La Couche 7

Généralités

Quelques Applicatifs

Généralité

Notion client/serveur

- Serveur : en attente de connexion → un port ouvert
- Client : veut une information détenue par le serveur
  - ***Connait le nom ou l'@IP du serveur***
  - Le numéro de port
  - La requête à effectuer

Client

- processus créé lorsque le besoin apparaît
  - par une personne
  - au démarrage du système
- l'entité-client doit savoir à quelle entité-serveur elle doit/peut s'adresser
  - au lancement du processus : fichier de configuration, argument
  - par saisie pendant l'exécution

Généralité - Côté serveur

- Les entités serveur
  - fonctionnement permanent (démons)
    - processus créé au démarrage du système
  - processus lancé lorsqu'une demande arrive
    - par un processus "écouteur"
- Méthodes de prise en charge d'une demande de Service
  - L'entité serveur peut traiter elle-même la demande
    - Mise en attente des autres demandes jusqu'à la fin du traitement
  - L'entité serveur peut déléguer à un processus fils (ou un thread) le traitement de la demande
    - Contrôle du nombre de fils (ou de thread) ->nombre maximum donné, pré-création …
    - Risque de surcharge de la mémoire

Quelques exemples
d'Applicatifs

DHCP : définitions

DHCP : Dynamic Host Configuration Protocol -> RFC 2131

(successeur de BOOTP)

utilisation de la couche transport UDP : port 67 client ->serveur

port 68 serveur -> client

• Utilisation pour récupération automatique @IP, etc… sur un ordinateur

Serveur fournit (en général) :

- Adresse IP
- Masque de réseau
- Adresse de la passerelle
- Adresse du DNS, nom du domaine

Un serveur a un « pool » d'adresses qu'il peut distribuer

➡ utilisation d'un bail sur la durée de location d'une adresse

DHCP : fonctionnement

1. Emission d'un broadcast pour la demande d'une adresse IP
   ->DHCPDISCOVER
2. Réponse en unicast d'un serveur vers le client en lui spécifiant les différents paramètres à utiliser
   (auparavant le serveur fait 2 pings pour savoir si l'adresse qu'il propose n'est pas déjà utilisée…)
   ->DHCPOFFER
3. Client donne son accord sur cette adresse en faisant un broadcast
   -> DHCPREQUEST
4. Le serveur acquitte cet accord en répondant en unicast
   -> *DHCPACK*

Pour libérer une adresse IP, utilisation de *DHCPRELEASE*

Utilisable que sur le réseau LAN (par défaut)

Abandonné pour IPv6, et remplacé par ICMPv6

ICMP

- *ICMP : Internet Control Message Protocol*
  - Permet le contrôle des erreurs de transmission
  - Paquet:
    - Basé au-dessus d'IP (protocole 1->ICMP, 58 ->ICMPv6)
    - Contient un type de message, un code et des données (optionnel)
  - Différent type de message :
    - Type 0 : echo réponse
      → réponse au type 8
    - Type 3 : destinataire inaccessible (16 codes différents)
    - Type 5 : redirection (4 codes différents)
    - Type 8 : demande echo
      → permet de savoir si une @IP répond (ping)

IPv6 : Auto-configuration Stateless

- L'équipement prend son adresse lien local → FE80:….
- Vérification de l'unicité de cette adresse sur lien local
  - Envoi d'une trame ICMPv6 "sollicitation d'un voisin" (type 135) sur l'adresse multicast ff02::1
    - Si pas de réponse (attente 1 s), l'adresse est valide
    - Sinon, ICMPv6 "annonce d'un voisin" (type 136), adresse déjà utilisée
- Envoi d'une trame ICMPv6 "sollicitation d'un routeur" *(type 133 = RS)* sur l'adresse multicast FF02::2
- Réception d'une trame ICMPv6 "annonce d'un routeur" *(Type 134 =RA)* avec à l'intérieure le préfixe du réseau
- Par défaut un routeur envoie des RA régulièrement (200 secondes pour Cisco)

NTP - Généralité

- NTP – Network Time Protocol
  - Protocole réseau permettant de mettre à jour son horloge en se synchronisant sur des serveurs de temps présents sur Internet.

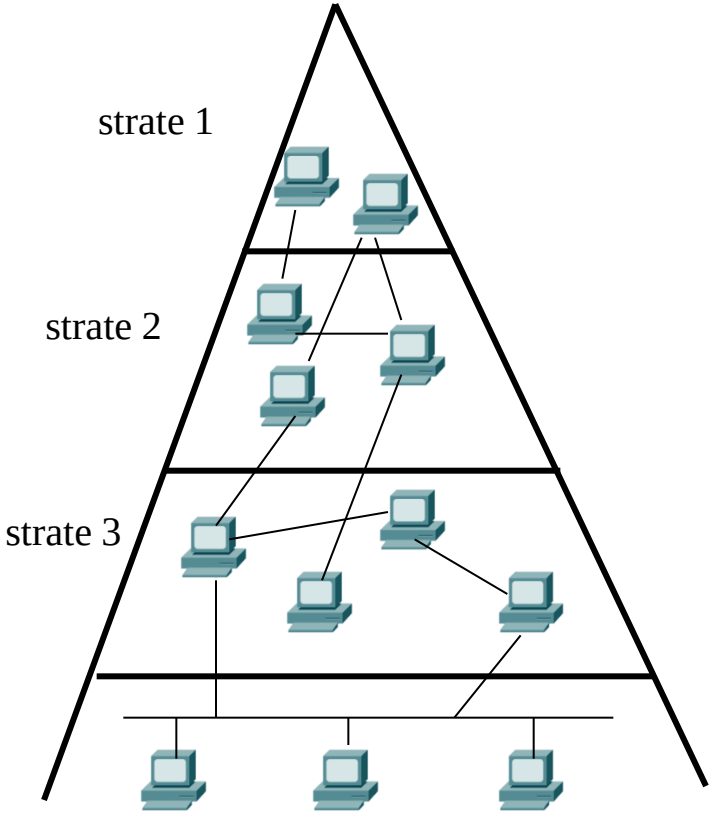
→ But : avoir un temps universel sur toutes les machines
(compilation séparée, synchronisation des processus, etc…)

-Contraintes :

- la différence entre deux machines doit être inférieure à une certaine valeur

- l'horloge d'une machine avance continûment dans le temps

NTP – Principe



Utilisation de la notion de strate

- strate 1 : serveurs qui sont synchronisés sur l'heure UTC
- strate 2 : serveurs qui se synchronisent entre eux et avec la strate 1, serveurs publics en général.
- strate 3 : serveurs qui se synchronisent entre eux et avec la strate 2, serveurs dans les entreprises.
- strate 4 : ordinateurs de réseaux locaux qui se synchronisent sur la strate 3.

D'après la norme, 15 couches maximum !!! → 4 couches.

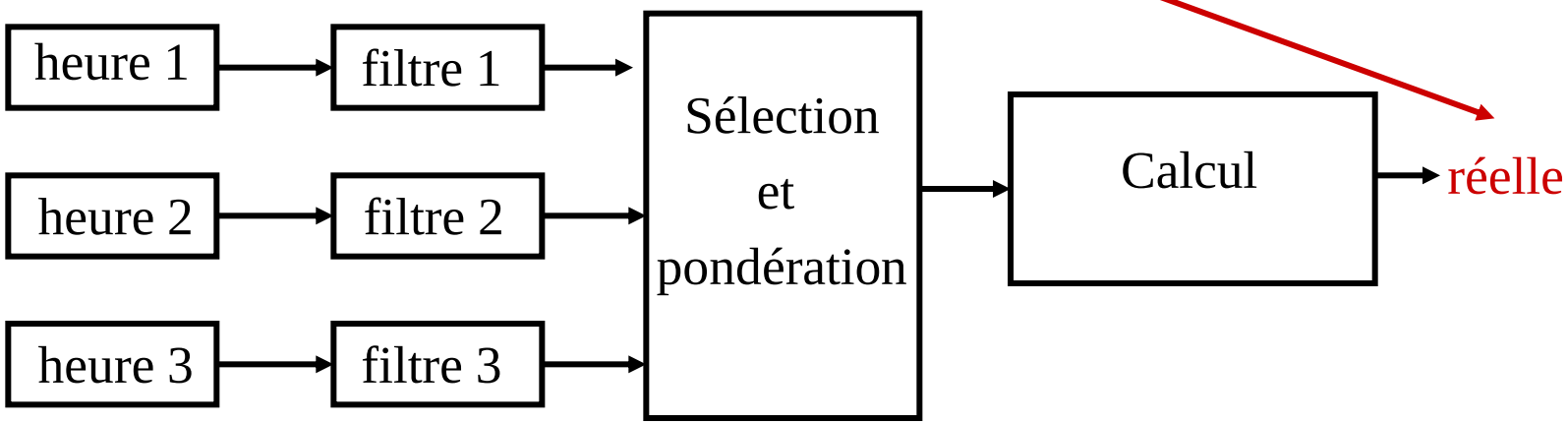
NTP –Synchronisation (1)

- Synchronisation

  → mise en place d'une variable d'ajustement

  besoin : { - heure actuelle de la machine
  - heure réelle de la machine

  - Calcul de l'heure réelle réalisé par le biais des différentes horloges récupérées



NTP –Synchronisation (2)

- Codage du temps sur 64 bits (Timestamp)
- Date du début du codage : 1 janvier 1900
- validité jusqu'en 2036…

- Pour calculer l'heure transmise, il faut connaître le délai de propagation

  Hypothèse : temps aller = temps retour

- La trame contient différents champs dont :
  - la version du protocole
  - le mode d'échange : client/serveur, symétrique, multicast
  - 3 timestamps :
    - Originate timestamp
    - Receive timestamp
    - Transmit Timestamp

Quel calcul doit-on faire pour trouver le délai de transmission ?

