

# TCP/IP

**MODULE 05**

**COUCHE  
APPLICATIONS**

# Plan de la séance

## Protocoles de la couche Transport

- Fonctions de la couche ;
- Accès Internet  
HTTP et HTTPS ;
- Courrier électronique  
SMTP, POP3 et IMAP4 ;
- Transfert de fichiers  
FTP, SFTP et TFTP ;
- Accès à distance  
Telnet et SSH ;
- Gestion des hôtes  
DHCP et DNS ;
- Gestion réseau  
SNMP et NTP ;
- Voix sur IP (VoIP)  
SIP et RTP.

# **Couche Applications**



# Couche Applications

## Fonctionnement général

Pour désigner les informations transmises et leur enveloppe, selon le niveau concerné, on parle de **message (ou de flux) entre applications**, de datagramme (ou segment) au niveau TCP, de paquet au niveau IP, et enfin, de trames au niveau de l'interface réseau (Ethernet ou Token Ring).

# Couche Applications

## Fonctionnement général

Les protocoles du niveau Application les plus connus sont ...

- **HTTP** (*HyperText Transfer Protocol*) permet l'accès aux documents HTML et le transfert de fichiers depuis un site WWW ;
- **FTP** (*File Transfer Protocol*) pour le transfert de fichiers s'appuie sur TCP et établit une connexion sur un serveur FTP ;
- **DNS** (*Domain Naming Service*) et **DHCP** (*Dynamic Hosts Configuration Protocol*) pour la configuration IP des hôtes ;

# Couche Applications

## Fonctionnement général

Les protocoles du niveau Application les plus connus sont ...

- **SSH** (*Secure shell*) pour les connexions à distance en émulation terminal à un hôte Linux ;
- **SMTP** (*Simple Mail Transfer Protocol*) pour la messagerie électronique (UDP et TCP).  
Il travaille conjointement avec **POP** et **IMAP** ;
- **SNMP** (*Simple Network Management Protocol*) et NTP (*Network Time Protocol*) pour l'administration du réseau ;
- **NFS** (*Network File System*) pour le partage des fichiers Linux.

# Couche Applications

## Fonctions

La couche Application du modèle TCP/IP ...

- **identifie et détermine la disponibilité des partenaires de communication** voulus ;
- **synchronise les applications coopératives** ;
- **établit une entente sur les procédures de reprise sur incident et de contrôle de l'intégrité** des données.

La couche Application propose un **ensemble complet de programmes d'interface à Internet**.

À chaque type d'application correspond un protocole d'application qui lui est propre.

# Couche Applications

## Fonctions

Exemple de service de la couche Application ...

- Les **programmes de messagerie électronique** supportent les protocoles de couche application SMTP, POP3 et IMAP4 pour le courrier électronique ;
- Les **programmes d'accès distant** utilisent le protocole SSH afin de se connecter directement aux ressources distantes ;
- Les **utilitaires de transfert de fichiers** utilisent le protocole FTP pour copier et déplacer les fichiers entre emplacements distants.  
Le protocole TFTP (Trivial File Transfer Protocol) est également un protocole de transferts de fichiers ;
- Les **outils de saisie et de contrôle des données** réseau utilisent le protocole SNMP et NTP ;
- Le **protocole d'accès Internet** comme HTTP ;
- Les **protocoles de gestion des hôtes** comme DHCP et DNS.



# Couche Applications

## Accès Internet

### HTTP (*Hypertext Transfert Protocol*)

HTTP est un **protocole de communication client-serveur développé pour le World Wide Web**. HTTPS (avec S pour *secured*) est la **variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS**.

**HTTP peut fonctionner sur n'importe quelle connexion fiable**. Toutefois, dans les faits on utilise **le protocole TCP comme couche de transport**.

Un serveur HTTP utilise alors par défaut le **port TCP 80** (**TCP 443** pour HTTPS).

# Couche Applications

## HTTP Méthodes

Pour le protocole HTTP, une **méthode est une commande spécifiant un type de requête**, c'est-à-dire qu'elle demande au serveur d'effectuer une action.

En général l'action concerne **une ressource identifiée par l'URL qui suit le nom de la méthode**.

# Couche Applications

## HTTP Méthodes

Il existe de nombreuses méthodes, les plus courantes étant GET, HEAD et POST ...

- **GET**

C'est la méthode la plus courante pour demander une ressource.

Une requête GET est sans effet sur la ressource, il doit être possible de répéter la requête sans effet ;

- **HEAD**

Cette méthode ne demande que des informations sur la ressource, sans demander la ressource elle-même ;

- **POST**

Cette méthode est utilisée pour transmettre des données en vue d'un traitement à une ressource (le plus souvent depuis un formulaire HTML).

L'URI fourni est l'URI d'une ressource à laquelle s'appliqueront les données envoyées.

# Couche Applications

## HTTP

### Du client au serveur

La liaison entre le client et le serveur n'est pas toujours directe car il peut exister des hôtes intermédiaires servant de relais ...

- Un **proxy** (ou serveur mandataire) peut modifier les réponses et requêtes qu'il reçoit et peut gérer un cache des ressources demandées ;
- Une **passerelle** (ou *gateway*) est un intermédiaire modifiant le protocole utilisé ;
- Un **tunnel** transmet les requêtes et les réponses sans aucune modification, ni mise en cache.

# Couche Applications

## HTTP Identification

HTTP permet l'identification du visiteur par transmission d'un nom et d'un mot de passe.

Il existe **2 modes d'identification** ...

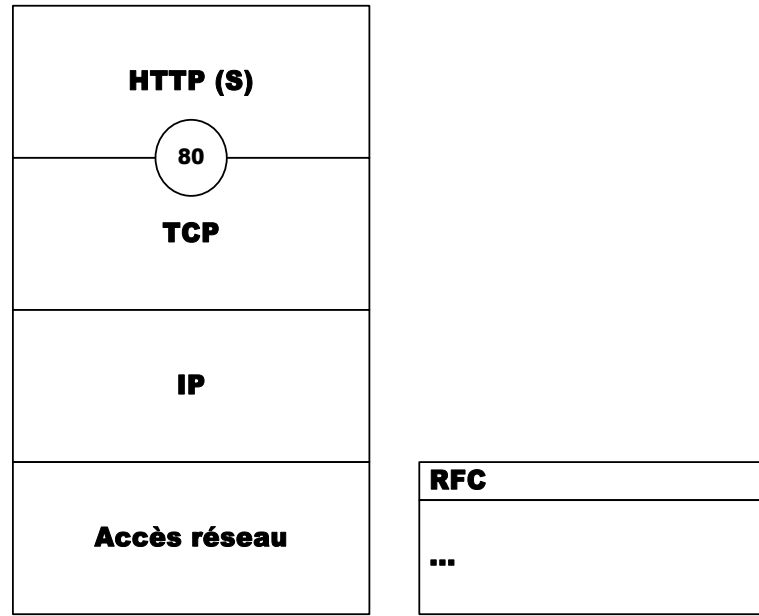
**Basic** et **Digest** (RFC 26176) ...

- Le **premier mode transmet le mot de passe en clair**, et ne doit donc être utilisé qu'avec le protocole HTTPS ;
- Le **deuxième mode permet une identification sans transmettre le mot de passe en clair**.

L'identification est cependant souvent effectuée par une couche applicative supérieure à HTTP.

# Couche Applications

## HTTP (S)



# Couche Applications

## Messagerie électronique SMTP, POP3 et IMAP4

Le courrier électronique permet l'envoi de messages entre des hôtes sur un réseau

### Présentation

Le courrier électronique, aussi simple soit-il à utiliser, repose sur un **fonctionnement plus compliqué que celui du web**.

Il est un des plus importants services réseau.

Pour la **plupart des utilisateurs son fonctionnement est transparent**, ce qui signifie qu'il n'est pas nécessaire de comprendre comment le courrier électronique fonctionne pour pouvoir l'utiliser.

Néanmoins, il est **important de comprendre le principe**.

# Couche Applications

## Messagerie électronique

### Fonctionnement du courrier électronique

Le fonctionnement du courrier électronique est basé sur l'utilisation d'une boîte à lettres électronique.

Lors de l'envoi d'un email, le message est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire.

Plus exactement, le message est envoyé au serveur de courrier électronique chargé du transport (nommé MTA pour *Mail Transport Agent*), jusqu'au MTA du destinataire. Sur internet, les MTA communiquent entre-eux grâce au protocole SMTP et sont logiquement appelés serveurs SMTP (parfois serveur de courrier sortant).

Le serveur MTA du destinataire délivre alors le courrier au serveur de courrier électronique entrant (nommé MDA pour *Mail Delivery Agent*), qui stocke alors le courrier en attendant que l'utilisateur vienne le relever.



# Couche Applications

## Messagerie électronique

Il existe deux principaux protocoles permettant de relever le courrier sur un MDA :

le protocole POP3 (*Post Office Protocol*), le plus ancien, permettant de relever son courrier et éventuellement d'en laisser une copie sur le serveur ;

le protocole IMAP (*Internet Message Access Protocol*), permettant une synchronisation de l'état des courriers (lu, supprimé, déplacé) entre plusieurs clients de messagerie. Avec le protocole IMAP une copie de tous les messages est conservée sur le serveur afin de pouvoir assurer la synchronisation.

# Couche Applications

## Messagerie électronique

### Terminologie

Les termes suivants sont souvent utilisés lorsque l'on parle de services de messagerie ...

#### Agent de transport de message – MTA

**MTA** (abréviation de *Mail* ou *Message Transport Agent*), également appelé **relais de messagerie**, est un logiciel chargé de **transférer les messages électroniques d'un serveur vers un client** (et inversement).

#### Agent d'utilisateur de messagerie – MUA

**MUA** (abréviation de *Mail User Agent*) est un programme informatique **utilisé pour accéder aux boîtes de réception de l'utilisateur et les gérer**.

L'agent de messagerie est le terme technique utilisé pour **désigner un client de messagerie**.

Les exemples de MUA comprennent, entre autres, *Thunderbird*, *Outlook* et les interfaces de messagerie Web telles que *Gmail*, *Outlook.com*, ....

# Couche Applications

## Messagerie électronique

### Terminologie

Les termes suivants sont souvent utilisés lorsque l'on parle de services de messagerie ...

#### Agent de distribution du courrier – MDA

**MDA** (abréviation de *Message* ou *Mail Delivery Agent*) est la partie logicielle qui **envoie les courriers électroniques aux boîtes de réception de l'utilisateur**.

