50 Mbit/s.

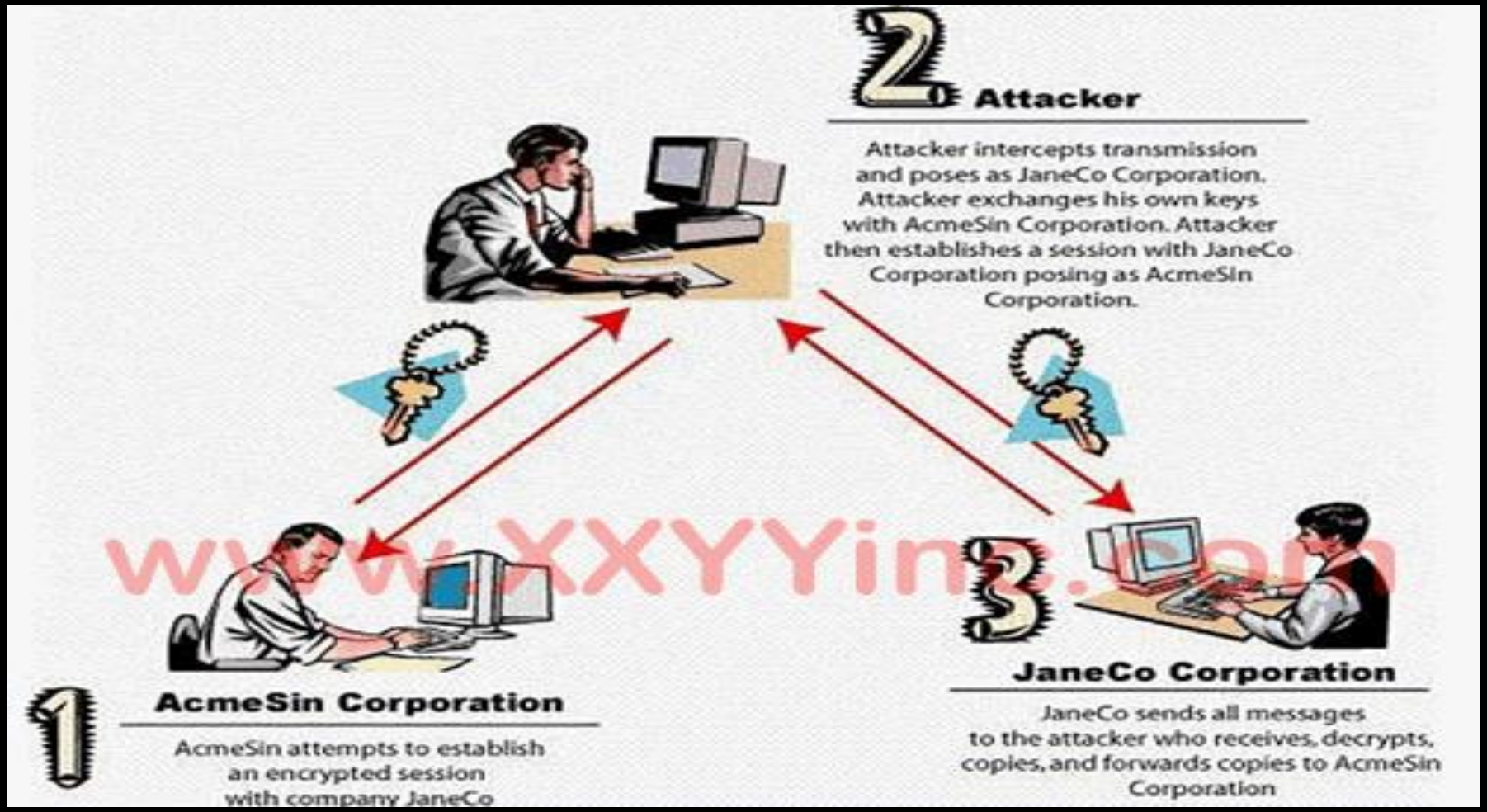
IV. *Attaque man-in-the-middle*

- L’attaque man-in-the-middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d’un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant à chaque acteur de l’échange la réalité de son interlocuteur.
- Il existe différentes architectures pour cette attaque.