Service de messagerie

- Autre nom : courrier électronique, e-mail, couriel

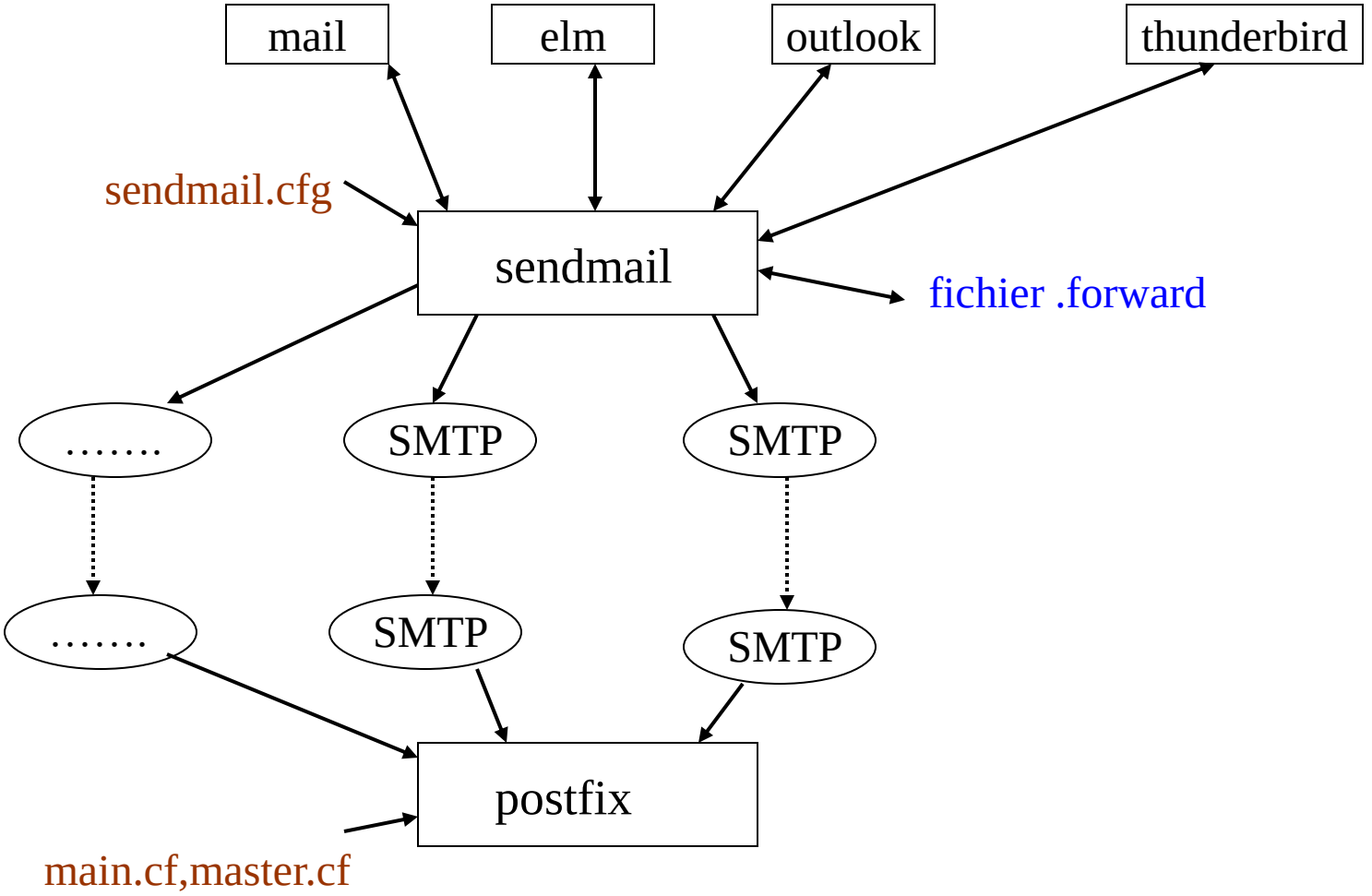
  ➡ permet d'échanger des messages et des fichiers

- Il nécessite un serveur de messagerie accessible à partir d'internet. Le serveur dispose d'une boîte à lettre (BAL) pour chaque client géré par la messagerie.

- Les messages sont stockés par le serveur de messagerie, en attendant que le client vienne consulter sa boîte aux lettres.

  - le message peut être lu :
    - en *mode online* - message stocké sur le serveur et lu à distance
    - en *mode offline* – message déplacé sur la station client et effacé du serveur

Rôle des entités du mail



SMTP/ ESMTP

- SMTP: RFC 821/ 5321

  (Extended) Simple Mail Transfert Protocol

  - Permet d'échanger du courrier électronique

- le format des adresses des utilisateurs fait figurer le nom de l'utilisateur suivi du nom de domaine : laurencot@isima.fr

  identifie de manière unique chaque boîte aux lettres (personne@machine.domaine, personne@domaine)

  (cf. requête MX du DNS)

- Quelques limitations :
  - nom d'utilisateur < 64 caractères
  - nom de domaine < 64 caractères
  - nombre de destinataires < 100
  - Extension avec le standard MIME (Multipurpose Internet Mail Extension) pour du texte formaté, des images ou du son (tout ce qui n'est pas ASCII)

RFC 821

Structure d'un message

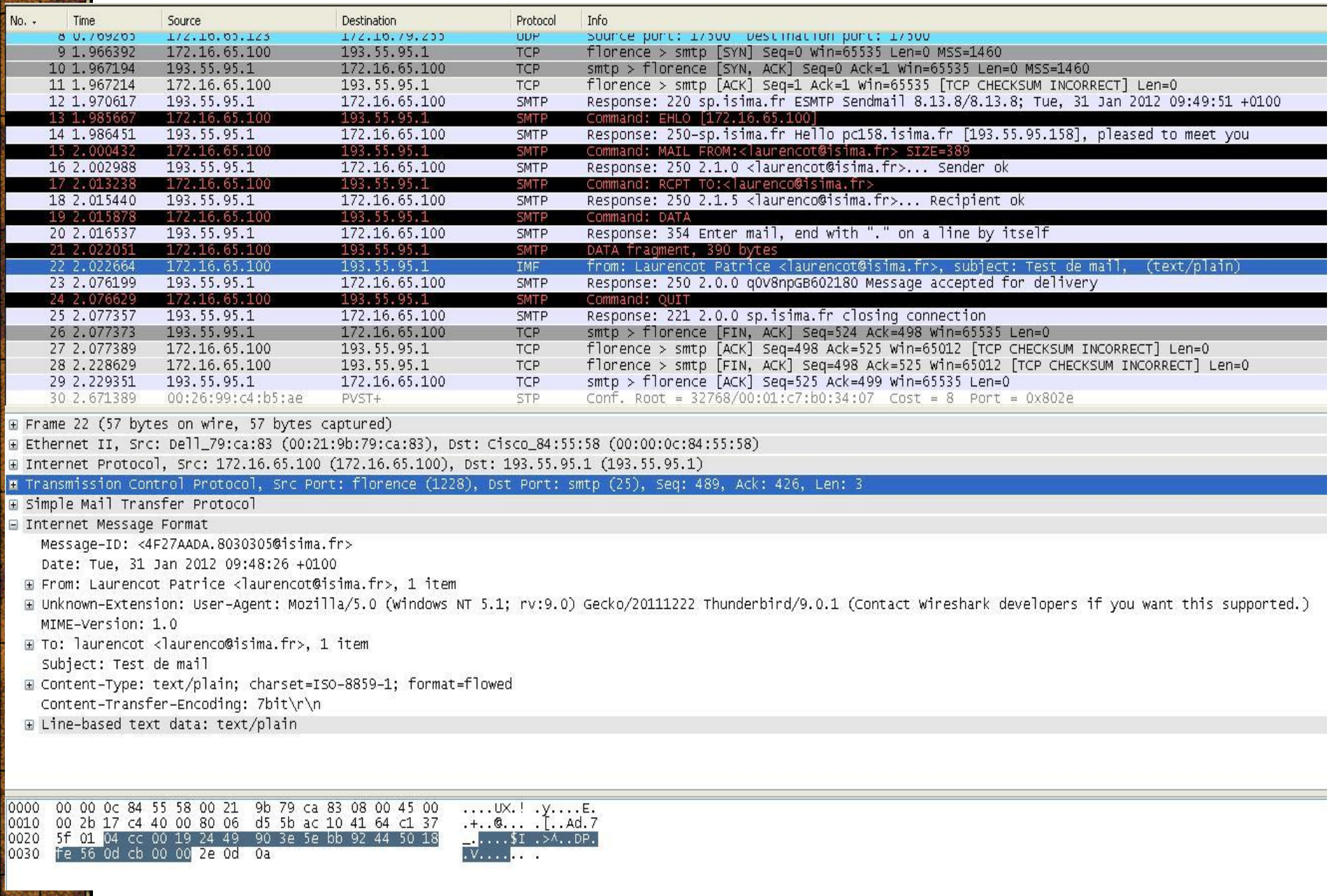
- En tête
- Ligne blanche
- Corps du message (suite de lignes terminés par CR/LF)