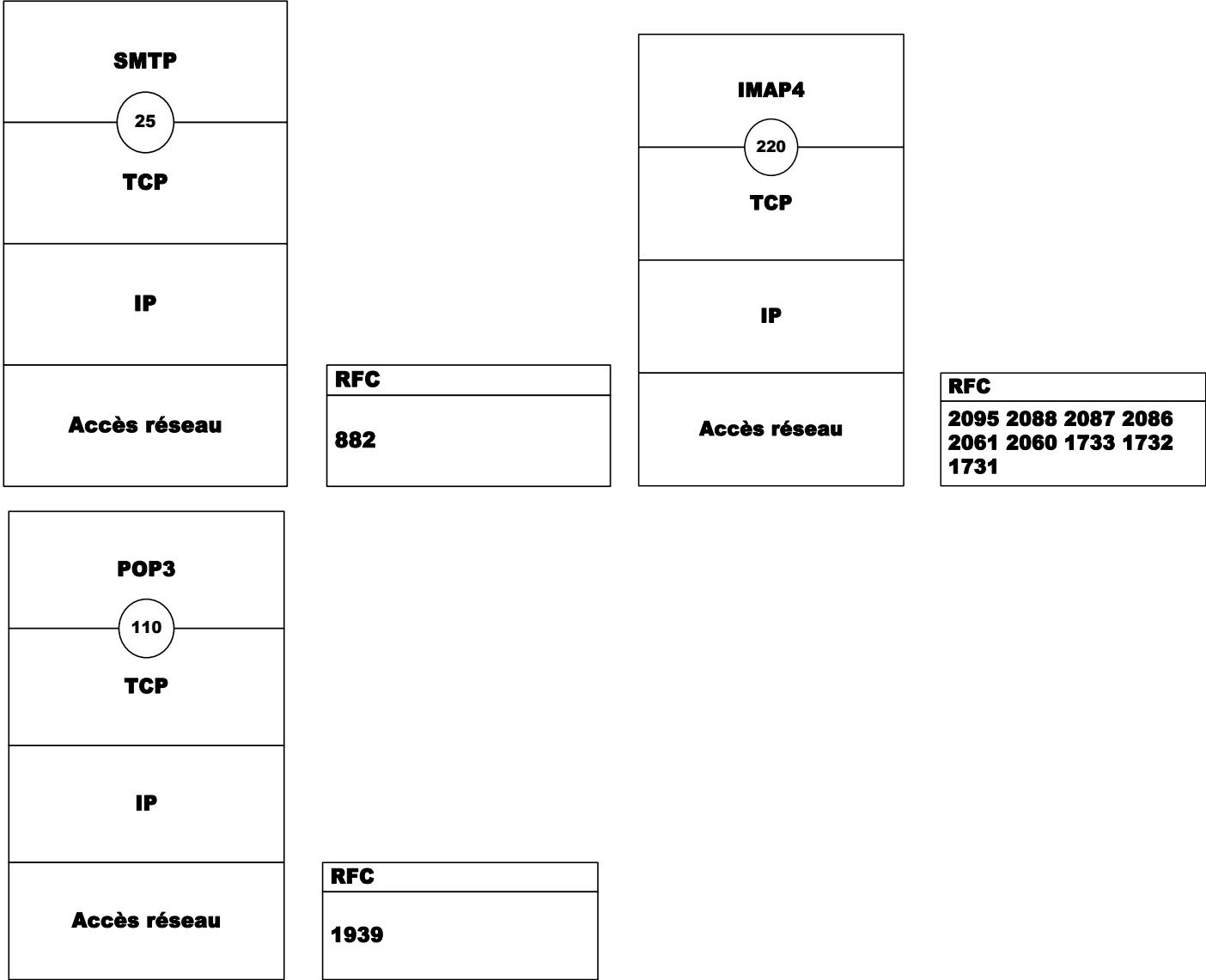
Le MDA se charge également de l'**authentification de l'utilisateur**.

#### Protocole de transfert de courrier simple – SMTP

Pour que ces **composants** puissent communiquer les uns aux autres, ils doivent **utiliser le même langage** (ou protocole), à savoir SMTP (*Simple Mail Transfer Protocol*), tel que défini dans le RFC 2821.

# Couche Applications

## Messagerie électronique



# Couche Applications

## Transfert de fichiers FTP

En règle générale, FTP est utilisé lorsque le **montage d'un partage permanent ou temporaire n'est pas souhaité** ou réalisable et la vitesse de transfert est un problème. Idéal pour les situations où les **fichiers sont partagés pour téléchargement uniquement**, par exemple lorsqu'un instructeur sur un réseau local de laboratoire local partage des fichiers binaires avec les débutants étudiants Linux.

Il est plus courant de **configurer un service FTP pour un accès anonyme et d'autoriser uniquement les téléchargements de fichiers**. Avec un accès FTP anonyme, au lieu d'un nom d'utilisateur attribué individuellement, un **nom d'utilisateur général, tel que anonymous ou ftp, est utilisé**. Il se peut qu'aucun mot de passe ne soit requis ou qu'une demande d'adresse de courriel ne soit demandée (bien que l'adresse de courriel ne soit pas vérifiée).

# Couche Applications

## FTP

### Connexions passives et actives

FTP utilise généralement **deux ports TCP**: le **port de données** et le **port de commande**.

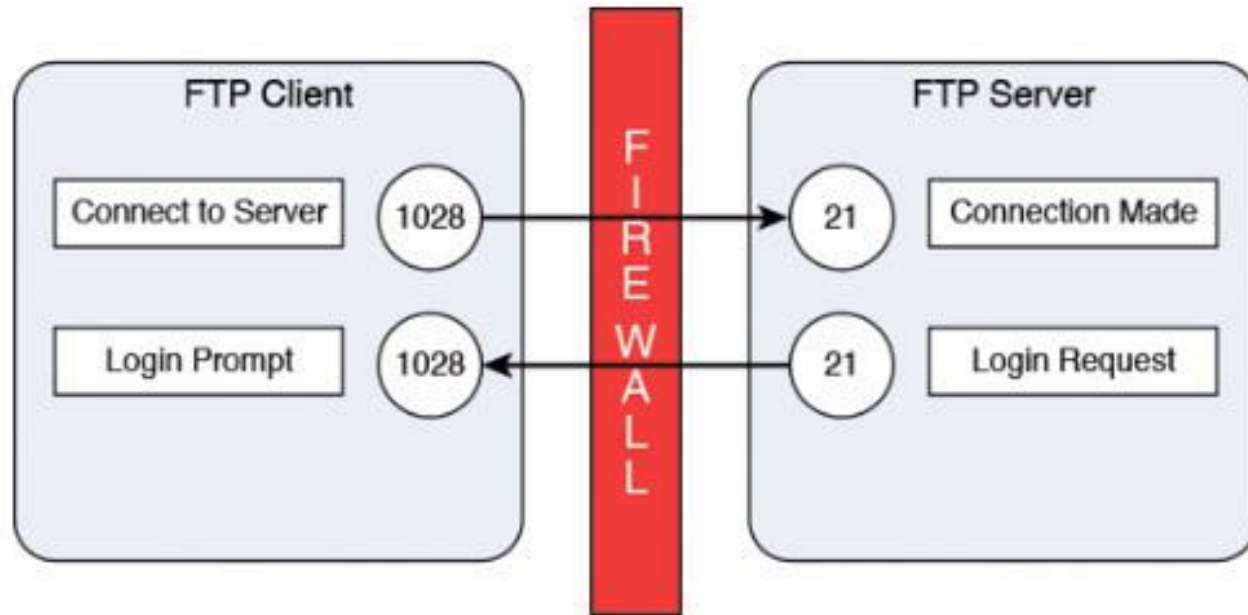
- Le **port de commande** est utilisé pour **envoyer des commandes** et **gérer les réponses aux commandes** ;
- Le **port de données** est utilisé pour le **transport des données de fichier**.

Il est important de savoir que **FTP utilise deux modes de fonctionnement ... passif et actif**.

# Couche Applications

## FTP

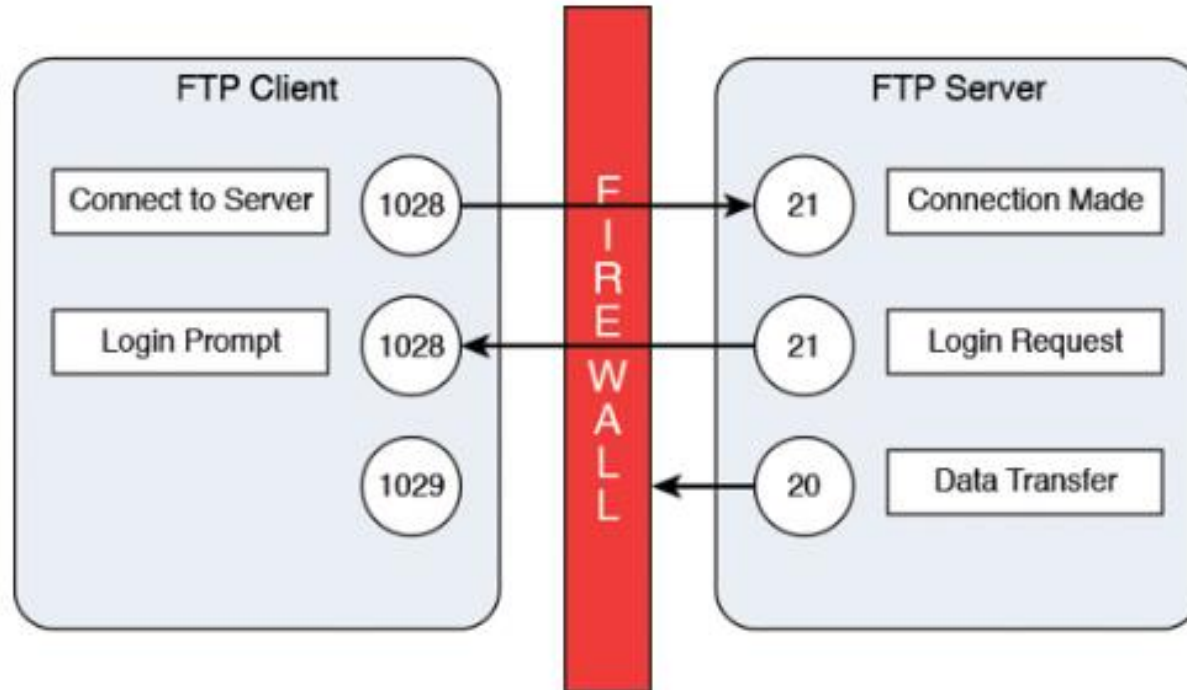
### Connexions passives et actives



# Couche Applications

## FTP

### Connexions passives et actives





# Couche Applications

## FTP

### En résumé ... par étapes

En mode actif, le serveur FTP et le client sont actifs pour établir les connexions.

