Architecture TCP/IP

Préambule

Ce cours vous présente un bref historique d'internet et de sa gouvernance. Il aborde également l'architecture en couches de la suite des protocoles TCP/IP en détaillant le format des messages et en présentant les protocoles associés aux couches et notamment TCP, les services web et la messagerie.

Historique

Internet est défini comme étant un ensemble de réseaux hétérogènes interconnectés.

Son concept a été développé dans le milieu des années 70 par le DARPA (Defense Advanced Research Agency) c'est-à-dire l'Agence pour les Projets de Recherches Avancées dans la Défense. Ce réseau s'appelait à cette époque Arpanet.

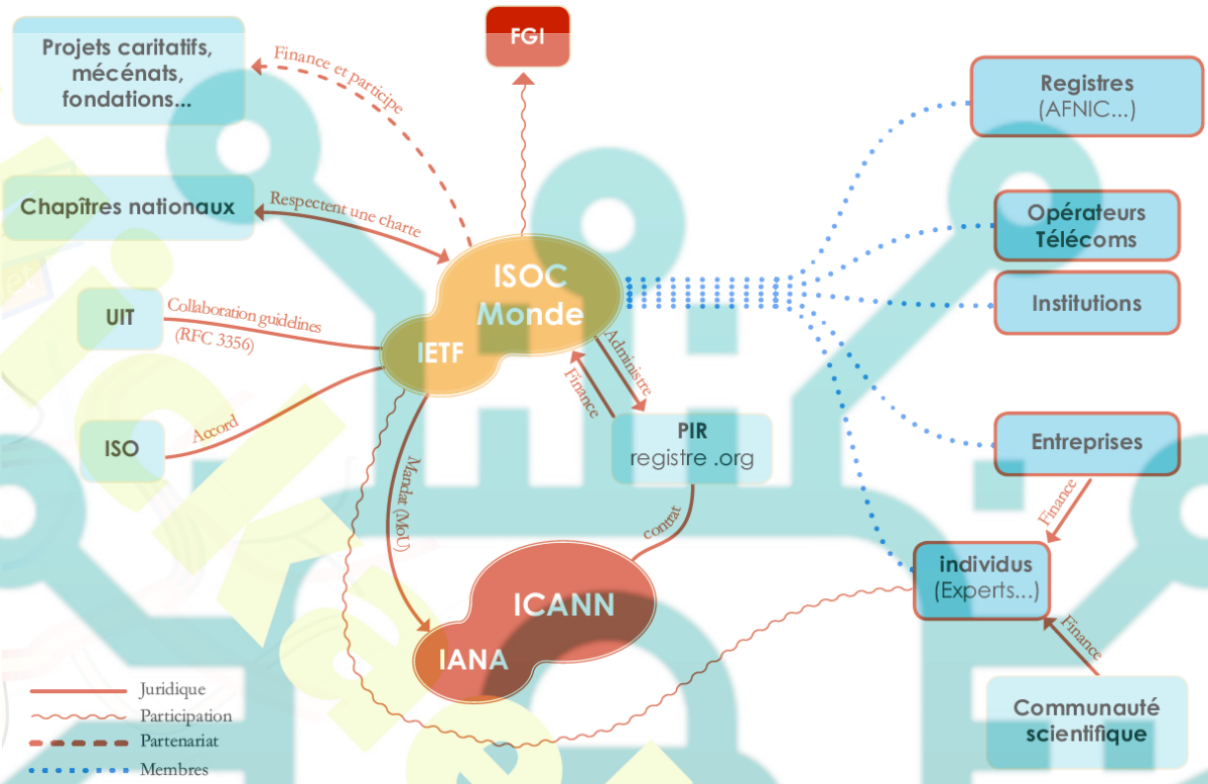
Le DARPA a démarré Internet en 1980 et trois ans après, il établit les protocoles TCP/IP (Transmission Control Protocol/Internet Protocol) dans les réseaux grande distance. Au même moment, Arpanet est scindé en deux réseaux séparés, un pour la recherche (ARPANET) et un autre, plus grand, réservé aux militaires (MILNET)

Ensuite, le protocole TCP/IP est intégré dans la plupart des universités qui utilisent la version UNIX de l'université Berkeley.

https://www.youtube.com/watch?v=5kXKPCqRbRI

Histoire d'internet

Gouvernance internet



Gouvernance internet

Internet Society

Cet univers intègre à la fois la gestion de problématiques techniques pointues au travers de l'IETF, qui élabore les standards de l'internet.

Internet Corporation for Assigned Names and Numbers

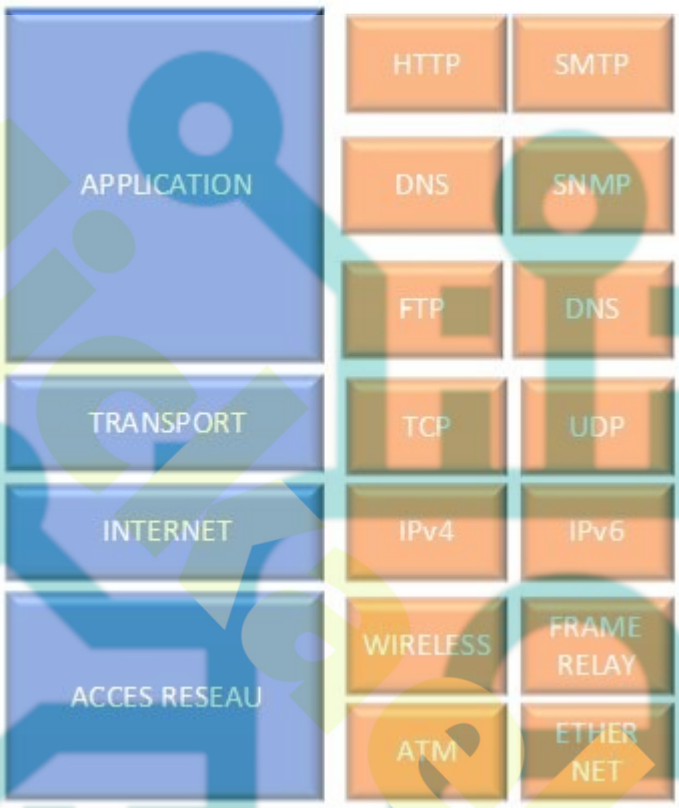
Organisme américain en charge de la gestion des adresses et noms de domaine. Il assure la fonction dite IANA, sous le contrôle du Département du Commerce Américain.