En tête

- From : expéditeur
- To : destinataire(s)
- CC : copies à
- Bcc : copie aveugle (destinataire caché)
- Reply-to : adresse de réponse
- Error-to : adresse en cas d'erreur
- Date : date et heure de l'envoi
- Message-id : numéro unique permettant de référencer le message
- Received : informations de transfert
- Subject : sujet

Session SMTP (1)

- SMTP
  - Basé sur TCP -> Triple poignée de main
  - Puis Etablissement de la connexion au niveau smtp et identification de la source et la destination
    - Envoie HELO ou EHLO, puis MAIL FROM, puis RECPT TO
  - Si OK, Envoi du message avec les différents entêtes
  - Libération de la connexion au niveau smtp
    - QUIT
  - Libération au niveau TCP
    - FIN+ACK , FIN+ACK, ACK


No. Time Source Destination Protocol Info
8 0.769265 172.16.65.123 172.16.79.255 UDP Source port: 17500 Destination port: 17500
9 1.966392 172.16.65.100 193.55.95.1 TCP florence > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1460
10 1.967194 193.55.95.1 172.16.65.100 TCP smtp > florence [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
11 1.967214 172.16.65.100 193.55.95.1 TCP florence > smtp [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0
12 1.970617 193.55.95.1 172.16.65.100 SMTP Response: 220 sp.isima.fr ESMTP Sendmail 8.13.8/8.13.8; Tue, 31 Jan 2012 09:49:51 +0100
13 1.985667 172.16.65.100 193.55.95.1 SMTP Command: EHLO [172.16.65.100]
14 1.986451 193.55.95.1 172.16.65.100 SMTP Response: 250-sp.isima.fr Hello pc158.isima.fr [193.55.95.158], pleased to meet you
15 2.000432 172.16.65.100 193.55.95.1 SMTP Command: MAIL FROM:<laurencot@isima.fr> SIZE=389
16 2.002988 193.55.95.1 172.16.65.100 SMTP Response: 250 2.1.0 <laurencot@isima.fr>... Sender ok
17 2.013238 172.16.65.100 193.55.95.1 SMTP Command: RCPT TO:<laurenco@isima.fr>
18 2.015440 193.55.95.1 172.16.65.100 SMTP Response: 250 2.1.5 <laurenco@isima.fr>... Recipient ok
19 2.015878 172.16.65.100 193.55.95.1 SMTP Command: DATA
20 2.016537 193.55.95.1 172.16.65.100 SMTP Response: 354 Enter mail, end with "." on a line by itself
21 2.022051 172.16.65.100 193.55.95.1 SMTP DATA fragment, 390 bytes
22 2.022664 172.16.65.100 193.55.95.1 IMF from: Laurencot Patrice <laurencot@isima.fr>, subject: Test de mail, (text/plain)
23 2.076199 193.55.95.1 172.16.65.100 SMTP Response: 250 2.0.0 q0V8npGB602180 Message accepted for delivery
24 2.076629 172.16.65.100 193.55.95.1 SMTP Command: QUIT
25 2.077357 193.55.95.1 172.16.65.100 SMTP Response: 221 2.0.0 sp.isima.fr closing connection
26 2.077373 193.55.95.1 172.16.65.100 TCP smtp > florence [FIN, ACK] Seq=524 Ack=498 Win=65535 Len=0
27 2.077389 172.16.65.100 193.55.95.1 TCP florence > smtp [ACK] Seq=498 Ack=525 Win=65012 [TCP CHECKSUM INCORRECT] Len=0
28 2.228629 172.16.65.100 193.55.95.1 TCP florence > smtp [FIN, ACK] Seq=498 Ack=525 Win=65012 [TCP CHECKSUM INCORRECT] Len=0
29 2.229351 193.55.95.1 172.16.65.100 TCP smtp > florence [ACK] Seq=525 Ack=499 Win=65535 Len=0
30 2.671389 00:26:99:c4:b5:ae PVST+ STP Conf. Root = 32768/00:01:c7:b0:34:07 Cost = 8 Port = 0x802e
Frame 22 (57 bytes on wire, 57 bytes captured)
Ethernet II, Src: Dell_79:ca:83 (00:21:9b:79:ca:83), Dst: Cisco_84:55:58 (00:00:0c:84:55:58)
Internet Protocol, Src: 172.16.65.100 (172.16.65.100), Dst: 193.55.95.1 (193.55.95.1)
Transmission Control Protocol, Src Port: florence (1228), Dst Port: smtp (25), Seq: 489, Ack: 426, Len: 3
Simple Mail Transfer Protocol
Internet Message Format
Message-ID: <4F27AADA.8030305@isima.fr>
Date: Tue, 31 Jan 2012 09:48:26 +0100
From: Laurencot Patrice <laurencot@isima.fr>, 1 item
Unknown-Extension: User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:9.0) Gecko/20111222 Thunderbird/9.0.1 (Contact Wireshark developers if you want this supported.)
MIME-Version: 1.0
To: laurencot <laurenco@isima.fr>, 1 item
Subject: Test de mail
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit\r\n
Line-based text data: text/plain
0000 00 00 0c 84 55 58 00 21 9b 79 ca 83 08 00 45 00 ....UX.! .y....E.
0010 00 2b 17 c4 40 00 80 06 d5 5b ac 10 41 64 c1 37 .+..@... .[..Ad.7
0020 5f 01 04 cc 00 19 24 49 90 3e 5e bb 92 44 50 18 _.....$I .>^..DP.
0030 fe 56 0d cb 00 00 2e 0d 0a .V.....

Format MIME (1)

- Types d'encodage
  - Texte 7 bits, ASCII
  - Texte 8 bits
    - les textes sont composés de caractères 8 bits
    - il faut préciser l'alphabet : ex : iso-latin1 (alias iso-8859-1)
  - Base 64
    - pour les messages binaires
    - groupe de 24 bits, segmentés en 6 bits
      (3 octets, 4*6 bits 0 – 25 → A – Z , 26 – 51 → a –z, 52 – 61 → 0 – 9, 62 → +, 63 → /)
  - Quoted-Printable
    - codage ASCII normal *(A =0x41, a= 0x61, 0=0x30, +=0x2B, /=0x2F)*
    - pour ce qui n'est pas ASCII, valeur = hexa.

Format MIME (2)

- Exemple
  - From :
  - Mime-Version : 1.0
  - To :
  - Subject
  - Content-type : multipart/mixed; boundary=« debutdumime"
    (ligne blanche)

This is a multi-part message in MIME format.

--debutdumime
content-type : text/plain; charset=iso-8859-1

bla-bla
--debutdumime
content-type : audio/basic
content-transfert-Encoding: base64

fichier audio
--debutdumime

Exemple

POP

- Protocole permettant de relever le courrier sur un serveur
  - POP 3 : Post Office Protocol (version 3) port 110
    - permet l'authentification (login, passwd en clair – codage bin64)
      (pops permet de sécuriser les échanges)
    - réception seulement des courriers sur un serveur (envoi par smtp)
    - réception des messages d'erreur ou d'acquittement
    - Nécessité de télécharger l'intégralité du courrier sur la station avant la lecture, sans possibilité de manipuler directement les messages sur le serveur
    - POP utilise une syntaxe en 4 caractères :
      - STAT : récupère le nombre et la taille des messages en attente
      - LIST ou UIDL : liste des messages à récupérer
      - RETR msg : permet de récupérer un msg
      - DELE msg : suppression
      - USER, PASS : login, passwd
      - QUIT : fin
        (ex : DELE 10, rep = OK, RETR 11, rep=OK+ msg, DELE 11,….)