De plus, le serveur FTP utilise ...

- le **port 20** comme **port de données**  
et
- le **port 21** comme **port de commande**.

# Couche Applications

## FTP

### En résumé ... par étapes

Les étapes de connexion de base en mode actif sont les suivantes ...

1. Le **client FTP sélectionne et ouvre un port aléatoire** non privilégié C (où C est  $> 1024$ ) pour lui servir de port de commande **afin d'envoyer et de recevoir des commandes** ;
2. Le **client FTP sélectionne et ouvre un autre port aléatoire non privilégié** D (où D est  $C + 1$ ) pour lui servir de port de données et commence à écouter les données du serveur FTP ;

# Couche Applications

## FTP

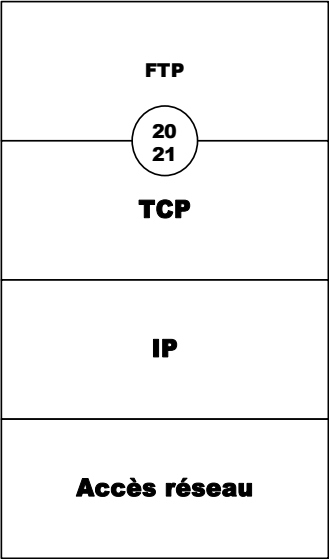
### En résumé ... par étapes

Les étapes de connexion de base en mode actif sont les suivantes ...

3. Le **client FTP** utilise son **port de commande** (port C) pour **informer le serveur FTP** à l'aide du port de commande du serveur (port 21) **qu'il écoute des données sur son port de données** (port D) ;
4. Le **serveur FTP** utilise son **port de commande** (port 21) pour **accuser réception de la demande**, qui est envoyée au port de commande du client FTP (port C) ;
5. Le **serveur FTP** utilise son **port de données** (port 20) pour se **connecter au port de données du client FTP** (port D).

# Couche Applications

## FTP



RFC
354 959

# Couche Applications

## Transfert de fichiers

### TFTP (*Trivial File Transfer Protocol*)

Le protocole TFTP permet de **télécharger des fichiers plus rapidement**. Cependant il **ne garantit pas la qualité du transfert** car il **utilise avec UDP** comme protocole de la couche Transport.

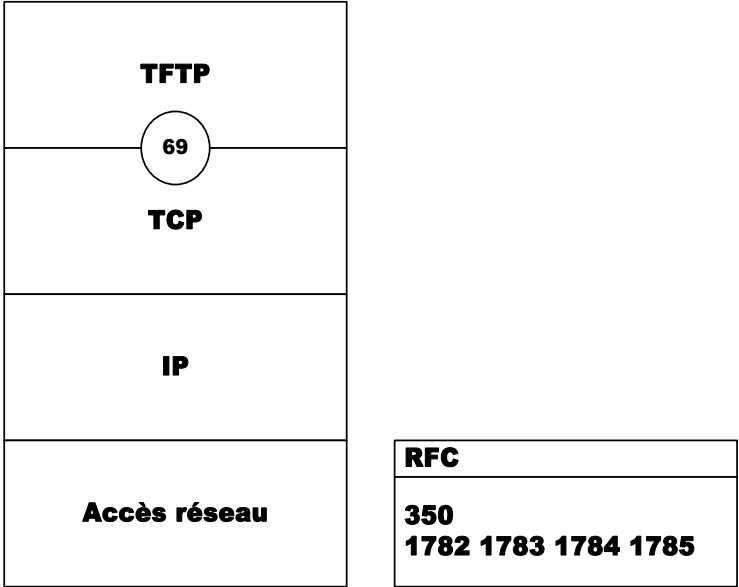
Puisque le **protocole TFTP utilise le protocole UDP** et possède donc sa propre correction d'erreur. TFTP propose ses propres **messages d'acquittement**.

Si un message d'acquittement n'est pas parvenu après un certain temps, **TFTP renvoie le paquet**.

**TFTP utilise une simple technique PAR**  
(*Positive Acknowledgement Retransmission*).

# Couche Applications

## TFTP



# Couche Applications

## Accès distant SSH

Secure SHell (SSH) est à la fois un **programme informatique** et un **protocole de communication sécurisé**.

Le protocole de connexion **impose un échange de clés de chiffrement en début de connexion**.

Par la suite, tous les **segments TCP** sont **authentifiés et chiffrés**.

Il devient alors **impossible (ou presque) d'utiliser un renifleur (*sniffer*) pour voir ce que fait un utilisateur**.

Le protocole SSH a été conçu avec l'**objectif de remplacer les différents protocoles non chiffrés** comme rlogin, telnet, rcp et rsh.

Habituellement le protocole **SSH utilise le port TCP 22**.

Il est **particulièrement utilisé pour ouvrir un shell sur un hôte distant**.

# Couche Applications

## Accès distant SSH

SSH peut également être utilisé pour **transférer des ports TCP d'un hôte vers un autre, créant ainsi un tunnel**.

Cette méthode est couramment utilisée afin de **sécuriser une connexion qui ne l'est pas** (par exemple le protocole de récupérations de **courrier électronique POP3**) en la faisant **transférer par le biais du tunnel chiffré SSH**.

Il est également possible de faire **plusieurs sauts entre consoles SSH**, c'est-à-dire ouvrir une console sur un serveur, puis, de là, en ouvrir une autre sur un autre serveur.



# Couche Applications

## Accès distant SSH

Les usages de base de SSH sont ...

- L'**accès à distance à la console en ligne commande** (shell), ce qui permet, entre autres, d'effectuer la totalité des opérations courantes et/ou d'administration sur un hôte distant ;
- Le **déport de l'affichage graphique** de l'hôte distant ;
- Le **transfert des fichiers en ligne de commande** ;
- Le **montage ponctuel et/ou automatique d'un répertoire distant**, soit en ligne de commande, soit à l'aide d'une interface graphique.

# Couche Applications

## Accès distant Tunnel SSH

Un tunnel, dans le contexte de réseaux informatiques, est une **encapsulation de données d'un protocole réseau dans un autre**, situé dans la **même couche du modèle en couches**, ou dans une **couche de niveau supérieur**.

Par exemple, pour faire passer le **protocole IPv6 par le réseau Internet actuel** (qui est en **grande partie en IPv4**) on va créer un **tunnel entre deux hôtes IPv4** ; ce tunnel, pour le protocole IPv6, semblera un **simple lien point-à-point** (un logiciel comme traceroute ne verra donc pas le tunnel).

# Couche Applications

## Accès distant Tunnel SSH

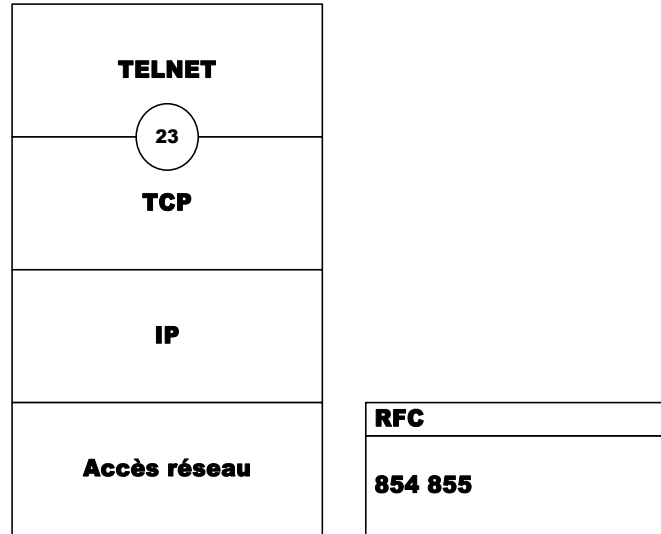
En sécurité, on crée souvent des **tunnels chiffrés**, par exemple comme le fait **SSH**. Les **données peuvent alors y circuler sans craindre d'être écoutées**. Les tunnels peuvent être utilisés pour **créer des réseaux privés virtuels (VPN)**.

Le **tunnel HTTP** est un cas particulier qui consiste à faire **passer une connexion explicitement interdite par un pare-feu** (le protocole SSH par exemple) **encapsulé dans un protocole HTTP presque toujours autorisé**.

C'est particulièrement utile quand le pare-feu ne bloque pas simplement les ports associés (22 pour SSH par exemple), mais analyse aussi les protocoles utilisés.

# Couche Applications

## Accès distant



# Couche Applications

## Protocoles de configuration des hôtes Protocole DHCP

*Dynamic Host Configuration Protocol* (DHCP) désigne le protocole réseau dont le rôle est d'**assurer la configuration automatique des paramètres TCP-IP d'un hôte**, notamment en lui assignant automatiquement une **adresse IP** et un **masque de sous-réseau**.

DHCP peut aussi configurer l'**adresse de la passerelle par défaut**, des **serveurs de noms DNS** et de **nombreux autres paramètres**.

DHCP apporte une **solution à deux inconvénients ...**

- **Seuls les hôtes en service utilisent une adresse** de l'espace d'adressage ;
- Toute **modification des paramètres** (adresse de la passerelle, des serveurs de noms) **est répercutée sur les stations lors du redémarrage**.

La modification de ces paramètres est **centralisée sur les serveurs DHCP**.

# Couche Applications

## **DHCP**

### **Possibilités offertes**

On compte parmi les avantages de l'utilisation de DHCPv4 les suivants ...

- **Vérification rapide des adresses IP et autres paramètres de configuration TCP/IP ;**
- **Configuration de l'étendue d'adresses IP se fait de façon centralisée ;**
- **Non nécessité de modifier manuellement chaque client ;**
- **Non attribution de la même adresse IP à deux clients ;**
- **Attribution d'adresses fixes tout en permettant l'attribution dynamique des autres paramètres IP ;**
- **Risques d'erreurs d'écriture et de saisie sont diminués ;**
- **Reconfiguration d'un hôte plus facile si ce dernier est déplacé d'un sous-réseau à un autre ;**
- **Meilleure répartition des adresse IP**  
(lorsqu'il y a plus d'hôtes que d'adresses IP disponibles).

# Couche Applications

## DHCP

### Limitations DHCPv4

Toutefois, le protocole possède **certaines limites** ...