L'**ICANN** est au centre d'enjeux clés pour le contrôle administratif de la «racine» comme la création ou la suppression d'extensions de premier niveau (tel le .com)

Forum pour la Gouvernance de l'Internet

Né du Sommet Mondial sur la Société de l'Information en 2005, on retrouve dans cet univers un certain nombre d'acteurs déjà présents dans celui de l'ICANN. Cependant, les sujets abordés sont plus larges que les ressources techniques (lutte contre la cybercriminalité, protection de l'enfance, des données personnelles ou encore réduction de la fracture numérique entre pays du Nord et pays du Sud)

L'architecture TCP / IP



Modèle en couche de TCP / IP

https://www.youtube.com/watch?v=_0thnFumSdA

Les couches TCP / IP

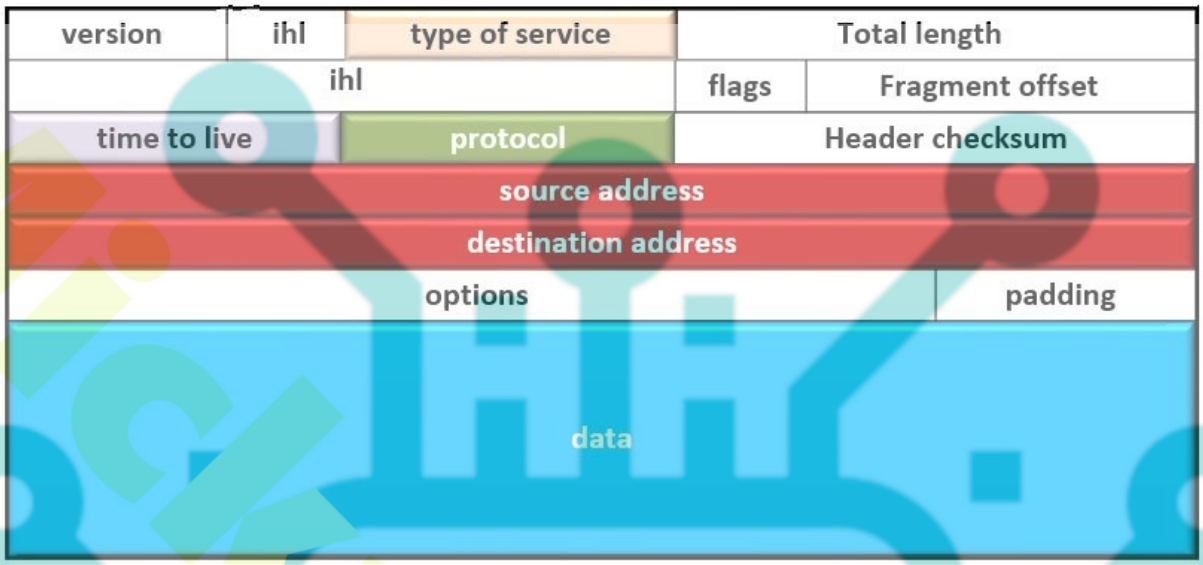
Les protocoles de la couche internet

Protocole IP

Ce protocole permet les fonctions suivantes :

- Adressage et acheminement des datagrammes à travers les réseaux IP.
- Fragmentation et ré assemblage des paquets, pour adapter les datagrammes aux caractéristiques des réseaux physiques.
- Technique de destruction des paquets ayant transités trop longtemps sur un réseau.
- Routage dynamique et auto-adaptatif.

Format de l'en-tête IP



en tête IP

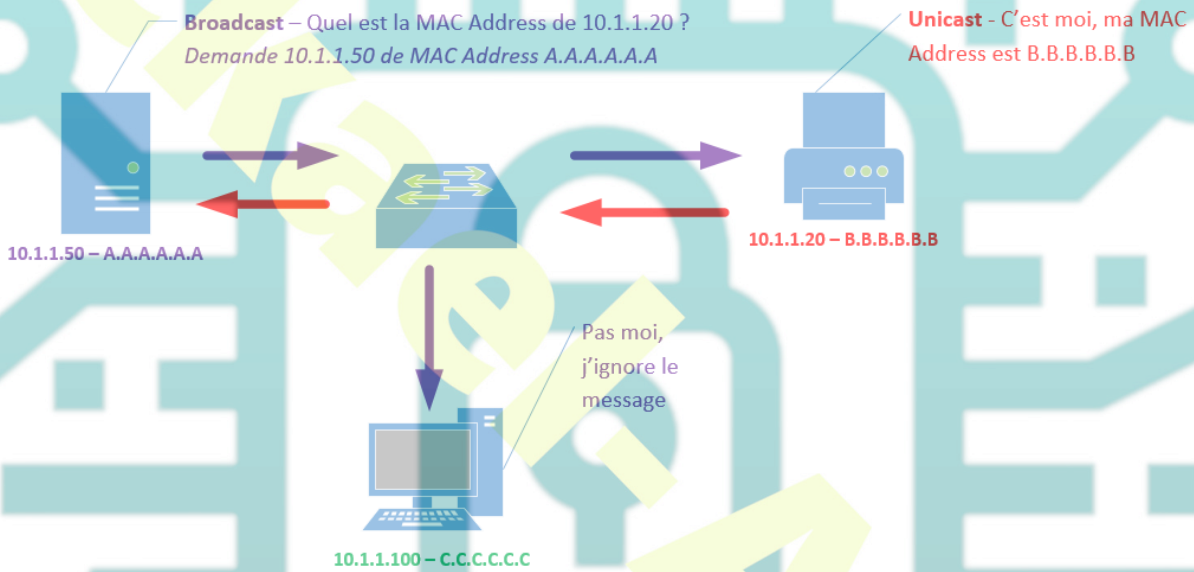
- **Version** : le champ Version renseigne la version IP.
- **Longueur d'En-Tête** : marque le début des données.
- **Type de Service** : sert à préciser le traitement effectué sur le datagramme pendant sa transmission à travers Internet.
- **Longueur Totale** : longueur du datagramme entier exprimé en octets, en-tête et données compris. Ce champ étant codé sur 2 octets, la longueur maximale d'un paquet IP est donc de 65 536 octets (0 à 65535)
- **Identification** : identifie les fragments d'un même datagramme.
- **Flags** : indique si le datagramme doit être fragmenté ou non.
- **Fragment Offset** : indique au récepteur la position du fragment reçu dans le datagramme original.
- **Durée de vie** : Ce champ permet de limiter le temps pendant lequel un datagramme reste dans le réseau.
- **Protocole** : indique quel protocole de niveau supérieur est utilisé dans la section data du datagramme Internet.
- **Checksum d'en-tête** : Contrôle d'erreur sur l'en-tête (recalculé par les routeurs)
  Il est calculé uniquement sur l'en-tête. Le principe consiste à faire la somme des valeurs des octets de l'entête et à inscrire le résultat dans l'octet de checksum. Le récepteur effectue la même opération, si la valeur trouvée est identique, il n'y a pas d'erreur. Dans le cas contraire, le paquet est rejeté.
- **Adresse source** : l'adresse Internet de la source.
- **Adresse destination** : l'adresse Internet du destinataire.