IMAP

- Protocole permettant de relever le courrier sur un serveur
  - IMAP : Internet Message Access Protocol port 143, imaps 993
    - permet l'authentification si nécessaire de façon chiffrée
    - gère les mails sur le serveur, donc pas besoin de télécharger
    - permet de trier les mails, faire des répertoires, etc…
    - utilise des drapeaux pour la gestion des mails

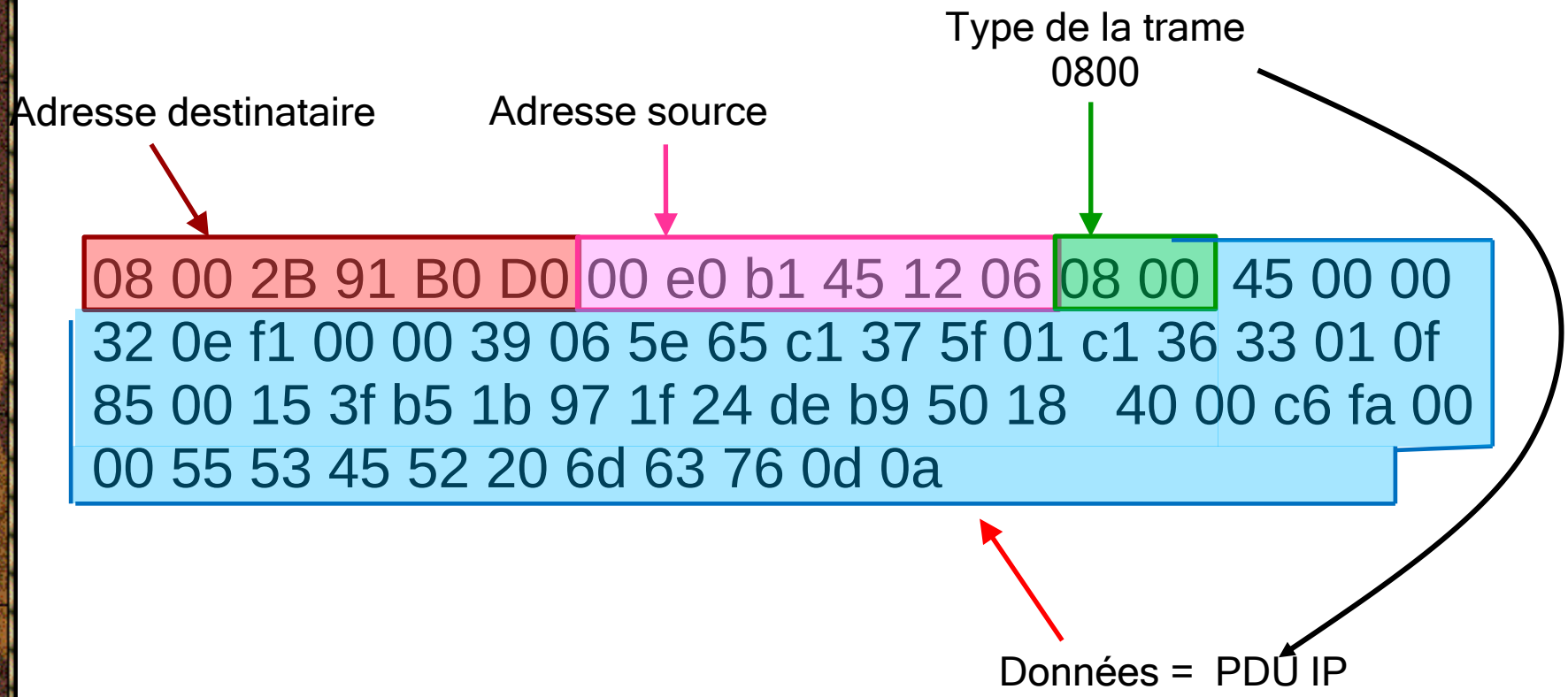
    - IMAP est très utilisé pour les serveurs webmail.

  - Actuellement, version 4 rev 1, RFC 3501
    - Permet de gérer le mode on-line et aussi off-line
    - Utilisation de mots-clés : open, login, list, fetch, logout,…