- Un serveur DHCP ne dispose d'**aucun moyen de communiquer avec un autre serveur DHCP** ;
- Il faut que les **étendues d'adresses soient bien définies et ne se recoupent pas** ;
- Les routeurs ne laissent pas passer les **messages de diffusion** (sauf s'ils sont configurés pour laisser passer les messages BOOTP) ;  
Il faut donc installer l'**agent de relais DHCP** ;
- Une **erreur de configuration DHCP peut entraîner des résultats catastrophiques**.

# Couche Applications

## DHCP Fonctionnement

DHCP fonctionne sur le **modèle client-serveur...**

- un serveur, qui **détient la politique d'attribution des configurations IP, envoie une configuration donnée pour une durée donnée** à un client donné (typiquement, un hôte qui vient de démarrer ou d'établir une connexion avec le réseau local).

Le **serveur va servir de base pour toutes les requêtes DHCP** (il les reçoit et y répond), aussi doit-il avoir une configuration IP fixe. Dans un réseau, on peut donc n'avoir qu'**un seul hôte avec adresse IP fixe** : le serveur DHCP.



# Couche Applications

## DHCP Fonctionnement

Le protocole DHCP s'appuie entièrement sur **BOOTP** : il en **reprend le mécanisme de base** (ordre des requêtes, mais aussi le format des messages). **DHCP est une extension de BOOTP.**

Quand un hôte **vient de démarrer ou d'établir une connexion au réseau**, il **ne possède pas de configuration réseau** (même pas de configuration par défaut), et pourtant, il doit **arriver à émettre un message sur le réseau** pour qu'on lui donne une vraie configuration.

La **technique utilisée est le diffusion** (*broadcast*) afin de trouver et dialoguer avec un serveur DHCP. L'hôte va simplement **émettre un paquet spécial**, dit de diffusion, sur **l'adresse IP 255.255.255.255** et sur le **réseau local**.

Ce paquet particulier **va être reçu par toutes les hôtes connectées** au réseau (particularité de diffusion).

# Couche Applications

## DHCP

### Fonctionnement

Lorsqu'un serveur DHCP reçoit ce paquet, il répond par un autre paquet de diffusion contenant toutes les informations requises pour la configuration. Si le client accepte la configuration, il renvoie un paquet pour informer le serveur qu'il garde les paramètres, sinon, il fait une nouvelle demande.

Les choses se passent de la même façon si le client possède déjà une adresse IP (négociation et validation de la configuration), sauf que le dialogue ne s'établit plus avec de diffusion.

# Couche Applications

## DHCP Fonctionnement

### Bail

Pour des raisons d'optimisation des ressources réseau, les **adresses IP sont délivrées pour une durée limitée**. C'est ce qu'on appelle un **bail (*lease*)**. Un client qui voit son **bail arriver à terme peut demander au serveur un renouvellement du bail**.

### Dynamique ou non ?

Un serveur **DHCP est censé fournir des adresses dynamiques** (un même hôte peut recevoir successivement 2 adresses différentes), mais il **peut fournir une adresse IP fixe à un client bien particulier**.

Ceci ne doit être utilisé que de manière modérée, sinon, le serveur DHCP ne sert à peu près plus à rien, mais cela peut se **révéler utile pour fournir l'adresse IP**, par exemple, à un **serveur TFTP qui va servir pour le démarrage** à distance des hôtes.

# Couche Applications

## DHCP

### Requêtes et les messages DHCP

On pourrait croire qu'un seul aller-retour peut suffire à la bonne marche du protocole.

En fait, il existe **plusieurs messages DHCP** qui permettent de **compléter une configuration ou de la renouveler ...**

Ces **messages** sont susceptibles d'être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client.

La valeur entre parenthèses est utilisée pour identifier ces requêtes dans les messages DHCP.

# Couche Applications

## DHCP

### Requêtes et les messages DHCP

- **DHCPDISCOVER** (1)  
Pour localiser les serveurs DHCP disponibles ;
- **DHCPOFFER** (2)  
Réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres ;
- **DHCPREQUEST** (3)  
Requête diverse du client pour par exemple prolonger son bail ;
- **DHCPDECLINE** (4)  
Annonce du client au serveur que l'adresse est déjà utilisée ;

# Couche Applications

## DHCP

### Requêtes et les messages DHCP

- **DHCPACK** (5)  
Réponse du serveur qui contient des paramètres et l'adresse IP du client ;
- **DHCPNAK** (6)  
Réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau ;
- **DHCPRELEASE** (7)  
Libération de l'adresse IP par le client ;
- **DHCPINFORM** (8)  
Demande du client pour des paramètres locaux (il a déjà son adresse IP).

# Couche Applications

## DHCP

### Requêtes et les messages DHCP

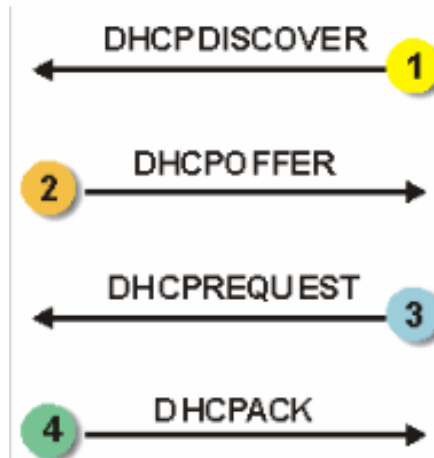
La valeur entre parenthèses est utilisée afin d'identifier ces requêtes dans les messages DHCP.

- La première requête émise par le client est un message **DHCPDISCOVER** ;
- Le serveur répond par un **DHCPOFFER**, en particulier pour soumettre une adresse IP au client ;
- Le client établit sa configuration, demande éventuellement d'autres paramètres, puis fait un **DHCPREQUEST** pour valider son adresse IP ;
- Le serveur répond simplement par un **DHCPACK** avec l'adresse IPv4 pour confirmation de l'attribution.

# Couche Applications

## DHCP

### Requêtes et les messages DHCP





# Couche Applications

## DHCP

### Adresse privée automatique (APIPA ou zeroconf)

Si les tentatives pour rejoindre un serveur DHCPv4 ont échouées, un client DHCP va s'attribuer automatiquement une adresse IP dans l'**étendue privée 169.254.0.1 à 169.254.255.254** et le **masque de sous-réseau 255.255.0.0**.

Le client DHCP s'assure à l'aide d'une requête ICMP que l'adresse choisie n'est pas déjà utilisée.

Ce **client va par la suite faire périodiquement un DHCPDISCOVER** afin de trouver un serveur pouvant lui fournir une configuration IP

Les clients qui n'utilisent pas cette fonctionnalité auront comme **adresse IPv4 0.0.0.0/32**.

# Couche Applications

## DHCP

### Réservation d'adresse IPv4

Il est possible d'effectuer des réservations d'adresses en limitant la possibilité d'octroi de cette adresse au client possédant une adresse physique ou un identifiant client donné.

Ceci peut s'avérer utile pour des hôtes dont l'adresse doit rester fixe mais dont on veut contrôler de manière centrale et automatique les autres paramètres IP.

Ce mécanisme est assuré par l'option 61 (voir RFC 21313).

# Couche Applications

## DHCP

### Réservation d'adresse IPv4

Le serveur DHCP choisi élabore un datagramme d'accusé de réception qui assigne au client ...

- l'adresse IP et son masque de sous-réseau,
- la durée du bail de cette adresse ;
- deux valeurs T1 et T2 qui déterminent le comportement du client en fin de bail, et éventuellement d'autres paramètres ...
  - adresse IP de la passerelle par défaut ;
  - adresses IP des serveurs DNS ;
  - ...

La liste des options que le serveur DHCP peut accepter est consultable dans la RFC 2132 : Options DHCP et Extensions fournisseur BOOTP.

# Couche Applications

## DHCP

### Client et serveur sur des segments différents

Lorsque le **serveur DHCP** et le **client** ne figurent pas sur le même **segment IP**, les **diffusions émises par ce dernier ne parviennent pas au serveur** parce que les routeurs, ne transmettent pas les diffusions générales (la RFC 1452 décrit toutefois la possibilité pour un aiguilleur de laisser passer les diffusions DHCP).

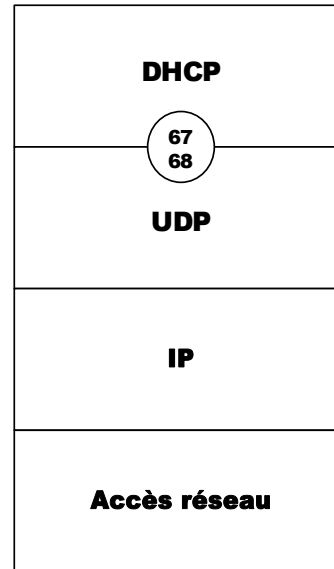
Dans ce cas on utilise un **agent de relais DHCP**.

Cet **hôte particulier** est configuré avec une **adresse IPv4 statique**, et **connaît l'adresse d'un serveur DHCP** auquel il transmet les **requêtes DHCP** qui lui parviennent sur le **port 68** (écouté par le programme agent de relais).

Il **diffuse sur son segment** (qui est aussi celui du client) les **réponses qu'il reçoit du serveur DHCP**.

# Couche Applications

## DHCP



RFC
903 2031 2032

# Couche Applications

## DNS

### Concepts de base

DNS (Domain Name Service) est un protocole conçu pour fournir une **résolution de nom en adresse IP**.

Il fait partie de la suite de protocoles TCP/IP standard et de l'un des protocoles pouvant fournir cette fonctionnalité ; les autres étant NIS et LDAP.

Ce qui distingue le DNS des autres protocoles similaires est que son **unique objectif est la résolution de noms** ; NIS et LDAP fournissent d'autres opérations de résolution.

DNS est également la solution de résolution de noms standard de facto pour la majorité des systèmes connectés à Internet.

# Couche Applications

## DNS

### Concepts de base

#### Fichier hosts.txt

Avant le DNS, la résolution d'un nom sur Internet devait se faire grâce à un **fichier texte appelé HOSTS.TXT** (RFC 60813) et copié sur chaque ordinateur du réseau par transfert de fichier.

En 1982, ce **système centralisé montre ses limites** et **plusieurs propositions de remplacement** voient le jour, parmi lesquelles le Domain Name System afin de gérer la croissance de l'internet en déléguant la gestion des noms de domaine à des serveurs de noms distribués.