- **Options** : variable (ex. sécurité, supervision réseau)

Protocole ARP

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines. Pour envoyer un datagramme, le logiciel réseau doit convertir l'adresse IP en une adresse physique qui est utilisée pour transmettre la trame.

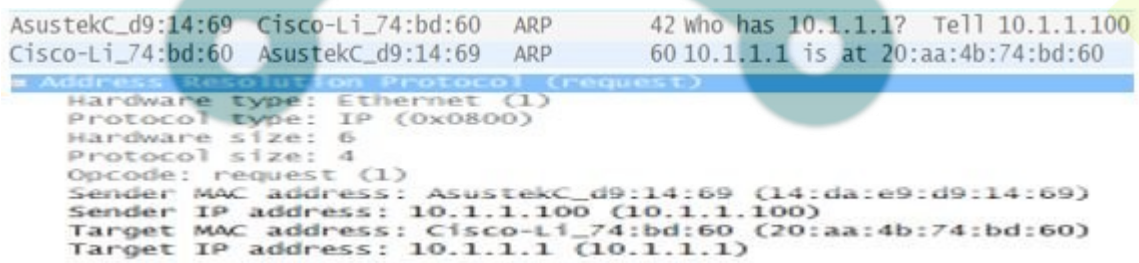
C'est le protocole ARP qui effectue cette traduction en s'appuyant sur le réseau physique. ARP permet aux machines de résoudre les adresses sans utiliser de table statique.



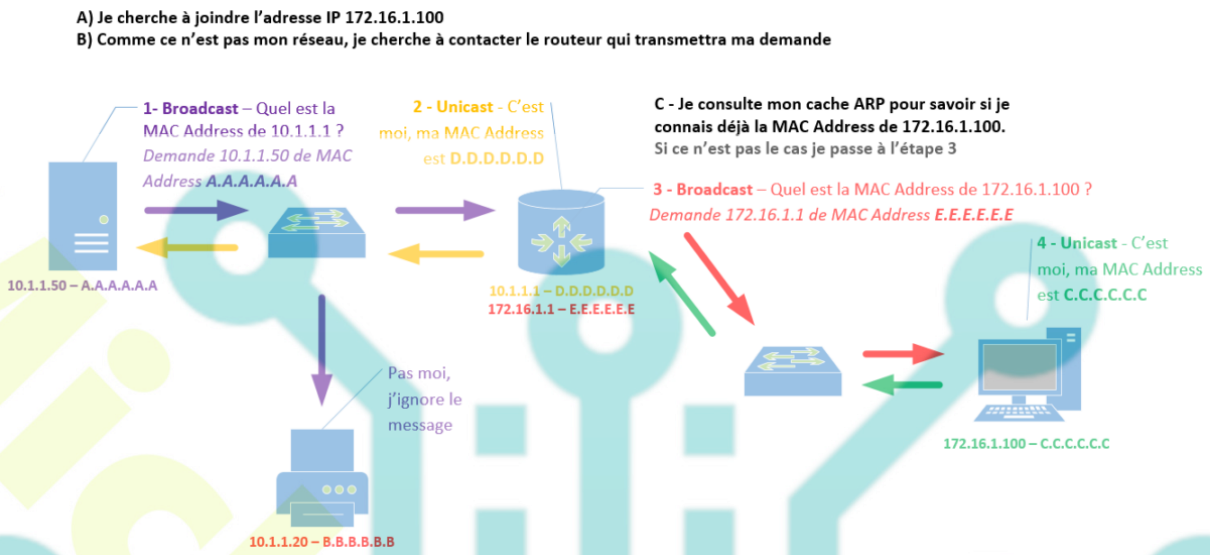
ARP dans un même domaine de diffusion

Une machine utilise ARP pour déterminer l'adresse physique destinataire en diffusant sur le sous réseau une requête ARP qui contient l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique.

Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode broadcast.



Capture message ARP



ARP sans un environnement avec plusieurs domaines de diffusion

Protocole RARP

Permet de récupérer une adresse IP au démarrage à partir d'un serveur RARP (alternative à BOOTP et DHCP)

Protocole IGMP

IGMP (Internet Group Management Protocol) permet aux machines de déclarer leur appartenance à un ou plusieurs groupes auprès du routeur multipoint dont elles dépendent, soit spontanément, soit après interrogation du routeur. Celui-ci diffusera alors les datagrammes destinés à ce ou ces groupes. Du point de vue de l'adresse MAC, le bit I/G est égal à 1, car il s'agit d'une adresse de groupe.

Le protocole comprend deux types de messages :

1. **Un message d'interrogation** (Host Membership Query), utilisé par les routeurs, pour découvrir et/ou suivre l'existence de membres d'un groupe.
2. **Un message de réponse** (Host Membership Report), délivré en réponse au premier, par au moins un membre du groupe concerné.

L'IGMP Snooping est la fonction intégrée dans les commutateurs, qui consistent à écouter et à gérer le trafic IGMP qui circule sur le réseau. Les commutateurs qui ne possèdent pas cette fonction transmettent les trames multicast sur tous leurs ports en broadcast, ce qui génère un trafic inutile.

En tête IGMP

Le champ **Type** est codé sur 8 bits et détermine la nature du message IGMP.
11 – 00001011 – Requête pour identifier les groupes ayant des membres actifs.
16 – 00010000 – Rapport d'appartenance au groupe émis par un membre actif du groupe (IGMP version 2)
17 – 00010001 – Un membre annonce son départ du groupe

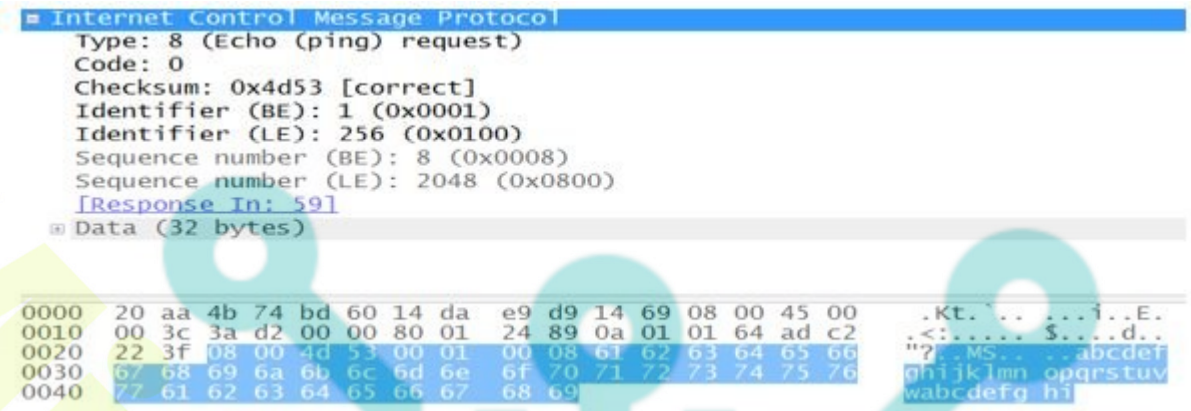
Temps de réponse max, ce champ n'est utilisé que pour les messages de type 11. Il indique le temps d'attente maximum pour un client avant l'émission du rapport d'appartenance. L'unité utilisée est le 1/10 de seconde. Pour les autres types, ce champ est marqué à 0.