Encapsulation des données :
Décodage d’une trame

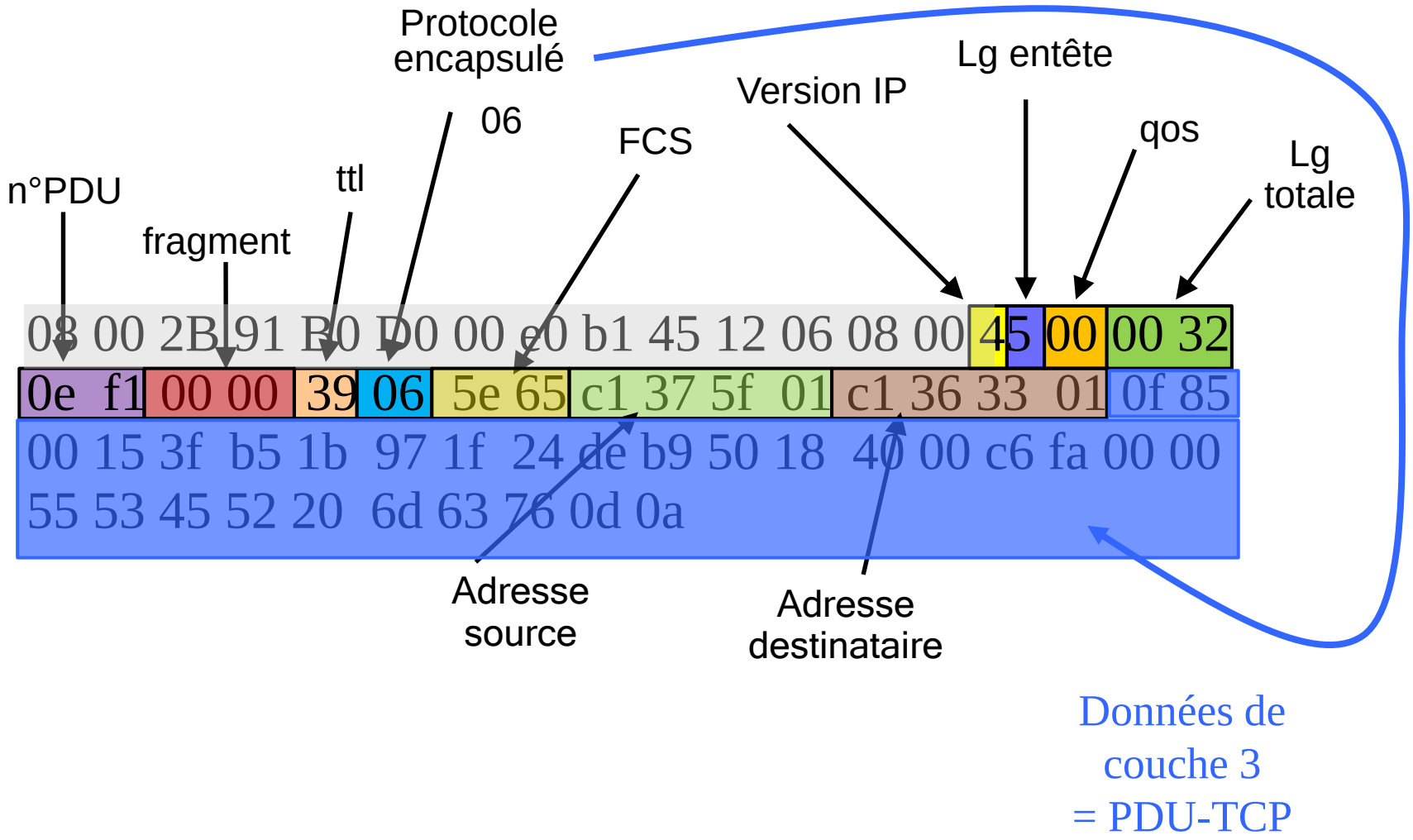
Exemple de trame

1) la PDU MAC-Ethernet

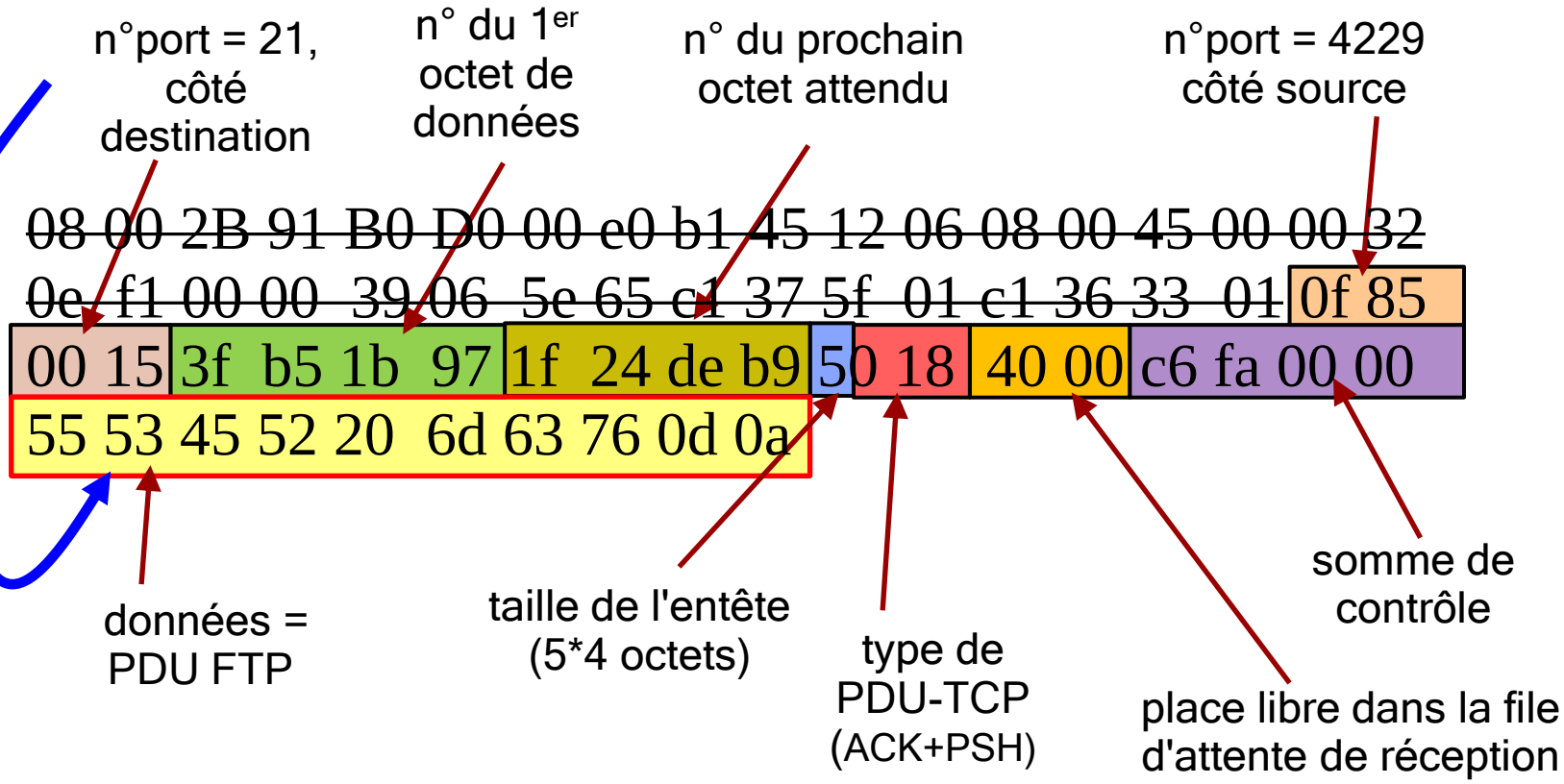


Exemple de trame

2) la PDU IP



Exemple de PDU-TCP



type de PDU-TCP

URG	ACK	PSH	RST	SYN	FIN
20	10	8	4	2	1

ASCII : 55->U, 53->S, 45->E, 52-> R, 6d->m

La sécurisation d'un réseau

1. Généralité
2. Sécurité d'un système appartenant à un réseau
3. Les Techniques et équipements
4. Le chiffrement

P. Laurençot

Généralité

- 4 mots clés et 1 concepts
  - Authentification
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Non-répudiation

Est-ce que TCP/IP respecte ces critères ?

NON

- Aucune vérification sur l'adresse IP source, ni sur le chemin parcouru
- Buffer de réception de dimension finie…

Objectifs, moyens, techniques

Objectifs de la sécurité

- sécurisation des systèmes
- Sécurisation des accès
  - pour protéger les systèmes
  - pour protéger les informations transmises

Techniques pour la sécurité

- chiffrement
- protocoles sécurisés
- restreindre les accès
- Anti-virus, patches
- etc...

Moyens

- définir une politique de sécurité
  - identifier les entités
  - définir quelle entité a le droit de faire quoi
  - définir ce qui est interdit
- installer la politique définie
- surveiller les systèmes
- participer à la surveillance des réseaux

Pb : les failles de sécurité proviennent à 80% de l'intérieur de l'entreprise

Sécurité d'un système appartenant à un réseau

- Rappel : un système ne peut être attaqué que s'il a un processus serveur en attente de demande (*port en état listen* → commande netstat –an).

- Configuration des services
  - quels services sont nécessaires ? pour quels clients ?
  - droits des services (UID, GID, chroot...)
  - choix des implémentations

- Contrôle des services actifs
  - à partir de la configuration du système
  - en examinant les services en attente, de l'intérieur (**`netstat`**) ou de l'extérieur du système (**`nmap`**)

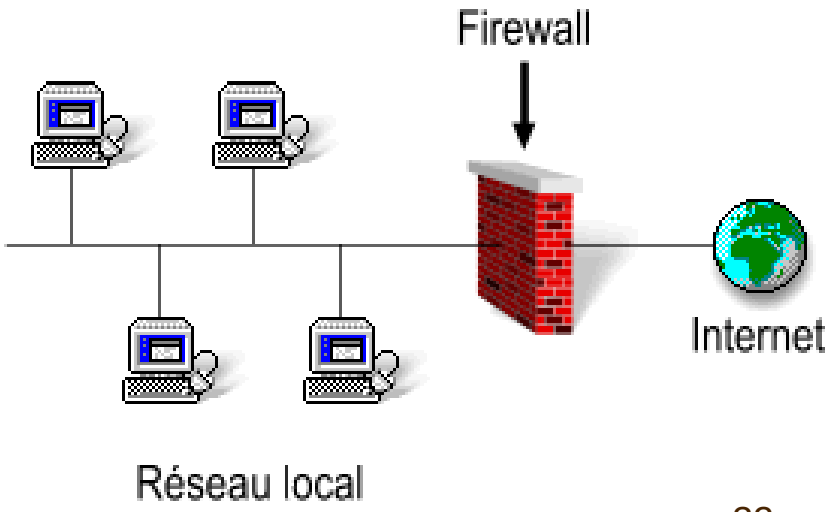
- Contrôle des demandes de service
  - filtrage des demandes avant de les livrer aux entités serveurs
  - journalisation des demandes
  - alertes en cas de demandes interdites
  - remonter les tentatives malveillantes

Le Pare-feu (1)

- La parefeu (firewall)
  - permet de protéger le réseau interne de l'extérieur
  - utilise des règles définies par la politique de sécurité
  - point de passage obligatoire des données
  - Architecture généralement logicielle

Rôle principal : **FILTRAGE**

- au niveau IP
- au niveau Transport
- quelque fois au niveau applicatif : proxy



Le Pare-feu (2)

- Restriction
  - Ne gère pas les communications sur le réseau interne
  - Ne protège pas contre les virus
  - Ne peut voir que le trafic qui passe par lui
  - Ne peut se configurer tout seul !!!

- Avantage
  - Journalisation du trafic

Actuellement, politique de tout interdire et de n'ouvrir que les services utiles.

Le NAT (1)

- Au niveau Réseau (pour un réseau isolé par un équipement)
  - identification du réseau et des systèmes qui le composent
    - adresses privées (RFC 1918)
      - Classe A : 10.0.0.0
      - Classe B : 172.16.0.0 à 172.31.0.0
      - Classe C : 192.168.0.0 à 192.168.255.0
  - protection par un équipement actif (routeur, pare-feu,…)
    - règles de filtrage sur la source, la destination ou les deux (fonction pare-feu)
    - traduction d'adresses (NAT)
      - **IP-masquerading,**
      - **Network Address Translation (statique ou dynamique),**
      - **Port Address Translation,**