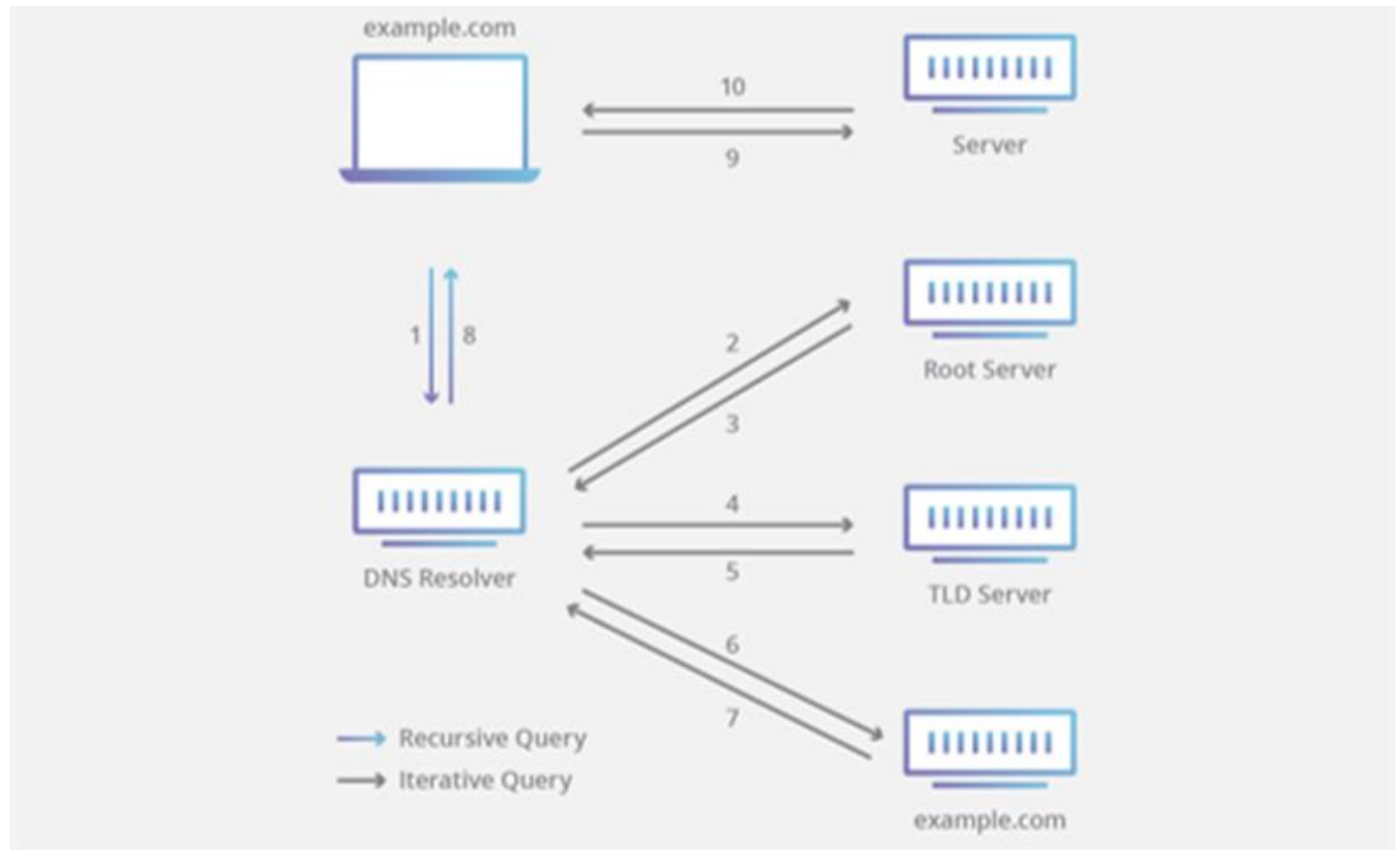
En **1987**, le **fichier hosts.txt contenait 5 500 entrées**, tandis que **20 000 hôtes étaient définis dans le DNS**.

# Couche Applications

## DNS

### Processus simplifié de résolution de noms

Voici un processus de résolution de noms générique ...



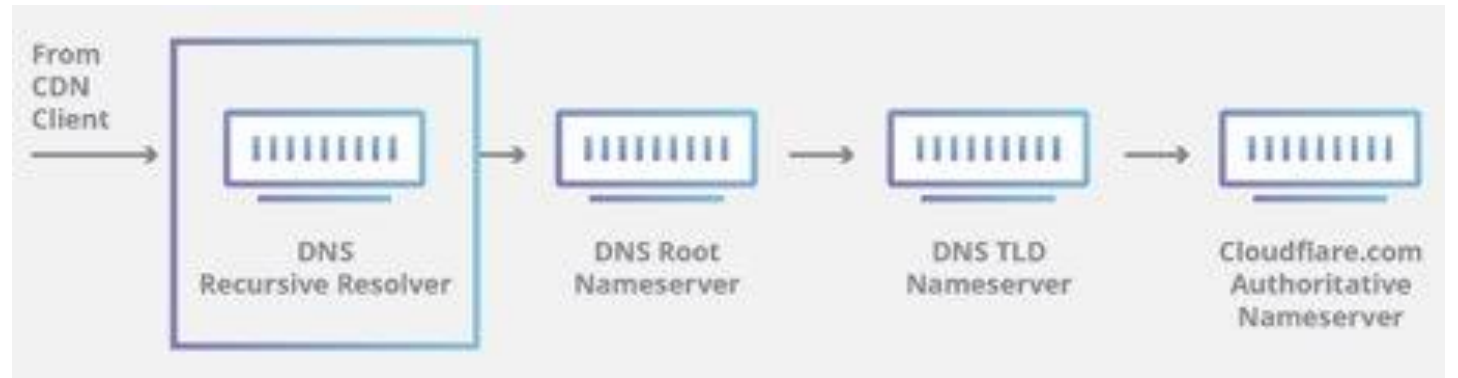


# Couche Applications

## DNS

### Processus simplifié de résolution de noms

Voici un processus de résolution de noms générique ...



# Couche Applications

## DNS

### Nom de domaine

On représente un nom de domaine en **indiquant les domaines successifs séparés par un point**, les **noms de domaines supérieurs se trouvant à droite**.

Par exemple, profsavard.info. ...

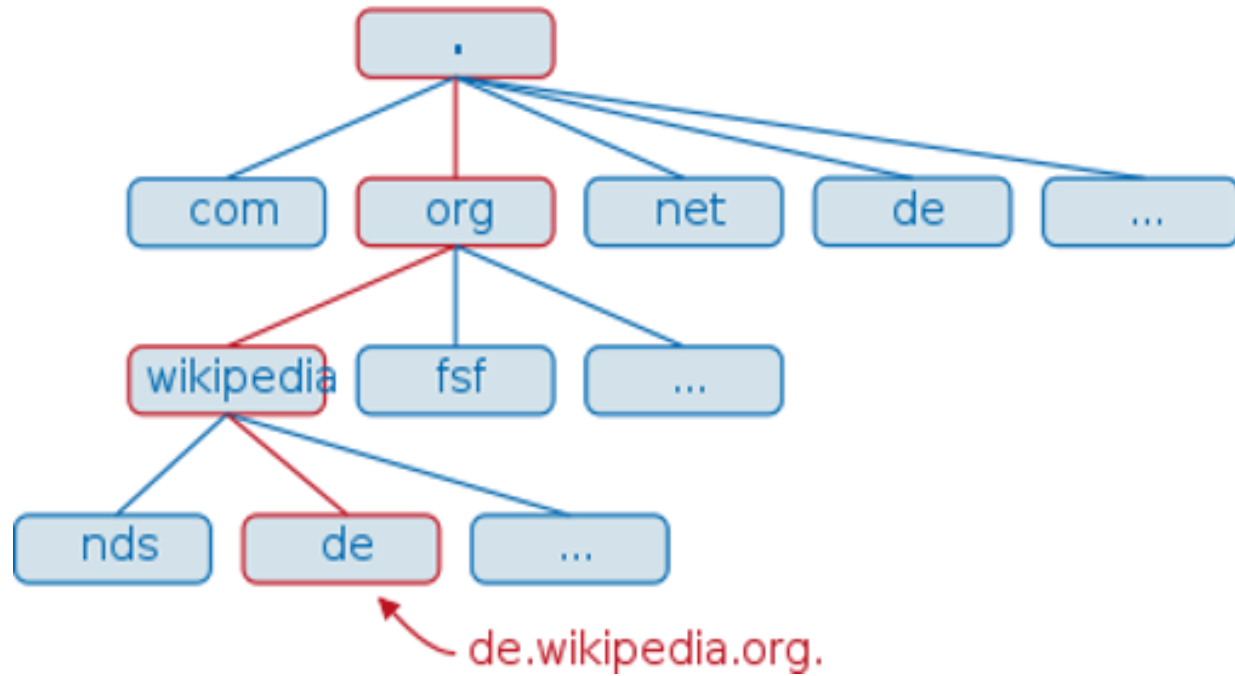
- Le **domaine info.** est un **TLD, sous-domaine de la racine** ;
- Le **domaine profsavard.** est un **sous-domaine de .info**.

Cette **délégation est accomplie en indiquant la liste des serveurs DNS associée au sous-domaine** dans le domaine de niveau supérieur.

Les noms de domaines sont donc **résolus en parcourant la hiérarchie depuis le sommet et en suivant les délégations successives**, c'est-à-dire en parcourant le nom de domaine de **droite à gauche**.

# Couche Applications

## DNS Noms de domaine



# Couche Applications

## DNS Résolveur

Le résolveur est un **acteur important dans la résolution de noms**.  
Le résolveur est un **programme ou une routine de bibliothèque qui forme une requête**,  
(par exemple ... Quelle est l'adresse IP de [www.profsavard.info](http://www.profsavard.info) ?) et  
qui doit obtenir la réponse à la requête.  
Un résolveur peut également faire **référence à un client DNS**.

Lorsqu'un résolveur crée sa requête, il **vérifie d'abord son propre cache DNS**, s'il est disponible.  
Si la réponse à cette requête est récente et que le cache du  
résolveur contient la réponse, le **processus de requête s'arrête**.

Les différentes résolutions de noms qui existent dans les différents  
caches DNS sont souvent **régies par un paramètre de durée de vie**  
(TTL).  
Une fois ce **délai écoulé**, la **résolution de noms est supprimée du cache**.

# Couche Applications

## DNS Résolveur

Si le cache du résolveur **ne contient pas la réponse**, le **résolveur envoie la requête à un serveur de noms interne ou externe (généralement un FAI)**. Cette requête est une **requête UDP unique** et le serveur de noms est généralement appelé serveur de noms récursif.

Si les **résolutions de noms précédentes** ont été stockées sur ce serveur (**mis en cache**) ou sur un serveur de mise en cache local, le serveur de **noms récursif répond à la requête** en utilisant une **seule réponse UDP contenant l'adresse IP appropriée**.