Group Address défini l'adresse utilisée par le groupe (224-239)

Protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Il permet de faire part de ces erreurs aux protocoles des couches voisines. Il ne corrige pas lui-même les erreurs.

En tête ICMP



Capture ICMP

Par exemple, Type 8 + Code 0 – echo-request, Type 0 + Code 0 – echo-reply

Ce protocole est utilisé par les commandes PING et TRACE ROUTE

Les protocoles de la couche transport

Numéros de ports TCP et UDP

Les ports sont utilisés dans TCP pour nommer une connexion avec une application.
TCP et UDP donnent la possibilité d'utiliser 65536 ports.
Ces ports sont référencés dans le fichier SERVICES.

Les ports de 0 à 1024 sont réservés aux applications serveur.
Les ports 1024 à 49151 sont appelés ports enregistrés.
Les ports 49152 à 65535 sont les ports dynamiques et/ou privés
Exemple de ports
21-FTP, 23-TELNET, 80-HTTP, 25-SMTP, 53-DNS, 110-POP3, 137 à 139-NETBIOS, 194-IRC

Protocole UDP

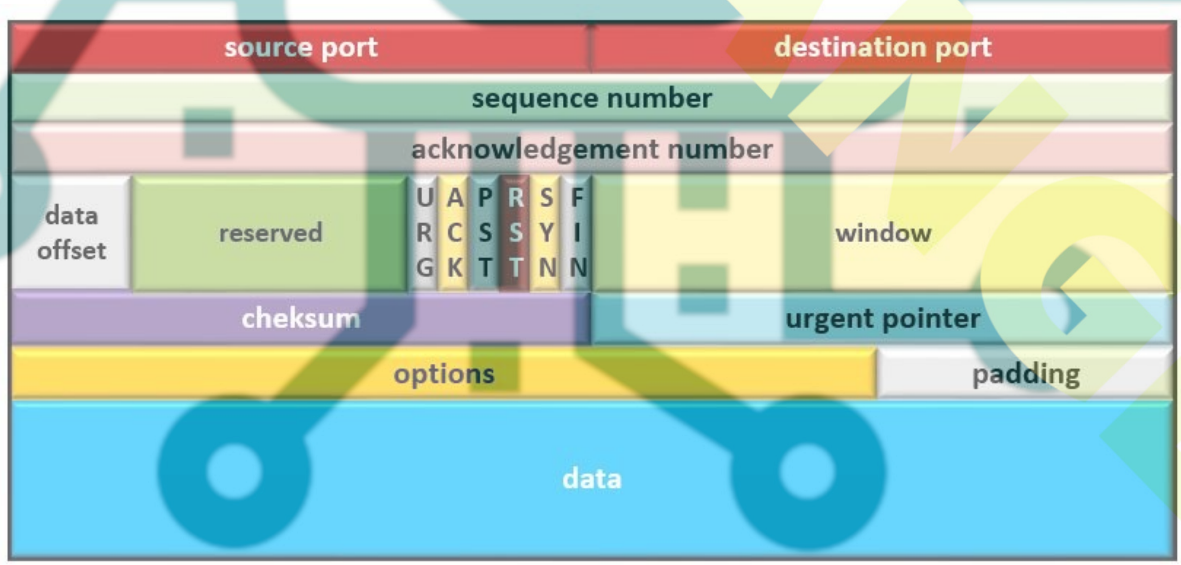
UDP (user datagram protocol) est utilisé principalement pour les communications avec les serveurs de noms de domaine et dans les transactions utilisant le protocole TFTP. Il utilise un mode sans connexion sans accusé de réception.

C'est un protocole non connecté non fiable. Il n'utilise pas les accusés de réception et n'assure pas le contrôle de flux. Les messages UPD peuvent donc être perdus, dupliqués ou dé-séquencés. C'est donc aux applications de la couche supérieure de gérer ces options.

En tête UDP

Protocole TCP

TCP (transmission control protocol) est un protocole orienté connexion (service de communication de processus à processus) conçu pour s'implanter dans un ensemble de protocoles multicouches supportant le fonctionnement de réseaux hétérogènes. TCP fournit un moyen d'établir une communication fiable sur deux ordinateurs distants (correction d'erreur, contrôle de flux, multiplexage, gestion de connexions, priorité et sécurité entre deux tâches exécutées)