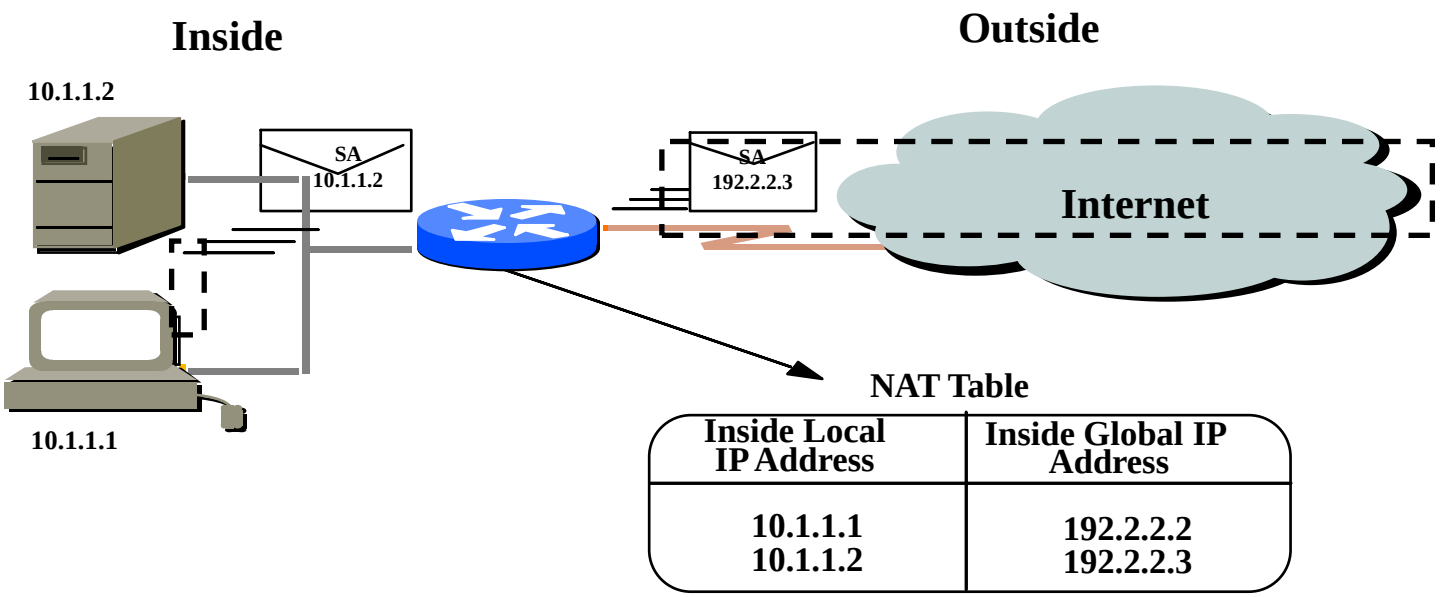
Attention, il peut être nécessaire de réécrire le message du fait du changement d ’@IP.

Le NAT (2)

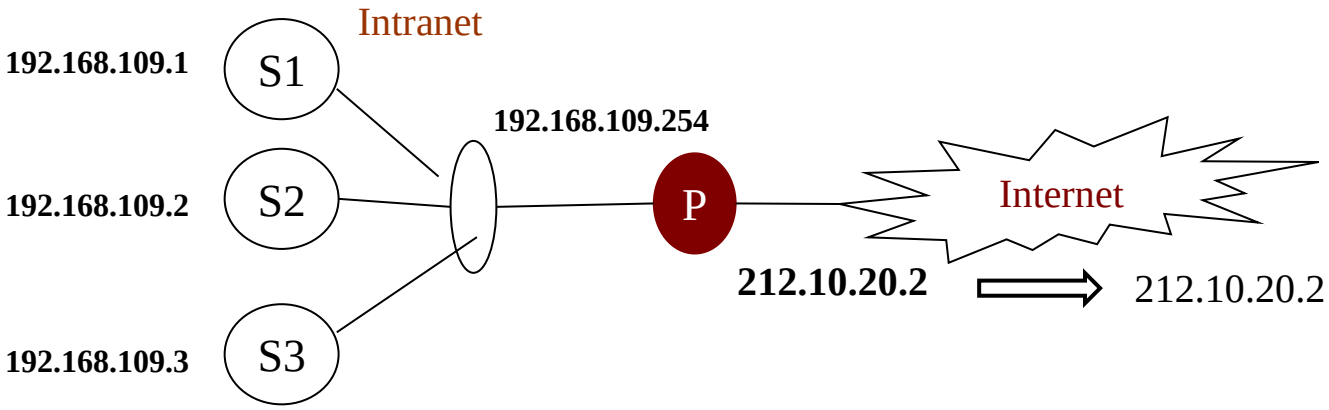
Le NAT statique = association de n adresses avec n adresses.

C'est à dire qu'à une adresse IP interne, on associe une adresse IP externe.

Rôle du système: remplacer l'adresse de la station du réseau par une adresse externe (publique).



Le NAT (3)



1 seule adresse est disponible pour envoyer des paquets IP vers Internet (ex: adsl)

Pb: Si plusieurs stations appartiennent au réseau local, comment peuvent-elles envoyer des PDU-IP vers l'internet et comment les différencier ?

=> Utilisation du NAT dynamique

Le NAT(4)

2 cas possibles :

- **1 seule adresse IP de sortie -> PAT**
- **n adresses de sortie pour m ordinateurs (m > n)**
  -> IP masquerading ou PAT

Fonctionnement :

- *En Masquerading*, traduction automatique de l'adresse IP de la station émettrice avec l'adresse IP de la Passerelle (routeur, proxy)
- *En PAT*, traduction automatique de l'adresse IP de la station émettrice avec l'adresse IP de la Passerelle (routeur, proxy) **et translation du port.**
  La translation du port permet de différencier les stations qui utilisent la même adresse IP Passerelle.

Application possible : mini-réseau derrière un routeur ADSL ➔ pb : adresse IP statique/dynamique

Les sondes (1)

Sonde IPS /IDS

- IDS **I**ntrusion **D**etection **S**ystem
- IPS **I**ntrusion **P**revention **S**ystem

➢ Chargés d'analyser le trafic réseau pour y **détecter des tentatives d'intrusion** :

- soit en analysant le comportement des flux réseaux ;
- soit en se basant sur une base de signatures identifiant des données malveillantes (principe similaire à celui des anti-virus).

➢En cas de détection d'une intrusion :

- Les **IDS alertent** les administrateurs, libre à eux d'intervenir ou non ;
- Les **IPS bloquent** les flux réseau concernés.

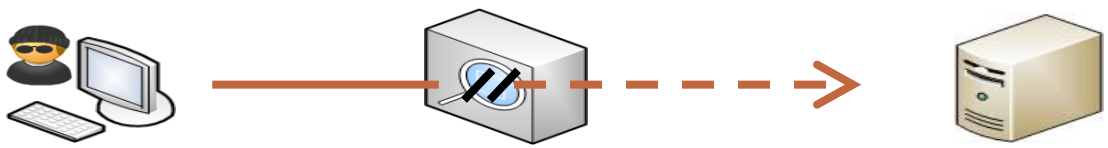
Les sondes (2)

➢Les IDS/IPS demandent une configuration fine et maintenue :

- Ils sont en effet connus pour présenter de nombreux faux-positifs (i.e. ils détectent à tort une tentative d'intrusion) → couplage possible avec SIEM
- De plus, les IDS/IPS basés sur des signatures ne peuvent détecter que les intrusions dont les caractéristiques *techniques sont déjà connues et référencées.*
- *Mise en place du Deep learning !!!*

➢Un IDS peut être soit en coupure du flux réseaux, soit **positionné en écoute.**

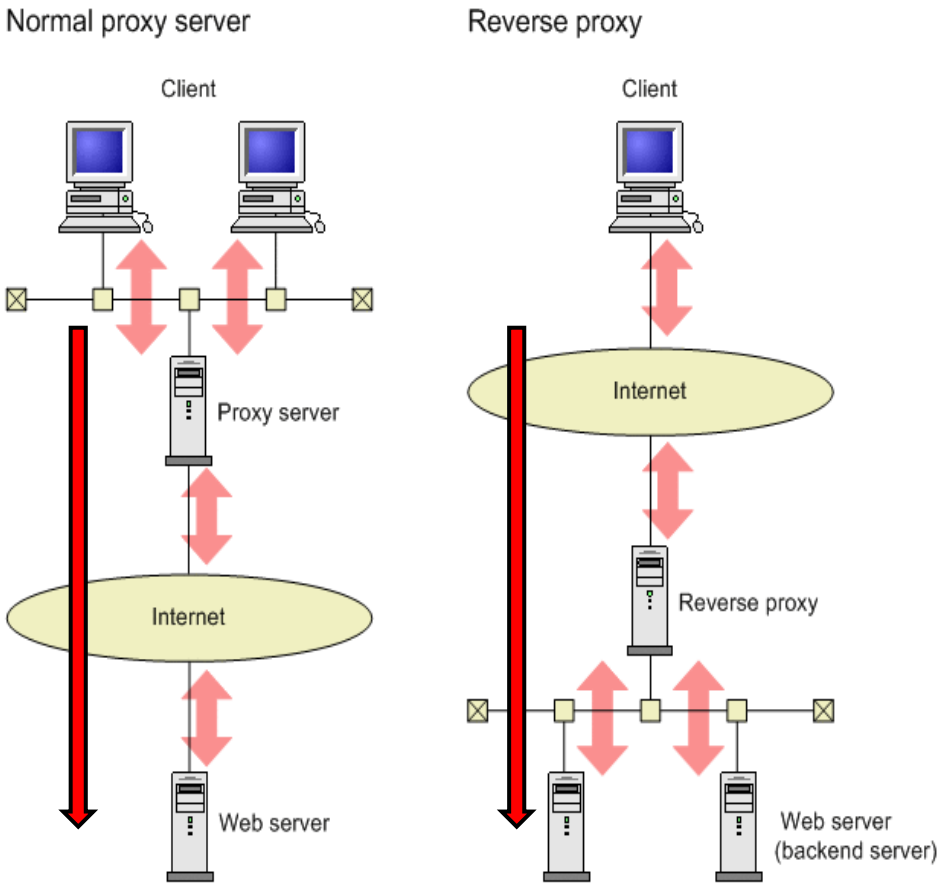
➢Un IPS **doit forcément** être en **coupure du flux** de façon à pourvoir bloquer le trafic lorsque cela est nécessaire.