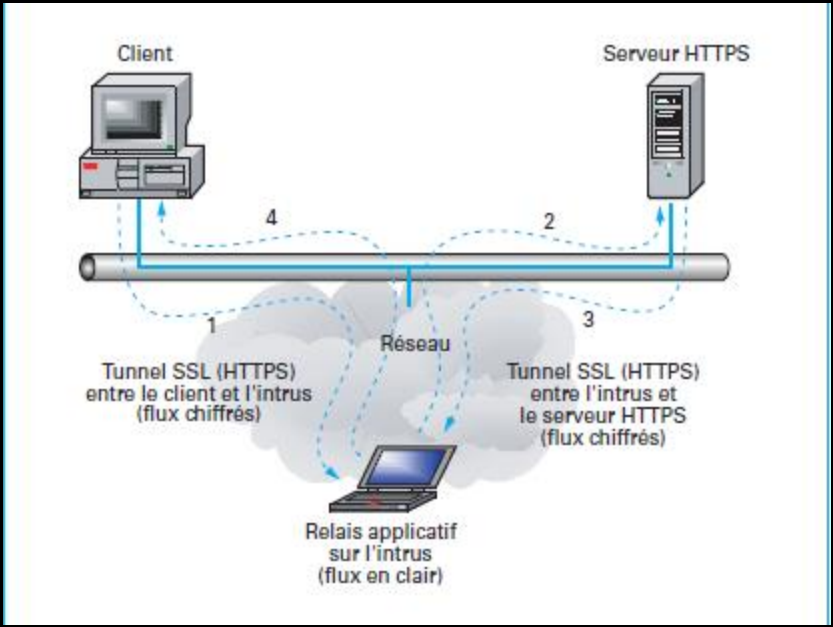
II.1-Relais applicatif

- Le relais applicatif n'est pas à proprement parler une technique d'attaque, mais plutôt une « architecture » que l'intrus désire obtenir pour augmenter l'efficacité et la discrétion de son piratage. Cette architecture présente l'énorme avantage de ne pas obliger le pirate à se trouver logiquement entre le client et le serveur.
- L'intrus cherche donc à se placer dans les flux circulant entre le client et le serveur afin d'avoir la visibilité de tous les flux en transit, mais également afin d'être à même de modifier ces flux .
- Prenons par exemple le cas de l'espionnage de flux HTTPS entre client et serveur. L'intrus, ne pouvant espérer déchiffrer une clé de 128 bits (par exemple) dans un délai raisonnable, peut préférer une meilleure tactique qui consiste à se placer sur le flux entre le client et le serveur. L'intrus joue alors le rôle de relais applicatif (proxy) HTTPS

IV.1-Relais applicatif



IV-Relais applicatif



1.le client envoie sa requête HTTPS vers l'intrus qui n'est pas du tout sur le chemin logique entre le client et le serveur HTTPS. Il négocie donc sa session chiffrée avec lui ;
2. l'intrus déchiffre la requête et la renvoie vers le serveur HTTPS. Il négocie donc sa session avec le serveur ;
3. le serveur HTTPS répond à l'intrus ;
4. l'intrus répond au client.

Cette architecture peut aisément être reproduite pour tous les services du réseau qui sont naturellement bâtis pour être relayés tels que HTTP, HTTPS, SMTP...
Notons tout de même que la discrétion n'est pas encore idéale car tant le client que le serveur HTTPS peuvent facilement se rendre compte qu'ils ne se parlent pas directement. Il suffit donc au serveur HTTPS de comparer l'adresse de provenance des paquets du client et l'adresse source indiquée dans les requêtes

V-DNS spoofing

- **DNS spoofing** est un type de cyberattaque qui exploite les vulnérabilités des serveurs DNS pour détourner le trafic des serveurs web légitimes vers des pages malveillantes des hackers .
  - **DNS spoofing :** est une attaque contre le serveur DNS, qui est un système utilisé pour traduire les noms de domaine en adresses IP. Dans cette attaque, un pirate informatique falsifie les informations que votre ordinateur reçoit lorsqu'il demande l'adresse IP d'un site Web.
  - **DNS cache poisoning:** est une méthode d'usurpation DNS côté utilisateur, dans laquelle votre système enregistre l'adresse IP frauduleuse dans la mémoire cache locale. Cela conduit le DNS à rappeler le mauvais site pour vous.

V-DNS spoofing

Il existe quelques méthodes pour effectuer une usurpation de DNS, notamment :

- Compromettre un serveur DNS : un attaquant détourne directement un serveur DNS pour rediriger le trafic de sites légitimes vers d'autres adresses IP.
- Attaques de l'homme du milieu (MIM): un attaquant se positionne entre votre navigateur et un serveur DNS pour vous acheminer vers une adresse IP malveillante.
- DNS cache **poisoning** via le spam : le code de l'empoisonnement du cache DNS se trouve souvent dans les URL envoyées via des e-mails de spam.

V. Attaques génériques sur les protocoles de routage

Les protocoles de routage ont aussi des faiblesses →un déni de service.

Débordement de table d'un protocole de routage:

- Les protocoles de routage doivent maintenir dans une table la liste des routes qu'ils sont chargés de distribuer. La taille de cette table est limitée par la mémoire de l'équipement.