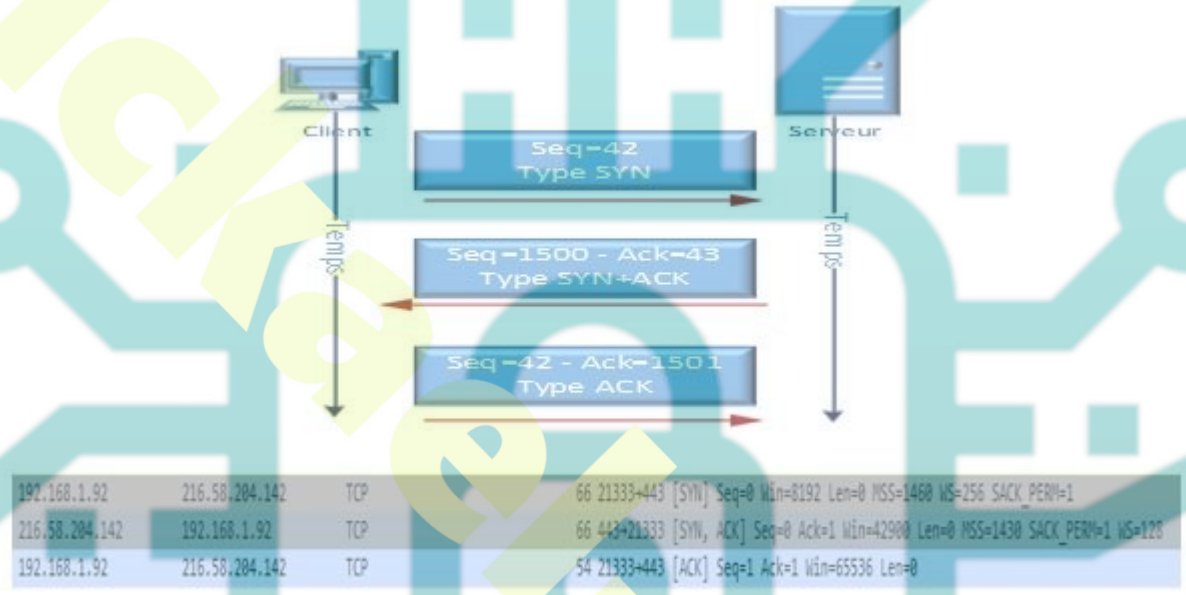
En tête TCP

- **Source Port** : 16 bits – Service de la couche application de l'émetteur.
- **Destination Port** : 16 bits – Service de la couche application du destinataire.
- **Sequence Number** : 32 bits
  On affecte un numéro de séquence à chaque octet de données pour en garder une trace lors du processus de transmission, réception et acquittement. Les numéros de séquence sont nécessaires à la mise en œuvre du système de fenêtre coulissante du protocole TCP. C'est ce système qui garantit fiabilité et contrôle de flots de données.
- **Acknowledgment Number** : 32 bits
  Le rôle des numéros d'acquittement est le même que celui des numéros de séquence. Simplement, chaque extrémité en communication initie son propre jeu de numéros. Ainsi, chaque extrémité assure la fiabilisation et le contrôle de flux de façon autonome.
- **Data Offset** : 4 bits
  Nombre de mots de 32 bits contenus dans l'en-tête TCP. Indication du début des données.
- **Reserved** : 6 bits – Champ réservé pour une utilisation ultérieure.
- **Control bits** : 6 bits – sert à l'établissement, au maintien et à la libération des connexions TCP. Leur rôle est essentiel dans le fonctionnement du protocole.
  1. **URG** : indique que le champ Urgent Pointer est significatif. Une partie des données du segment sont urgentes.
  2. **ACK** : Le segment acquitte la transmission d'un bloc d'octets.
  3. **PSH** : indique à l'hôte en réception de «pousser» toutes les informations en mémoire tampon vers l'application en couche supérieure. L'émetteur notifie le récepteur qu'il a transmis toutes ses données «pour l'instant».
  4. **RST** : indique un arrêt ou un refus de connexion.
  5. **SYN** : Demande d'ouverture de connexion TCP.
  6. **FIN** : indique que l'émetteur n'a plus de données à transmettre. Demande de libération de connexion.
- **Window** : 16 bits – Nombre d'octets de données à partir de celui indiqué par le champ Acknowledgment.
- **Checksum** : 16 bits
- **Urgent Pointer** : 16 bits – Ce champ est interprété uniquement si le bit de contrôle URG est à 1. Le pointeur donne le numéro de séquence de l'octet qui suit les données urgentes.
- **Options** : variable entre 0 et 44 octets
  Il existe 2 formats d'options : un seul octet de catégorie d'options ou un octet de catégorie d'options + un octet de longueur d'options + l'octet des données de l'option.

Le mode connexion avec accusé de réception

Ce mode avec connexion utilise 3 phases distinctes :

- Établissement de la connexion,
- transfert de données,
- libération de la connexion.



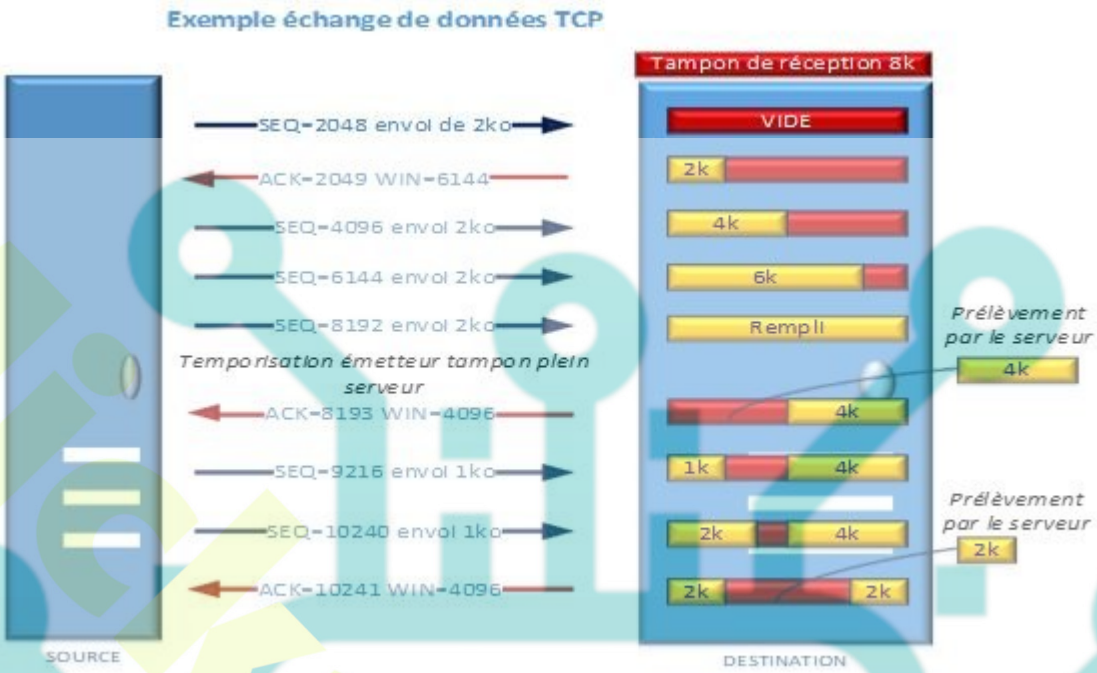
3 poignées de mains - Three way Handshake

Une communication TCP est identifiée par le quadruplet (adresse IP source, port source, adresse IP destination, port destination).

L'option la plus courante dans TCP est l'annonce de la taille maximum de segment (MSS : Maximum Segment Size)

Cette option est présente dans les segments ayant le bit SYN positionné pour indiquer quelle est la quantité maximale de données que veut recevoir l'émetteur.

Lorsque la connexion est locale, le MSS est fixé à la MTU du protocole de niveau 2 moins la taille des entêtes IP et TCP : pour un réseau Ethernet le MSS sera fixé à 1460 dans la plupart des cas.