Proxy et reverse proxy

- Proxy : *composant logiciel servant d'intermédiaire entre la source et la destination*
  - Filtrage
  - Cache
  - Etc…

Le reverse proxy permet de faire aussi:
- load balancer

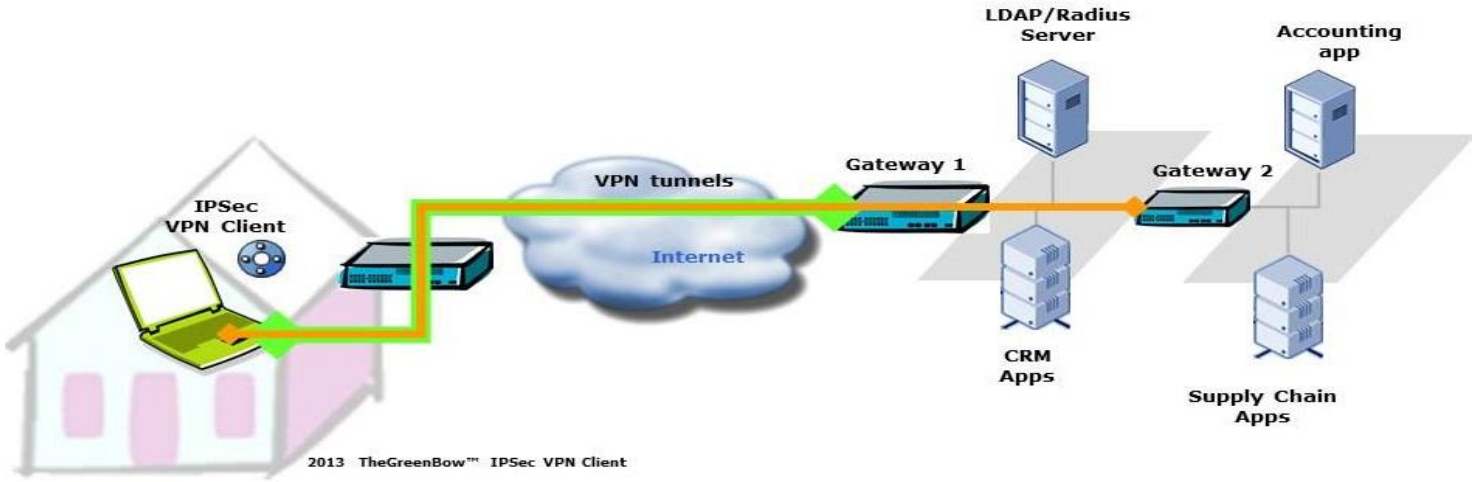


VPN (1)

Virtual Private Network

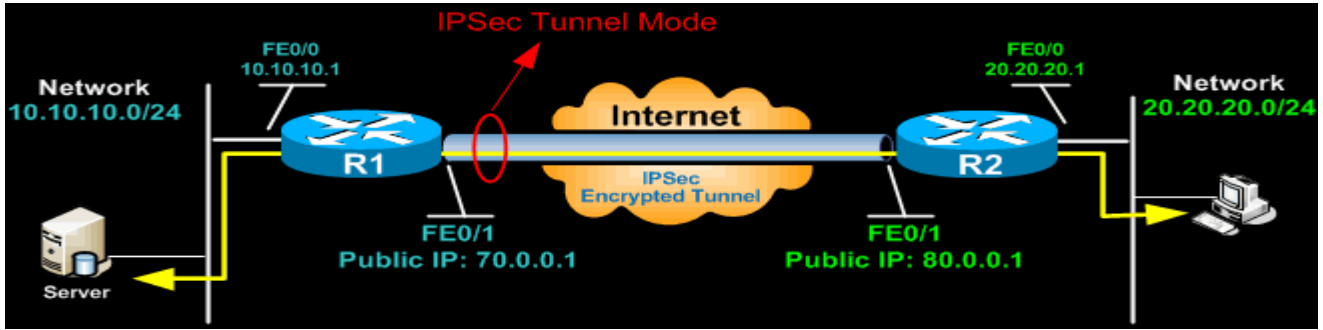
Un VPN est un **réseau virtuel** qui permet à **deux réseaux distants de communiquer en toute sécurité**, y compris si la communication s'effectue via des réseaux inconnus et auxquels nous ne faisons pas confiance.

Exemple avec une entreprise qui possède deux sites distants et qui ont besoin de communiquer entre eux via internet : comment faire passer les flux en toute sécurité via Internet que l'on ne maitrise pas ?



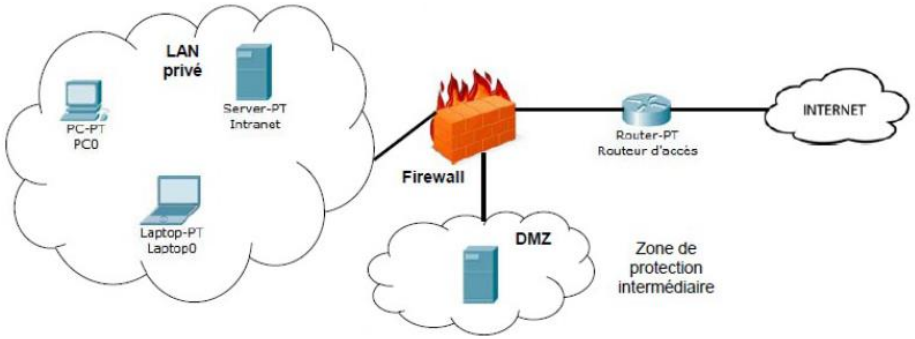
VPN (2)

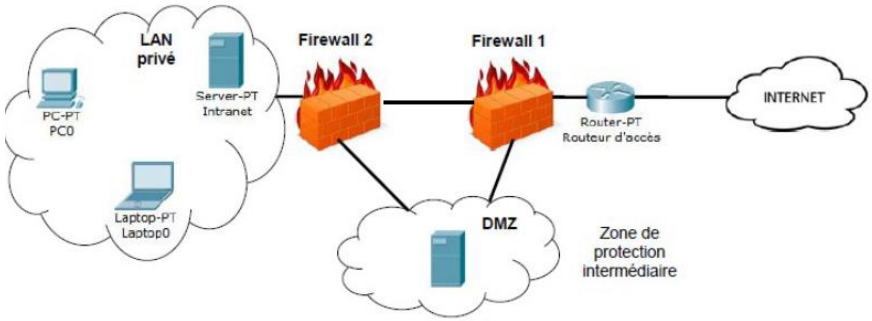
- Nécessite un serveur VPN
  - Le client VPN se connecte sur le serveur VPN et reçoit une nouvelle adresse IP pour communiquer avec ce serveur
  - Les communications passent par ce serveur avant de retourner sur Internet
  - Les communications sont chiffrées entre le client VPN et le serveur VPN.
- Plusieurs méthodes pour créer des VPN
  - Poste à entreprise : OpenVPN
  - D'une succursale à une autre
    - Utilisation de IPSEC
      - Protocole Ikev1 ou Ikv2 utilisé



Architecture (1)

- DMZ: est un sous-réseau séparé du réseau local et isolé de celui-ci et d'internet par un parefeu. Ce sous-réseau contient des machines étant susceptibles d'être accédées depuis internet. (wikipédia)
  - Possibilité d'attaques…
  - Plus ou moins de protection suivant l'architecture utilisée





- Utilisation adresse IP privée
  - Mise en place de NAT

Le chiffrement

Chiffrement : principes

- Définitions
  - chiffrement $M \xrightarrow{E_k} C$
  - déchiffrement $C \xrightarrow{D_{k'}} M$

E	algorithme de chiffrement
D	algorithme de déchiffrement
k	clé de chiffrement
k'	clé de déchiffrement