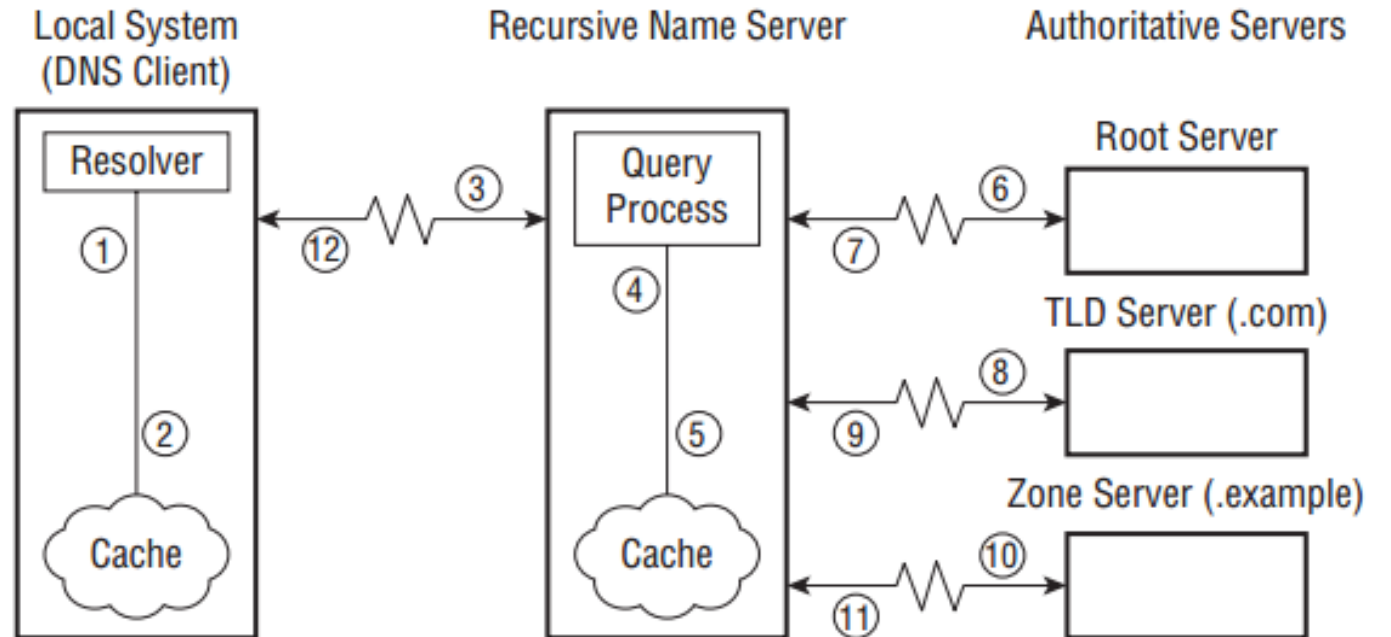
Si la **résolution de nom n'a pas été mise en cache**, le **serveur de noms récursif démarrera son propre processus de requête**.

Par exemple, lorsqu'un résolveur tente de déterminer l'adresse IP du site Web [www.example.com](http://www.example.com).

L'exemple de processus de résolution de noms est illustré à la figure suivante.

# Couche Applications

## DNS Résolveur



# Couche Applications

## DNS Résolveur

Chaque étape du processus de résolution de nom dans cet exemple de requête est ...

1. Le **résolveur recherche l'adresse IP** de [www.example.com](http://www.example.com) dans le cache de son propre serveur ;
2. Le résolveur est informé que les données de résolution de nom **ne se trouvent pas dans le cache local** ;
3. Le résolveur interroge le serveur de noms récursif de son FAI, qui **lance un processus de requête** ;
4. Le processus de requête du **serveur de noms récursif vérifie dans son cache local** l'adresse IP de [www.example.com](http://www.example.com) ;
5. Le **serveur de noms récursif interroge le serveur racine** faisant autorité pour connaître l'emplacement du serveur TLD .com ;
6. Le **serveur racine répond avec les informations faisant autorité** indiquant l'emplacement du serveur TLD.com ;

# Couche Applications

## DNS Résolveur

Chaque étape du processus de résolution de nom dans cet exemple de requête est ...

7. Le **serveur de noms récursif interroge le serveur TLD .com faisant autorité** afin de connaître l'emplacement du serveur de zone .exemple ;
8. Le **serveur TLD .com répond avec les informations faisant autorité indiquant l'emplacement du serveur de la zone .exemple ;**
9. Le **serveur de noms récursif interroge le serveur de la zone .example** faisant autorité pour connaître l'adresse IP de l'hôte **www ;**
10. Le **serveur de la zone .exemple répond avec les informations faisant autorité indiquant l'adresse IP de l'hôte www ;**
11. Le **serveur de noms récursif transmet l'adresse IP de [www.example.com](http://www.example.com) au résolveur.**



# Couche Applications

## DNS Résolveur

Ce processus de résolution de nom **se déroulerait beaucoup plus lentement si la base de données DNS n'était pas distribuée.** En outre, la **mise en cache des résolutions** de nom récentes est **bénéfique pour les performances.**

Du **côté client** de la résolution du nom, **différentes configurations de serveur de transfert ou de mise en cache sont possibles.**

La configuration côté client DNS particulière sera dictée par les applications et les besoins en données du/des système (s) ainsi que par leurs ressources.

# Couche Applications

## DNS

### Type de requêtes DNS

Il existe 2 types de requêtes DNS ...

- **Requête récursive**  
(client au serveur DNS)
- **Requête itérative**  
(serveur au autres serveurs DNS)

# Couche Applications

## DNS

### Serveurs DNS racine

Les serveurs racine sont gérés par douze organisations différentes ...

- deux sont européennes ;
- une japonaise  
et
- neuf autres sont américaines.

Sept de ces serveurs sont en réalité **distribués dans le monde et neuf disposent d'une adresse IPv6.**

Plus de **200 serveurs répartis dans 50 pays du monde** assurent ce service.

Il existe 13 autorités de nom appelées de **a.root.servers.net** à **m.root-servers.net**.

Le **serveur k** reçoit par exemple de l'ordre de **70 000 à 100 000 requêtes par seconde** en avril 2019.

# Couche Applications

## DNS

### Serveurs DNS racine

Le DNS ne fournit pas de mécanisme pour découvrir la liste des serveurs racine, chacun des serveurs doit donc connaître cette liste au démarrage grâce à un encodage explicite.

La mise à jour de cette liste est peu fréquente de façon que les serveurs anciens continuent à fonctionner.

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Hôte

Un hôte est généralement un ordinateur connecté à un réseau. Une autre façon de voir le terme est qu'un hôte est un périphérique ou nœud capable de communiquer sur un réseau ;

#### Nom de domaine

Les hôtes Internet établissent mutuellement un contact à l'aide de numéros d'adresse IP.

Les humains ont du mal à se souvenir de ces numéros, c'est pourquoi un nom unique est souvent attribué à un hôte.

Lorsque ce nom est enregistré sur un serveur DNS autorisé, le nom est considéré comme un nom de domaine ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Domaine de premier niveau

Les noms de domaine sont structurés en arborescence, un peu comme les fichiers sont organisés en structure de système de fichiers virtuel.

Le niveau supérieur de la structure DNS est simplement appelé **point** et est symbolisé par le **caractère ..**

Les domaines directement sous la racine (.) sont les domaines de premier niveau.

Les domaines de premier niveau d'origine étaient **.com**, **.org**, **.net**, **.int**, **.edu**, **.gov** et **.mil**.

Beaucoup d'autres ont été ajoutés au fil des années ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### FQDN (*Full Qualified Domain Name*)

Un nom de domaine pleinement qualifié est le nom de domaine d'un hôte commençant au sommet de la structure DNS.

Par exemple, le nom [www.profsavard.info](http://www.profsavard.info) serait un FQDN.

Il est important de ne pas oublier le caractère . à la fin du nom de domaine complet.

C'est le domaine situé au-dessus des domaines de premier niveau.

Ce caractère est souvent omis lorsque les utilisateurs habituels fournissent un nom de domaine car le «.» Est supposé être le dernier caractère d'un nom de domaine complet dans la plupart des cas.

Toutefois, il est important de s'habituer à toujours inclure le caractère .

Si on souhaite administrer des serveurs DNS, comme cela est requis dans certains fichiers de configuration du serveur DNS ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Sous-domaine

Un sous-domaine est un domaine qui est un composant d'un domaine plus grand. Par exemple, supposons que l'on souhaite avoir trois domaines pour son organisation afin d'organiser de manière fonctionnelle les hôtes. On peut appeler ces domaines ventes, ingénierie et support. Si le domaine de l'entreprise est profsavard.info., ces trois sous-domaines s'appelleraient ventes.profsavard.info., ingénierie.profsavard.info. et support.profsavard.info ;



# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Serveur de noms

Un serveur de noms est un système qui répond aux demandes du client DNS.

Les serveurs de noms fournissent la traduction d'adresse IP en noms de domaine (et parfois l'inverse: traduction de nom de domaine en adresse IP).

#### Remarque ...

Un serveur de noms possède une copie de ces informations stockées localement (appelée fichier de zone) ou stocke en mémoire les informations obtenues temporairement par d'autres serveurs de noms, ou transmet la requête à un autre serveur (ou serveurs) disposant de ces informations ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Serveur de noms faisant autorité

Un serveur de noms faisant autorité renvoie des résultats en fonction des informations stockées localement sur le système (les enregistrements originaux) ;

#### Fichier de zone

Nom du fichier utilisé pour stocker les informations de conversion d'adresse IP en nom de domaine (également appelées enregistrements DNS).

Ce fichier contient également des informations permettant de définir le domaine lui-même ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Enregistrement

Dans le fichier de zone, un enregistrement est une entrée qui définit un bloc d'informations unique pour la zone, telles que les données qui traduiraient une adresse IP en nom de domaine ;

#### Mise en cache du serveur de noms

Un serveur de noms en mise en cache est un serveur qui renvoie des résultats en fonction d'informations obtenues d'un autre serveur de noms, tel qu'un serveur de noms faisant autorité. Le principal avantage d'un serveur de noms en cache est qu'il peut accélérer la résolution d'adresse IP en noms de domaine, car il peut mettre en cache les résultats et répondre aux futures demandes en utilisant les informations contenues dans ce cache ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### **TTL** (*Time to Live*)

Les données stockées dans un serveur de noms en cache ne sont généralement pas stockées de manière permanente.