Gestion de tampon TCP

Contrôle de flux

TCP fournit un moyen au destinataire pour contrôler le débit de données envoyées par l'émetteur. Ceci est obtenu en retournant une information de "fenêtre" avec chaque accusé de réception, indiquant la capacité de réception instantanée en termes de numéros de séquence.
Ce paramètre noté "window" indique le nombre d'octets que l'émetteur peut envoyer avant une autorisation d'émettre ultérieure.

On parle de fenêtre coulissante dans le cadre des connexions TCP, c'est à dire que l'on envoie plusieurs paquets en même temps avant d'avoir eu l'accusé réception. La machine réceptrice stocke alors les paquets dans un buffer (fenêtre) et les traite en même temps qu'elle reçoit d'autres paquets. Une fois un paquet traité, elle envoie un ACK et fait glisser sa fenêtre pour stocker en mémoire les paquets suivants.

La fenêtre coulissante (sliding Window), est employée pour transférer des données entre les hôtes. La fenêtre définit le volume de données susceptibles d'être passées via une connexion TCP, avant que le récepteur n'envoie un accusé de réception.

Chaque ordinateur comporte une fenêtre d'émission et une fenêtre de réception qu'il utilise pour bufférisér les données en continu, sans devoir attendre un accusé de réception pour chaque paquet.

Cela permet au récepteur de recevoir les paquets dans le désordre et de profiter des délais d'attente pour réorganiser les paquets. La fenêtre émettrice contrôle les données émises, si elle ne reçoit pas d'accusé de réception au bout d'un certain temps, elle retransmet le paquet.

https://www.youtube.com/watch?v=LnbvhoxHn8M

Gestion de fenêtres TCP

Silly window Syndrome

Si le tampon d'envoi est toujours plein, seul des petits paquets sont envoyés. L'émetteur doit éviter d'envoyer de petits segments qui saturent la connexion.
Coté récepteur il ne faut pas notifier de fenêtre de réception trop petites.

Exemple : après avoir envoyé une taille de 0, attendre d'avoir libérer la moitié du tampon avant d'envoyer une notification non nulle.

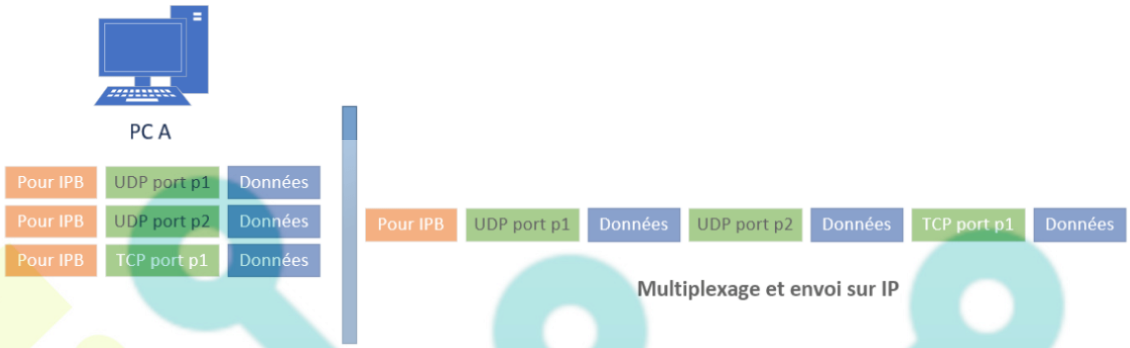
Une autre technique consiste à ne pas envoyer tout de suite les acquittements (500 ms) tant que la notification de la taille de réception est de 0.

Multiplexage TCP/UDP

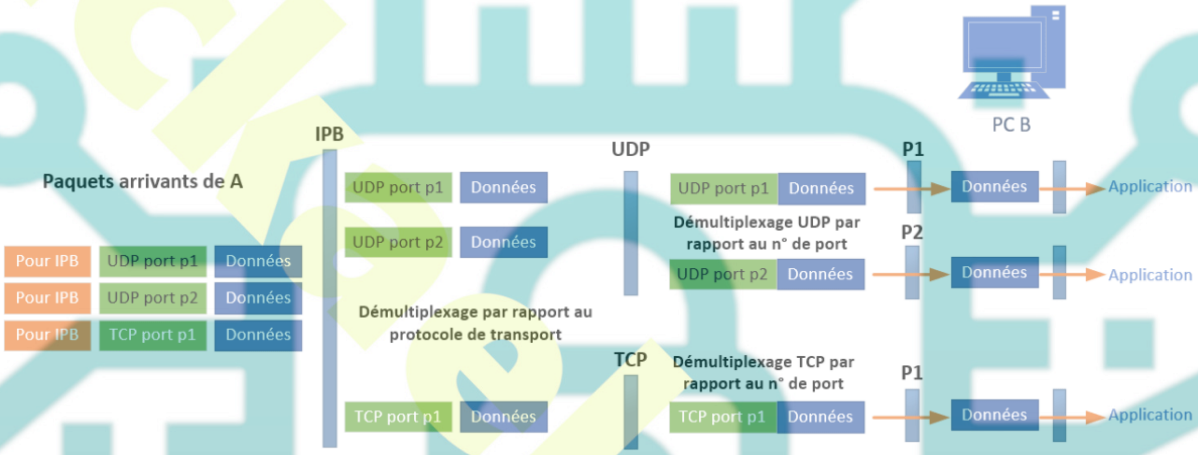
Pour permettre à plusieurs tâches d'une même machine de communiquer simultanément, les protocoles définissent un ensemble d'adresses et de ports pour la machine.

Une "socket" est défini par l'association des adresses Internet source, destinataire, ainsi que les deux numéros de port à chaque extrémité.

Une connexion nécessite la mise en place de deux sockets. Un socket peut être utilisé par plusieurs connexions distinctes. L'affectation des ports aux processus est établie par chaque ordinateur.



Multiplexage



Démultiplexage

Les protocoles de la couche application

BOOTP

Bootstrap Protocol est un protocole réseau d'amorçage (s'appuyant sur UDP), qui permet à une machine cliente sans disque dur de découvrir sa propre adresse IP, l'adresse d'un hôte serveur et le nom d'un fichier à charger en mémoire pour exécution.

Comme RARP, il sert principalement à fournir son adresse IP à une machine que l'on démarre sur un réseau. Cependant, il est plus intéressant que RARP car il se situe à un niveau supérieur, il est donc moins lié au type de matériel du réseau. De plus, il transmet plus d'informations que RARP qui lui ne renvoie qu'une adresse IP.
BOOTP donne une adresse IP de manière statique en utilisant un serveur possédant un fichier d'adresses IP à distribuer à chaque machine. Le transfert du fichier utilisera typiquement le protocole TFTP.