- Une technique consiste à envoyer à un routeur un nombre de tables supérieur à ce qu'il est capable de supporter. Selon la marque et le modèle de routeur.

- Les réactions diffèrent. Certains passent en déni de service car ils ont épuisé leur mémoire disponible, d'autres redémarrent, et enfin d'autres se contentent de ne plus pouvoir accepter de nouvelles routes.

V.1 Usurpation d'adresse MAC ou IP

un intrus peut envoyer des paquets de modification du routage en usurpant l'adresse MAC d'un ou de plusieurs équipements de réseaux, ce qui engendre des boucles (loop) du trafic et donc un déni de service.

- Si nous imaginons par exemple que le paquet est envoyé au mauvais routeur, celui-ci le renvoie vers sa route par défaut s'il en a une,
- ou jette le paquet. Pour peu que la route par défaut pointe vers le routeur qui a envoyé le paquet, cela engendre une situation de boucle puisque les routeurs se renvoient ce paquet indéfiniment.

V.2 Technique du « trou noir »

- Pour être qualifiée de « trou noir » (black hole attack ou sinkhole attack), cette attaque doit provoquer deux situations :
- le routage doit être modifié afin que toutes les informations soient envoyées vers un équipement (en général un ordinateur) ;
- ledit équipement ne cherche pas à acheminer les données jusqu'à leur destination, mais se contente de les détruire.

VI. Traversée du filtrage d'un pare-feu

Dans la plupart des cas, les réseaux des entreprises sont protégés par un pare-feu, ou firewall.

Une des missions du pare-feu est de garder des traces (logs) des flux réseaux qu'il a laissé passer ou qu'il a bloqués, mais sa mission principale reste le contrôle d'accès et donc de laisser passer uniquement les flux autorisés par l'administrateur de la politique de sécurité.

- Malheureusement, il existe des techniques pour passer outre ces contrôles .

VI.1 Fragmentation des paquets IP :

la technique la plus efficace pour traverser un pare-feu reste la fragmentation de paquets.

Pourquoi la plus efficace ? Parce qu'elle fonctionne sur le plus grand nombre d'équipements filtrants. Il existe deux techniques de fragmentation :

par petits paquets et par chevauchement.

VI.1 Tiny fragments

- D'après la RFC (*Request For Comment*) 791 (IP), tous les nœuds Internet (routeurs) doivent pouvoir transmettre des paquets d'une taille de 68 octets sans les fragmenter d'avantage.
- En effet, la taille minimale de l'en-tête d'un paquet IP est de 20 octets sans options. Lorsqu'elles sont présentes, la taille maximale de l'en-tête est de 60 octets.
- Un fragment de données occupe donc au moins 8 octets. Nous arrivons bien à un total de 68 octets.L'attaque consiste à fragmenter sur deux paquets IP une demande de connexion TCP.
- Le premier paquet IP de 68 octets ne contient comme données que les 8 premiers octets de l'en-tête TCP (ports source et destination ainsi que le numéro de séquence).
- Les données du second paquet IP renferment alors la demande de connexion TCP (flag SYN à 1 et flag ACK à 0).

Tiny Fragments

- Or, les filtres IP appliquent la même règle de filtrage à tous les fragments d'un paquet. Le filtrage du premier fragment (Fragment Offset égal à 0) déterminant cette règle elle s'applique donc aux autres (Fragment Offset égal à 1) sans aucune autre forme de vérification. Ainsi, lors de la défragmentation au niveau IP de la machine cible, le paquet de demande de connexion est reconstitué et passé à la couche TCP. La connexion s'établit alors malgré le filtre IP.