Le serveur de noms qui fournit les données fournit également au serveur de noms de mise en cache une durée de vie (TTL). Le serveur de noms de mise en cache stocke les informations en mémoire jusqu'à la fin de cette période TTL. Cette période est généralement de 24 heures, mais cela peut varier en fonction du nombre de mises à jour des enregistrements du serveur de noms faisant autorité ;

# Couche Applications

## DNS

### Termes essentiels

Les termes suivants sont associés à DNS ...

#### Redirecteur DNS

Ce serveur DNS est conçu afin de prendre des requêtes DNS d'un réseau interne et les envoyer à un serveur DNS externe ;

#### Recherche directe (*Forward lookup*)

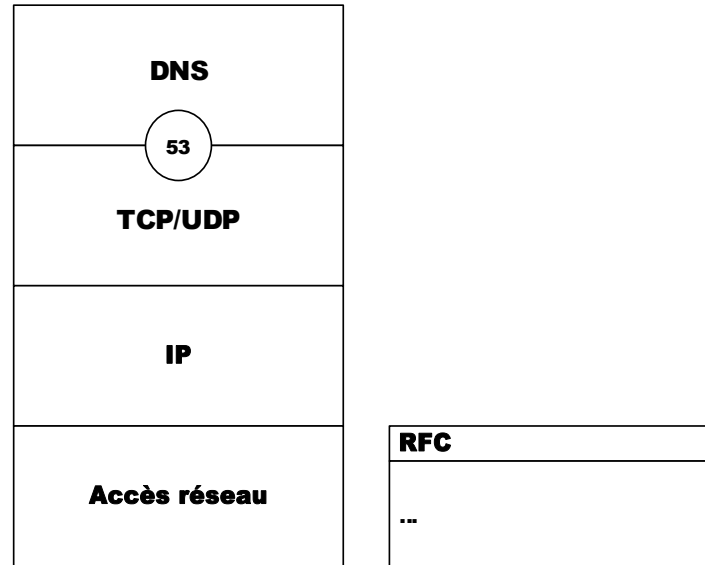
Processus de traduction d'une adresse IP en un nom de domaine. La plupart des serveurs DNS fournissent cette fonctionnalité ;

#### Recherche inversée (*Reverse lookup*)

Processus de traduction d'un nom de domaine en une adresse IP. Alors que de nombreux serveurs DNS fournissent cette fonctionnalité, elles sont toutefois moins fréquentes que les recherches directes.

# Couche Applications

## DNS



# Couche Applications

## Gestion de périphériques réseau SNMP (Simple Network Management Protocol)

Le protocole SNMP (*Simple Network Management Protocol*) a été défini afin de **servir de standard aux échanges d'informations concernant l'état de santé et la configuration des périphériques d'un réseau.**

C'est un protocole, mais comme d'autres protocoles (par exemple DNS) il **repose aussi sur un modèle.**

Le modèle SNMP définit **deux types d'entités** :

- Les **entités gérées** (hôtes, commutateurs, routeurs) ;
- Les **entités de gestion** (les hôtes qui reçoivent les informations provenant des entités gérées).

Avec SNMP, **on ne parle pas de client ou de serveur**, mais plutôt **d'agent et de gestionnaire.**

# Couche Applications

## Gestion de périphériques réseau SNMP (Simple Network Management Protocol)

### MIB

Les informations qui caractérisent les hôtes et périphériques sont contenues dans des MIB (*Management Information Base*), elles aussi définies dans un standard.

Les MIB sont composées d'un ensemble de variables ayant un nom et une valeur; ces valeurs peuvent être lues ou écrites à partir d'un gestionnaire SNMP.

Certaines variables sont en lecture seule.



# Couche Applications

## Gestion de périphériques réseau SNMP (Simple Network Management Protocol)

### Messages

Le protocole SNMP permet **2 types de communication** ...

- Un **gestionnaire** interroge les agents (*polling*) ;
- Les **agents** envoient des alertes (*trap*) au gestionnaire.

Le **polling** ou sondage est utile pour collecter des statistiques d'usage ou des informations de configuration.

Toutefois, lorsqu'on veut être prévenu des problèmes dès qu'ils surviennent, **un mécanisme d'alerte est nécessaire**.

**UDP** est utilisé comme protocole de transport; le **port 161** est le **port d'écoute sur les agents** (requêtes) et le **port 162** est le **port d'écoute sur les gestionnaires** (alertes).

# Couche Applications

## Gestion de périphériques réseau SNMP (Simple Network Management Protocol)

Les classes de messages sont ...

- **Lecture**  
*GetRequest, GetNextRequest, GetBulkRequest ;*
- **Écriture**  
*SetRequest ;*
- **Réponse**  
*Response ;*
- **Alertes**  
*Trapv2, InformRequest*

# Couche Applications

## Gestion de périphériques réseau SNMP (Simple Network Management Protocol)

### Description des principaux messages

- **GetRequest**  
Le gestionnaire envoie une requête à l'agent, qui répond avec un message Response ;
- **GetNextRequest**  
Similaire à un GetRequest, mais le gestionnaire demande d'envoyer l'objet suivant celui qui est spécifié dans la requête ;
- **GetBulkRequest**  
Similaire à un GetRequest, mais Response contient un ensemble d'objets ;.

# Couche Applications

## Gestion de périphériques réseau SNMP (Simple Network Management Protocol)

### Description des principaux messages

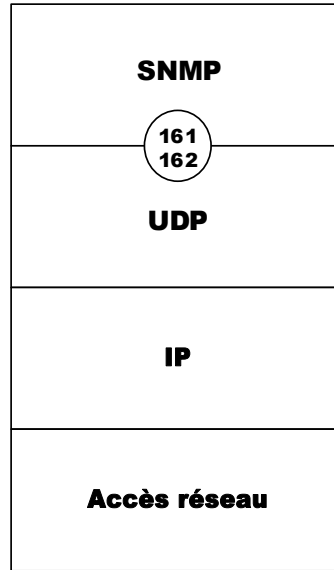
- **SetRequest**  
Le gestionnaire envoie une requête à l'agent, qui retourne un message Response après avoir fait les modifications (si possible/permis) ;
- **Trapv2**  
L'agent envoie une alerte au gestionnaire; le gestionnaire peut retransmettre cette alerte en envoyant un message InformRequest à un autre gestionnaire, qui doit lui retourner une confirmation avec un message Response.

### Remarque ...

Un agent qui envoie un message Trapv2 ne reçoit jamais de confirmation.

# Couche Applications

## SNMP



RFC
3411-3418

# Couche Applications

## Gestion de périphériques réseau NTP (Network Time Protocol)

Dans un système d'information moderne, la **synchronisation des hôtes sur une horloge commune est un prérequis** pour de nombreuses actions comme l'**analyse des journaux (logs)** ou la **supervision système et réseau**.

Le Protocole d'Heure Réseau (*Network Time Protocol* ou NTP) est un protocole qui **permet de synchroniser, à partir d'un réseau informatique, l'horloge locale d'hôtes** sur une référence d'heure.

Le protocole NTP utilise le **port UDP 123 pour effectuer les requêtes sur le réseau**.

Le serveur NTP doit donc être en écoute sur ce port.

Si le réseau est protégé par un pare-feu, il faudra bien entendu le configurer pour autoriser les requêtes sur ce port.

.

# Couche Applications

## Gestion de périphériques réseau NTP (Network Time Protocol)

Le processus de synchronisation dispose de **différents niveaux hiérarchiques symbolisant la distance par rapport à la source UTC**, que l'on appelle également **stratum (mot latin pour couches) ou strate**.

L'ensemble des appareils techniques obtenant l'heure à partir d'un **serveur primaire ou d'un système de navigation par satellite** sont classés dans la catégorie **stratum 0**.

Les **horloges atomiques** ou **radiopilotées** en font notamment partie.

Un **hôte obtenant l'UTC à partir d'une telle horloge** atomique ou radiopilotée entre dans la **catégorie stratum 1** et **ainsi de suite**. **Chaque système est ainsi à la fois client du stratum précédent et serveur des systèmes du stratum suivant** (tout du moins en théorie).

# Couche Applications

## Gestion de périphériques réseau NTP (Network Time Protocol)

**pool.NTP.org -- Cluster Internet de milliers de serveurs NTP**

Il existe un **immense cluster virtuel composé de plus de 4 000 serveurs d'horloge NTP**.

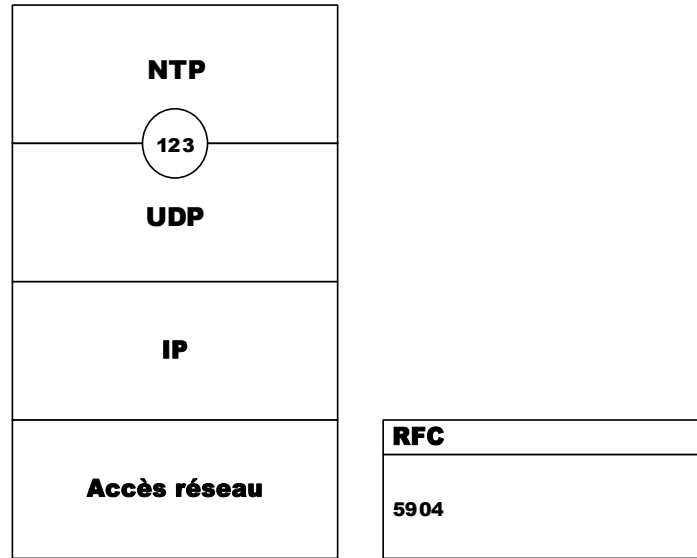
La croissance constante du pool de NTP au fil du temps est due aux **efforts de la communauté de ce projet réussi** : toute personne disposant d'un serveur avec une **adresse IP statique et connecté en permanence à Internet** peut faire **enregistrer ce serveur dans le cluster**.

Malgré une demande grandissante, le service peut donc être **utilisé gratuitement et sans restriction jusqu'à aujourd'hui**.



# Couche Applications

## NTP



# Couche Applications

## Voix sur IP

Jusqu'à il y a environ **40 ans**, les appels téléphoniques étaient transmis sur le **réseau téléphonique public commuté (RTPC)** au moyen d'**interrupteurs et de câbles de cuivre physiques**.

Depuis l'invention de la VoIP au milieu des **années 1980**, les **appels** peuvent être effectués sur les **mêmes réseaux de données IP** dont se sert les ordinateurs (et, maintenant, les téléphones intelligents et tablettes) pour transmettre des données.