Protocole TELNET

Le protocole Telnet est un protocole standard d'Internet qui permet de gérer un terminal réseau virtuel. Ce protocole est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3)

Telnet est un protocole de transfert de données non sûr, car les données circulent en clair sur le réseau. Lorsque le protocole Telnet est utilisé à partir d'un hôte distant, une connexion virtuelle est ouverte sur le serveur.

Protocole SSH

Ce protocole est un protocole de connexion sécurisée via des clés de chiffrement.
Le protocole SSH a été conçu avec l'objectif de remplacer les différents programmes rlogin, telnet, rcp, ftp et rsh.

Protocoles NFS et SMB

Ces 2 protocoles majeurs dans l'accès aux fichiers distants sont utilisés dans UNIX/LINUX et WINDOWS.

NFS

Le Network File System est historiquement un protocole conçu et utilisé par Sun Microsystems, en 1984. Ce réseau est utilisé pour Linux ou Unix. Le NFS permet à un utilisateur d'accéder, via son ordinateur (le client), à des fichiers stockés sur un serveur distant.

SMB

Le protocole SMB (Server Message Block) est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.

Protocole HTTP

Le protocole HTTP (HyperText Transfer Protocol) permet de transférer des données sur Internet (pages HTML)

Le client (navigateur) envoie des requêtes au serveur WEB (HTTPd) à l'aide d'URL (http://nom_serveur/chemin_d'accès) en effectuant une demande de connexion au port TCP 80.

Lors de la connexion le client et le serveur négocient pour l'objet envoyé, les caractéristiques de connexion (accès authentifié ou non), de représentation (format des images…), de contenu (langage) et de commande (durée de validité d'une page)

Exemple de demande d'un client

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: fr-FR\r\n
    User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
    Accept-Encoding: gzip, deflate\r\n
    Host: www.google.fr\r\n
    Connection: Keep-Alive\r\n
    [truncated] Cookie: PREF=ID=a87327679ce230a9:U=e99368521eb0749e:FF=0:T
    \r\n
```

En tête HTTP demande client

Réponse du seveur

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Last-Modified: Mon, 07 Nov 2011 05:34:12 GMT\r\n
    ETag: "/f9JaRugbCdGbYGp30bKpbE8KsY="\r\n
    Server: Microsoft-IIS/7.5\r\n
    VTag: 279297100500000000\r\n
    P3P: CP="ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo
    X-Powered-By: ASP.NET\r\n
    Content-Type: text/javascript; charset=utf-8\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
    X-AspNet-Version: 2.0.50727\r\n
  Content-Length: 16599\r\n
    Cache-Control: public, max-age=385\r\n
    Expires: Sat, 24 Mar 2012 18:27:57 GMT\r\n
    Date: Sat, 24 Mar 2012 18:21:32 GMT\r\n
    Connection: keep-alive\r\n
```

En tête HTTP réponse serveur

HTML

L'Hypertext Markup Language est conçu pour représenter les pages web. C'est un langage de balisage permettant d'écrire de l'hypertexte. HTML permet de mettre en forme le contenu des pages, d'inclure des images, des formulaires de saisie et des programmes.

XML

L'Extensible Markup Language est un langage informatique de balisage générique. Cette syntaxe est dite « extensible », car elle permet de définir différents langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG…
L'objectif initial est de faciliter l'échange automatisé de contenus complexes entre systèmes d'informations hétérogènes.

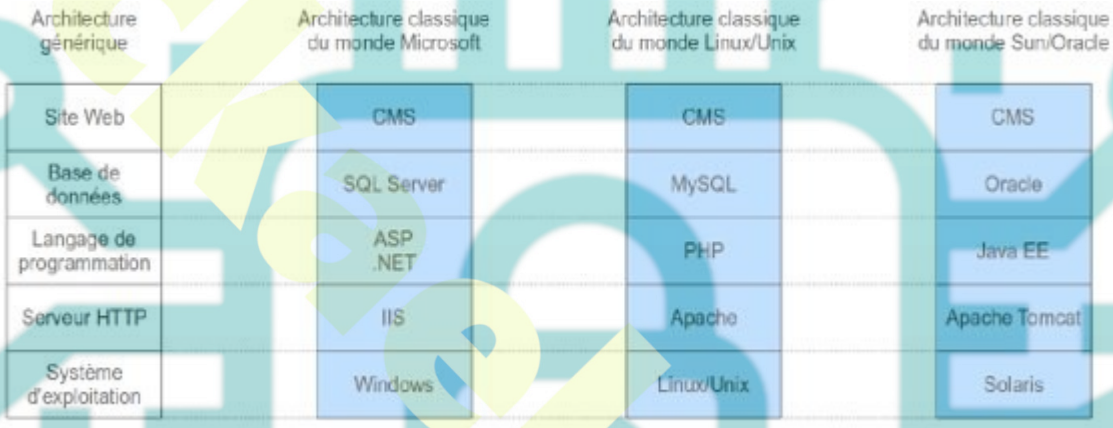
Les serveurs WEB/FTP

Un serveur web est un ordinateur connecté à Internet et sur lequel sont hébergés des sites web, composés de pages HTML.
La fonction d'un serveur web est de répondre aux requêtes des navigateurs Internet.

Les principaux produits

Apache (libre), IIS (Microsoft), Apache Tomcat (Sun), Zeus Web Server (Unix)

Architecture



Architecture des serveurs Web

Sécurité

Le protocole HTTPS (HyperText Transfer Protocol Secure) est un protocole HTTP auquel il a été ajouté une couche de chiffrement SSL (Secure Socket Layer). Le protocole HTTPS existe pour pallier aux défauts du protocole HTTP.

Le protocole HTTPS permet aux visiteurs d'un site web de vérifier l'identité de l'éditeur et de l'organisme de certification grâce à un certificat électronique. Le certificat SSL garanti par chiffrement la confidentialité et l'intégrité des données envoyées par les visiteurs sur un site internet.

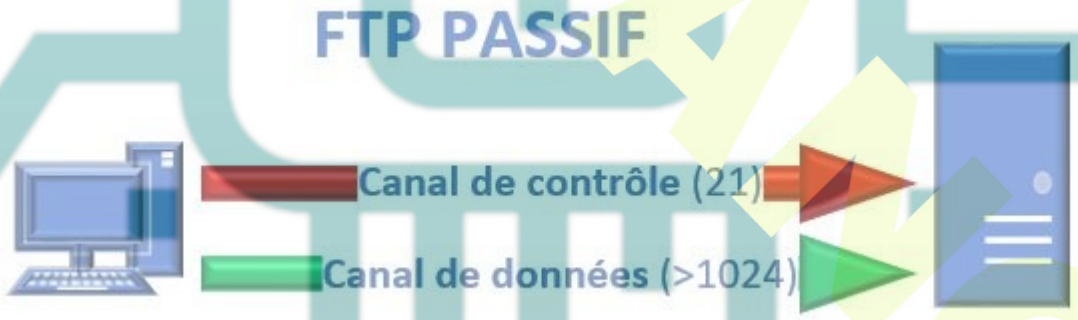
Protocole FTP

Le protocole FTP est un protocole de transfert de fichiers qui permet un partage de fichiers entre machines distantes.