Tiny fragments

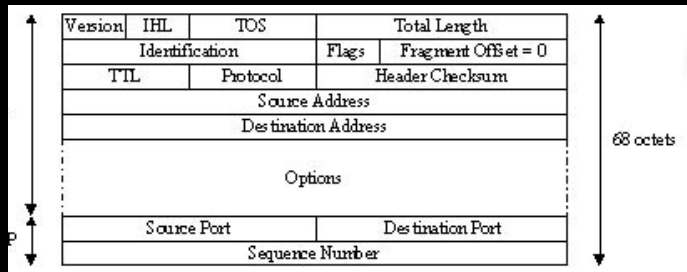


Fig. 1 : Fragment 1

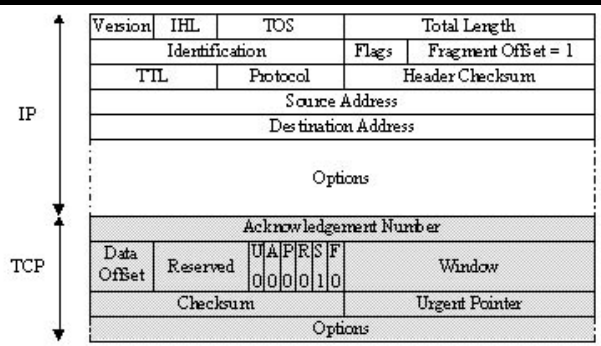


Fig. 2 : Fragment 2

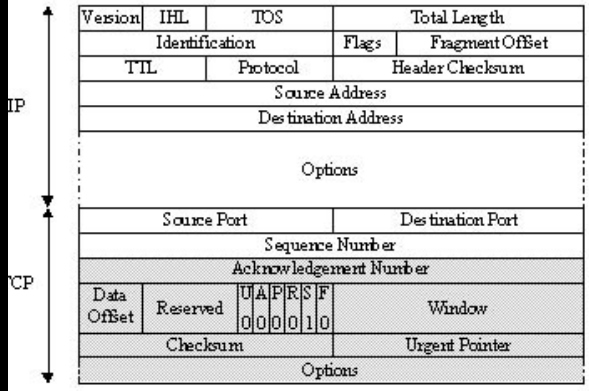


Fig. 3 : Paquet défragmenté

VI.2 Fragment Overlapping

- Toujours d'après la RFC 791 (IP), si deux fragments IP se superposent, le deuxième écrase le premier.
- L'attaque consiste à forger deux fragments d'un paquet IP. Le filtre IP accepte le premier de 68 octets (voir Tiny Fragments) car il ne contient aucune demande de connexion TCP (flag SYN = 0 et flag ACK = 0).
- Cette règle d'acceptation s'applique, là encore, aux autres fragments du paquet. Le deuxième (avec un Fragment Offset égale à 1) contenant les véritables données de connexion est alors accepté par le filtre IP. Ainsi, lors de la défragmentation les données du deuxième fragment écrasent celles du premier à partir de la fin du 8ème octet (car le fragment offset est égal à 1). Le paquet réassemblé constitue donc une demande de connexion valide pour la machine cible. La connexion s'établit malgré le filtre IP.

VI.2.Fragm n Overlapping

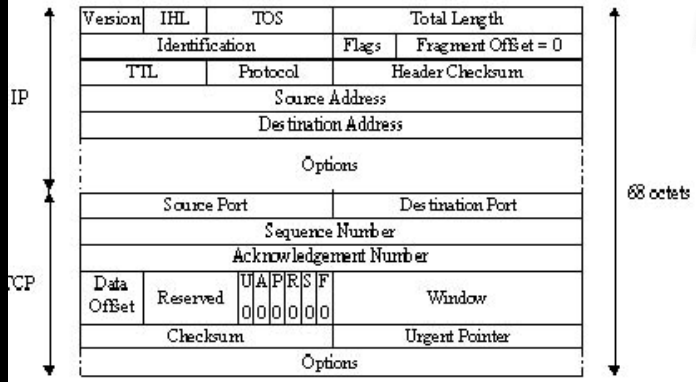


Fig. 4 : Fragment 1

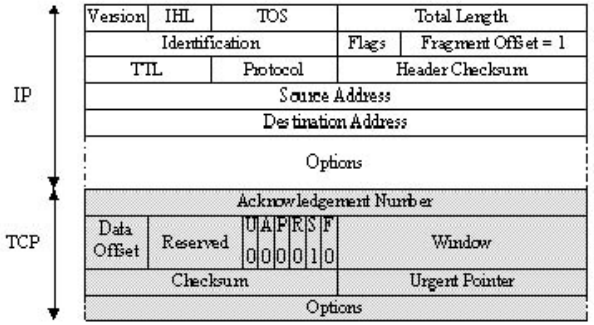
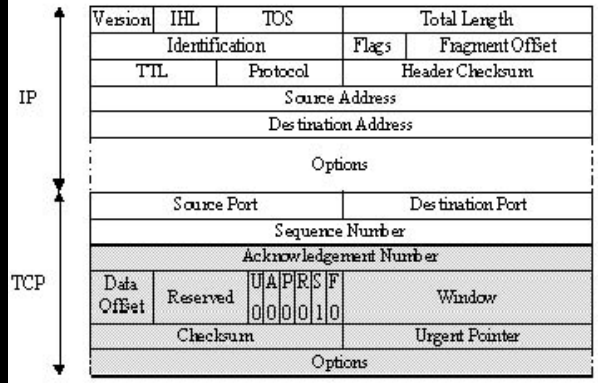


Fig. 5 : Fragment 2



Questions de cours 7

- Q1: Citer les deux cas de vol de session (TCP)
- Q2: Quel est le cas le plus difficile à réaliser et pourquoi?
- Q3: Quels sont les types d’attaque de dénie de service?
- Q4 Quelles sont les attaques de routage