- Propriétés (souhaitées) d'un cryptosystème
  - $D_{k'}(E_k(M)) = M$ où les clés k et k' sont associées
  - $D_{k'}$ et E_k dépendent totalement ou partiellement d'informations secrètes
  - les algorithmes doivent être économiques : processeur, mémoire, taille de code
  - le secret doit reposer sur les clés plutôt que sur les algorithmes
    - algorithme public - > qualité meilleure
  - le calcul de k' doit être très difficile, même si on connaît C et M
  - $D_{b'}(E_a(M))$ doit être une information non valide

Chiffrement : cryptosystèmes

A chiffre symétrique (k = k')

- économique
- problème de la gestion des clés

DES *(Data Encryption Standard –fin en 2001)*
Triple-DES
IDEA *(International Data Encryption Algorithm)*
AES *(Advanced Encryption Standard)*

A chiffre asymétrique (k ≠ k')

- $D_{k'}(E_k(M)) = E_k(D_{k'}(M)) = M$
- peu économique

DH *(Diffie-Hellman)*
RSA *(Rivest, Shamir, Adleman)*

$E_k(M) = M^e$ modulo n k = {e,n}
$D_{k'}(C) = C^d$ modulo n k' = {d,n}

n = p*q
p et q premiers entre eux
e premier avec (p-1)*(q-1)
d*e = 1 modulo ((p-1)*(q-1))

hachage

- pour créer des empreintes d'information (*digest*)
- algorithmes analogues à ceux du chiffrement
- pas de déchiffrement possible

MD5 *(Message Digest)*
SHA-256 *(Secure Hash Algorithm)*

Chiffrement : asymétrique

- **3 éléments essentiels :**
- Nécessité de deux clés -> créer en même temps par la même personne

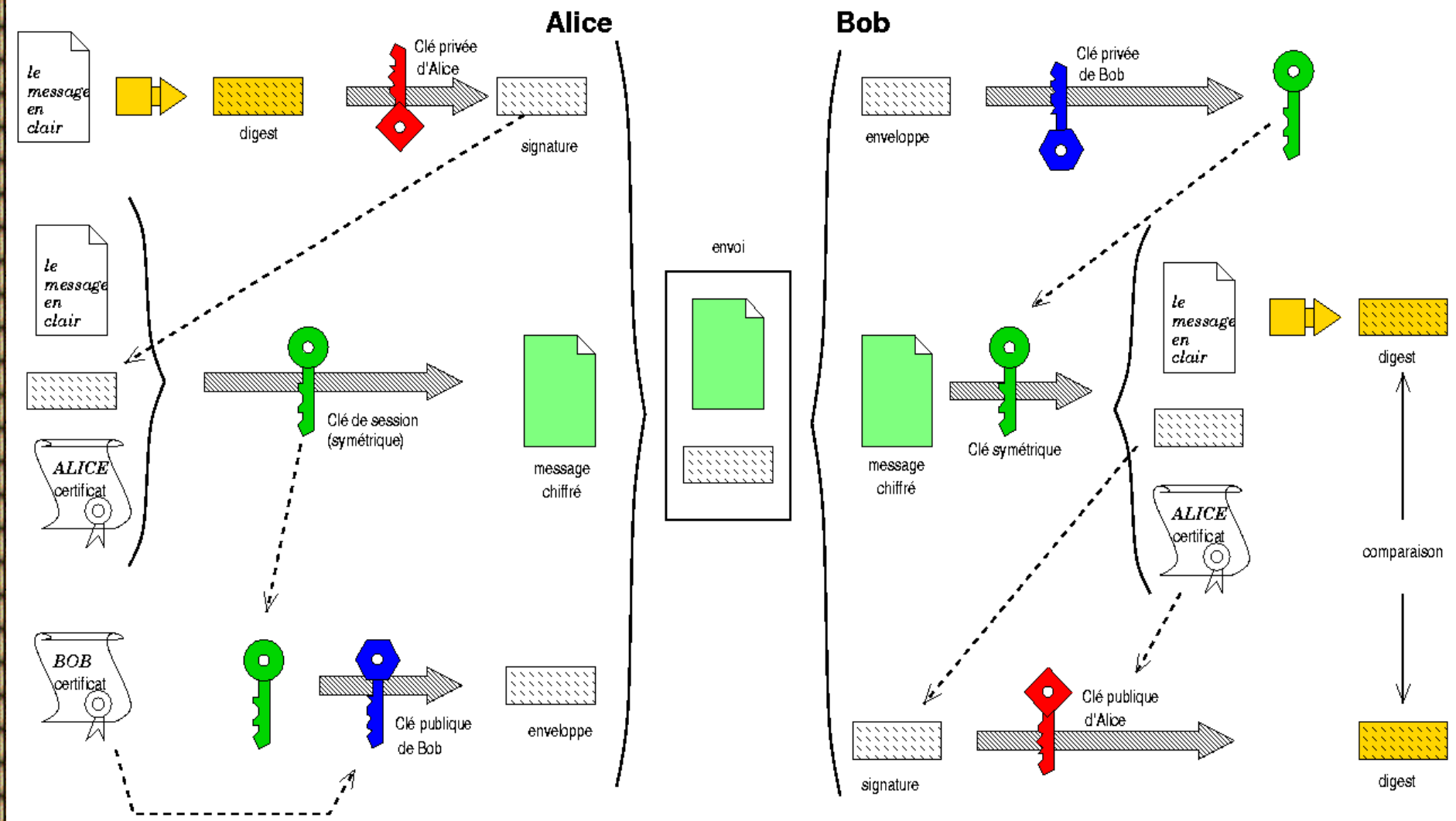
- Clé privée : comme son nom l'indique, cette clé est personnelle et connue de son seul propriétaire
- Clé publique : clé distribuée à tout le monde permettant de chiffrer un message

clé privée (clé publique (M)) = clé publique (clé privée ((M)) = M

- Certificat : donner par une autorité de certification

-> permet de s'assurer qu'une clé publique appartient bien au propriétaire annoncé.

Chiffrement : exemple résumé



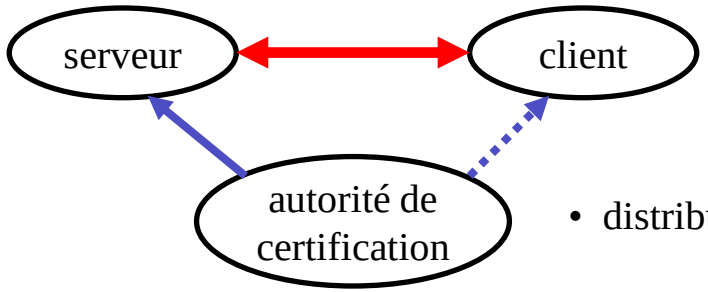
Hachage

- Création d'une empreinte numérique
  - Unique pour un objet
  - Fonction à sens unique
  - Obtention : hash ou condensat ou empreinte sur n bits
  - Problème collision
- Fonctions
  - Md5, sha-1, sha2-256,Sha2-384, sha3-384, sha2-512, …
  - HMAC (Keyed-hash message authentication code)
    - Chiffrement clé secrète + hachage

Protocole sécurisé : SSL/TLS

Secure Socket Layer (Netscape 1994), puis IETF

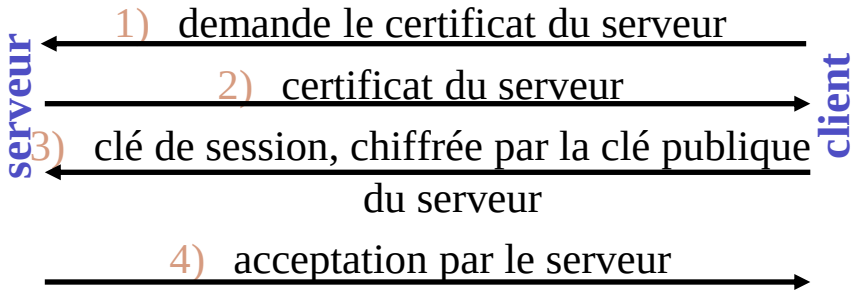
- fournit des services
- possède un certificat



- achète des services
- possède ou non un certificat

- distribue des certificats

établissement de connexion ssl



transmission d'informations

- non chiffrée
- chiffrée avec la clé publique du serveur
- chiffrée avec la clé de session

- compression éventuelle
- Hachage du message envoyé

problèmes

- le client n'est certifié qu'optionnellement ⇒ risque pour le serveur
- si le client est certifié, il ne peut pas être anonyme ⇒ risque pour le client
- pas de contrôle de validité des certificats entre délivrance et fin de validité
- autorités de certification

Protection

Aide

- ANSSI

- Lutte contre le téléchargement illégal : HADOPI

Haute Autorité pour la Diffusion des œuvres et la protection des droits sur Internet.

Comment cela fonctionne-t-il ?

Différent web

TOR