Lors d'une connexion FTP, deux canaux de transmission sont ouverts :
1. Un canal pour les commandes (canal de contrôle)
2. Un canal pour les données.

Il est à noter que l'on peut ouvrir des sessions FTP au travers d'un navigateur.

C'est le mode par défaut des clients FTP. Le client établi dans un premier temps une session TCP sur le port 21 (FTP) du serveur. Une fois la session établie et l'authentification FTP acceptée, c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données puis le serveur établit une session TCP (avec le port source 20, FTP-DATA) vers un port dynamique du client.



Le mode passif peut être conseillé lorsque les clients se trouvent derrière un Firewall/NAT. Dans ce mode, toutes les initialisations de sessions TCP se font à partir du client.

Le client établi une première session TCP sur le port 21 (FTP) du serveur. Une fois la session établie et l'authentification FTP acceptée, on demande au serveur de se mettre en attente de session TCP grâce à la commande PASV.

Le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client suite à la commande PASV. Alors, le client peut établir une seconde session TCP sur un port dynamique vers le serveur.

Sécurité

- **FTPS** est FTP avec SSL pour la sécurité. Il utilise un canal de contrôle et ouvre de nouvelles connexions pour le transfert de données. Comme il utilise SSL, il nécessite un certificat. Les ports utilisés sont le 989 et 990.
- **SFTP** (SSH File Transfert Protocol ou Secure File Transfert Protocol) est un protocole de transfert de fichiers qui s'appuient sur SSH. On peut donc le voir comme une extension de SSH.
  SFTP utilise le port par défaut 22 comme SSH et l'établissement de la connexion est identique. Cela implique que l'envoie du mot de passe est chiffré.

Protocole NTP

Le NTP (Network Time Protocol) est un protocole permettant de synchroniser l'horloge d'un ordinateur avec celle d'un serveur de référence.

Le NTPv3 utilisé permet une synchronisation de l'ordre de la milliseconde ou mieux sur des réseaux locaux (LAN), et avec des écarts inférieurs à 10 secondes sur des réseaux nationaux (WAN).

https://services.renater.fr/ntp/serveurs_francais

Serveur de temps français

Protocole SMTP

C'est le protocole standard pour de transférer le courrier d'un client vers un serveur ou de serveur à serveur.
C'est un protocole très simple qui se contente de transférer le courrier sans se soucier de savoir comment le serveur accepte le courrier, ni comment le courrier est présenté, ni comment le courrier est stocké et ni la fréquence de remise du courrier.

Voici un exemple d'échange de messages entre un client (toto.bo.fr) qui envoie un mail aux utilisateurs dupond et dupuis du domaine tox.fr

S 220 mail.box.fr Simple Mail Transfer Ready
C HELO bo.fr
C MAIL FROM : <toto@bo.fr>
S 250 OK
C RCPT TO <dupond@box.fr>
S 250 OK
C RCPT TO <dupuis@box.fr>
S 550 No such user here
C DATA
S 354 start mail input
C émission
C corps du message
C fin du message
S 250 OK

Sécurité

SMTPS est une méthode de sécurisation du utilisant la couche transport en enveloppant SMTP dans TLS. Conceptuellement, cela ressemble à la façon dont HTTPS encapsule HTTP dans TLS (port 587 ou 465).

Protocole POP

Le protocole POP (Post Office Protocol) permet de récupérer le courrier dans une boite aux lettres située sur un serveur.
Tous les fichiers sont téléchargés et disponibles et accessibles localement.

Le protocole POP3 gère l'authentification à l'aide d'un nom d'utilisateur et d'un mot de passe. Il n'est en revanche pas sécurisé car les mots de passe, au même titre que les courriels, circulent en clair sur le réseau.

Ce protocole bloque la boîte aux lettres lors de la consultation, ce qui signifie qu'une consultation simultanée par 2 utilisateurs d'une même boîte est impossible.

Une fois les e-mails récupérés, ils sont généralement supprimés de la boîte aux lettres.

Protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) est un protocole plus évolué que POP3, car il permet de gérer plusieurs accès simultanés, de ne télécharger que les en-têtes des messages et de gérer de multiples critères.

A la différence du protocole POP, qui transfère les messages de votre boîte aux lettres sur votre ordinateur puis les efface du serveur, IMAP effectue une synchronisation des messages et des dossiers (boîte de réception, messages envoyés, brouillons, archives, etc.) entre le serveur et votre terminal.

Votre messagerie reste stockée dans son intégralité sur le serveur. Vous pouvez donc y accéder par différents terminaux, vous aurez accès aux mêmes données. Toute action que vous effectuez depuis un terminal sera automatiquement reportée sur le serveur.

Sécurité

IMAPS (IMAP over SSL) permet l'accès sécurisé au serveur en utilisant le protocole SSL. Il utilise le port TCP 993.

Format MIME

MIME (Multipurpose Internet Mail Extension) permet la transmission de données non-ASCII par courrier électronique. Cette extension permet de coder tous types de données (texte, image, audio, vidéo)

Sécurité

S/MIME est un standard qui s'appuie sur les des certificats pour signer et chiffrer des courriels.

Processus d'envoi et de réception d'un mail

Analyse d'un courrier

`Received: from server.bidon.fr(184.184.184.184)`	Serveur par lequel a transité le message
`by smtp.monFAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC`	Serveur destinataire
`Received: from besthacker ([100.100.100.100])`	Expéditeur du message
`by server1.hack.com (8.7.5) ID LAA28548;`	Serveur expéditeur
`Message-Id: <599b403f348fd8529caa342af911e6ac1@johntheripper>`	Nom réseau de l'ordinateur de l'expéditeur
`Reply-To: bof@gmail.com`	Adresse où sera acheminée votre réponse
`From: hackhack@meeto.com`	Adresse présumée de l'expéditeur
`To: moi@monFAI.fr`	Mon adresse mail
`Subject: Message important vous avez été piraté`	Objet du mail
`X-Mailer: Microsoft Outlook Express 4.72.3110.5` **Ou user-agent**	Client mail utilisé par l'expéditeur
`MIME-Version: 1.0 Content-Type: text/plain; charset="ISO-8859-2"`	Version de l'encodage

Réception mail

https://mxtoolbox.com/EmailHeaders.aspx

Analyser les en-tête