La voix sur IP, ou VoIP pour *Voice over IP*, est une **technologie informatique qui permet de transmettre la voix sur des réseaux compatibles IP**, à l'aide du réseau Internet ou des réseaux privés (intranets) ou publics, qu'ils soient **filaire ou non**.

# Couche Applications

## Voix sur IP

Longtemps confinés au transport de la voix, des logiciels de VoIP tels que **Facebook Messenger**, **WhatsApp**, **Snapchat**, **Discord** ou encore **Viber**<sup>2,3</sup> gèrent aujourd'hui tous les **flux multimédia** (**téléphonie**, **appels vidéo**, **messagerie instantanée** et **transferts de fichiers**).

En ce qui concerne la **téléphonie uniquement**, cette technologie est complémentaire de la **téléphonie sur IP** (ToIP pour *Telephony over Internet Protocol*), qui concerne les fonctions réalisées par un **autocommutateur téléphonique IPBX**.

# Couche Applications

## Voix sur IP

Les **données sont chiffrées et acheminées de différentes façons**, selon le fournisseur de services VoIP. Le **protocole d'ouverture de session (SIP)** constitue toutefois la **norme de l'industrie**.

Le protocole SIP **définit les messages transmis entre les points d'extrémité** et **régit l'établissement et l'arrêt des communications** de même que d'autres aspects nécessaires à un appel.

Il peut être **utilisé pour transmettre de l'information** entre **deux ou plusieurs points d'extrémité**.

# Couche Applications

## Voix sur IP

En plus de la téléphonie, le **protocole SIP** peut être utilisé pour les **vidéoconférences**, les **textos**, la **messaging instantanée**, le **partage de fichiers** et d'autres applications. Il a été conçu et normalisé sous l'égide du groupe de travail pour la participation à la **standardisation de l'Internet (IETF)**.

La VoIP est maintenant le **service téléphonique le plus utilisé par les entreprises américaines**.

Selon un rapport de Software Advice sur l'utilisation de la VoIP par les entreprises, **environ 36 % des entreprises** utilisent aujourd'hui la téléphonie VoIP pour leurs **besoins en matière de communication**.

# Couche Applications

## Voix sur IP Avantages

Plusieurs raisons valables expliquent pourquoi tant d'entreprises ont **opté pour une telle solution** ...

- **Économies d'échelle** ;
- La technologie VoIP est **facile à déployer et à gérer** ;
- La VoIP permet d'**augmenter ou de réduire les ressources** en un instant ;
- Les **appels VoIP peuvent être acheminés partout** ;
- Les **fonctionnalités** de la VoIP vont **au-delà de la téléphonie** ;
- La VoIP **s'intègre** avec **d'autres systèmes d'entreprise**.

# Couche Applications

## **Voix sur IP** **Transport de la voix**

La technologie VoIP **numérise les signaux vocaux analogiques** dans des ensembles de données **sous forme de 0 et de 1** sur les réseaux.

Les réseaux de données disposent d'une **bande passante beaucoup plus importante que les lignes téléphoniques en cuivre traditionnelles**, ce qui permet aux communications VoIP de profiter d'un **son haute définition** tout en **ajoutant la flexibilité** et les **fonctionnalités propres à Internet**.

# Couche Applications

## Voix sur IP Transport de la voix

Le transport de la voix sur IP est relativement complexe.

- La **première étape** est la **numérisation du signal analogique** capté par le microphone.
- Selon le protocole utilisé pour transporter le signal numérique, une **étape complémentaire d'encodage peut être nécessaire** (par exemple en utilisant un encodeur "A-law" ou "μ-law"), notamment pour **compresser les signaux**.
- Ensuite, les **informations sont découpées en paquets** pouvant circuler sur un réseau informatique.



# Couche Applications

## Voix sur IP Transport de la voix

Divers **protocoles** peuvent alors être utilisés pour acheminer les **informations** au(x) destinataire(s).

Ainsi le **protocole RTCP** est utilisé pour **contrôler le transport des paquets RTP**.

Le protocole réseau RTCP (*Real-time Transport Control Protocol*) **repose sur des transmissions périodiques de paquets de contrôle** par tous les participants à une session multimédia.

C'est un **protocole de contrôle des flux RTP** (*Real-time Transport Protocol*), permettant de **véhiculer des informations basiques** sur les participants d'une session, et sur la **qualité de service**.

Le **RTCP est un protocole couplé au RTP**.

# Couche Applications

## Voix sur IP Transport de la voix

RTCP fournit les **statistiques de bandes passantes** et des **informations de contrôle pour un flux RTP**. Il est couplé aux paquets RTP, mais **ne transporte aucune information** relative au média lui-même. Typiquement, **RTP sera envoyé sur un port UDP** (*User Datagram Protocol*) de **numéro pair**; le **message RTCP** couplé sera envoyé sur le **port impair suivant**.

La fonction principale du **RTCP** est de **fournir des informations sur la qualité de service (QoS)** dans la distribution des médias en **envoyant périodiquement des informations statistiques** aux participants à une session de flux multimédia (audio ou vidéo).

# Couche Applications

## Voix sur IP Transport de la voix

Les **statistiques RTCP** rassemblent pour une connexion média des informations telles que ...

- le **nombre d'octet et de paquets transmis** ;
- le **nombre de paquets perdus** ;
- la **gigue** et
- le ***Round-Trip delay Time***.

Une application peut utiliser cette information pour **contrôler la qualité du service**, et par exemple **adapter le débit du flux vidéo** en **utilisant un autre codec**.

# Couche Applications

## **Voix sur IP** **Transport de la voix**

RTCP lui-même ne fournit pas de méthodes de chiffrement de flux ou d'authentification. Ces mécanismes peuvent être mis en œuvre, par exemple, par le **protocole Secure Real-time Transport Protocol (SRTP)**.

**RTCP est encapsulé dans des paquets UDP tout comme RTP.**

# Couche Applications

## Voix sur IP Codage de la voix

La voix est ce qui permet aux humains d'échanger de l'information, de communiquer, et de faire passer des émotions. Il s'agit d'un **phénomène physique complexe**.

Lorsque l'on parle, nous produisons un **ensemble de sons possédant des niveaux de fréquences différents** (grave, médium, aigüe...).

La **voix captée par le microphone** du combiné fournit un **signal analogique**.

Pour l'envoyer sur un réseau TCP/IP (numérique), il va falloir **convertir ce signal analogique en un signal numérique** en format **PCM** (Pulse Code Modulation), par exemple à **64 kb/s**.

# Couche Applications

## Voix sur IP Codage de la voix

Une fois convertie, la **voix, ainsi numérisée**, doit être **compressée** grâce à un **codec** (Codeur/Décodeur) pour l'**insérer dans un paquet IP**.

Le codage doit offrir la **meilleure qualité de voix possible**, pour un **débit le plus faible possible** et un **temps de compression le plus court possible**.

Il existe **plusieurs techniques de codage**, chacune étant mesurée de **façon totalement subjective** par une masse de population prise au hasard.

Elle doit **noter chaque codage par un chiffre de 1 à 5** (1 = Insuffisant - 5 = Excellent). Cette technique s'appelle le **MOS**.

# Couche Applications

## Voix sur IP Interfaces VoIP

Le terme **VoIP** est en général utilisé pour décrire des **communications point à point**. Pour la diffusion de son ou de **vidéos sur IP en multipoints**, on parlera plutôt de **streaming pour une simple diffusion**, comme les **radios Web** par exemple. Le terme **multipoints** sera réservé à des **visioconférences** dont le nombre de **participants est plus grand que deux**.

La **voix ou le son sur IP** peut se faire en mode **Unicast**, **Broadcast** ou **Multicast** sur les réseaux, c'est-à-dire en **mode point à point**, en **mode une émission et plusieurs réceptions** (comme un émetteur TV, par exemple) et en **mode une émission pour plusieurs réceptions** (mais le signal n'est routé que s'il y a des récepteurs) comme les radios Web.

# Couche Applications

## Voix sur IP Interfaces VoIP

Le transport de communication sur IP est très dépendant du délai de latence d'un réseau.

Ce délai influe beaucoup sur la qualité psycho-acoustique d'une conversation.

Avec l'avènement des réseaux 100 Mbit/s, ADSL ou par fibres optiques, les temps de latence deviennent tout à fait acceptables pour une utilisation quotidienne de la voix sur IP.

À l'inverse, les connexions par liaison satellite souffrent d'un temps de latence souvent trop important pour prendre en charge les applications de voix sur IP.

En moyenne, le temps de latence sur ce type de liaison est estimé entre 400 et 800 millisecondes. Une connexion filaire (fibre optique ou cuivre) bénéficie d'un temps de latence de 60 à 200 millisecondes.



# Couche Applications

## Voix sur IP Interfaces VoIP

Plus que la latence, c'est la **gigue (*jitter*)** qui pénalise la **voix sur IP**.

En effet, s'il y a des **fluctuations du signal en amplitude et fréquence**, il faudra un mécanisme de **remise en ordre des paquets afin de restituer le message vocal**, processus qui se traduira par des **blancs et des attentes**.

# Couche Applications

## Voix sur IP Contraintes

Il existe **plusieurs contraintes** relatives à la transmission de la voix sur IP.

- **Perte de paquets** (*Packet Loss*)  
Lorsqu'il y a **saturation**, les **mémoires tampons** ont besoin de **libérer une partie de la bande passante**, négligeant ainsi certains paquets.  
Néanmoins, le trafic VoIP est transmis au-dessus de la **couche UDP**, ce qui implique qu'**aucun mécanisme de contrôle de flux** ou de **retransmission des paquets perdus** n'est offert par la couche transport. Cela implique qu'il faut **accorder une forte importance aux protocoles RTP et RTCP** (*Real-Time Transport (Control) Protocol*) qui vont permettre de **calculer le taux de perte de paquets**, et de **réagir en conséquence** au niveau de la couche applicative.

# Couche Applications

## Voix sur IP Contraintes

Il existe **plusieurs contraintes** relatives à la transmission de la voix sur IP.

- **Bande passante**

C'est le terme utilisé pour **évoquer le flux de connexion**.

C'est une unité **souvent prise** pour une **unité de débit**, mais elle ne définit en réalité que **l'étendue de fréquence et le débit en dépend, d'où la confusion**.

- **Sécurité**

La sécurité de la téléphonie est **souvent restée un sujet à part** dans l'entreprise.

Désormais, les **risques associés aux systèmes téléphoniques** peuvent avoir des **conséquences graves sur le système d'information** et sur l'entreprise.

# Couche Applications

## Voix sur IP Protocoles – Signalisation

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **H.323**

Le protocole H.323 est un **protocole standard de l'UIT** (Union Internationale des Télécommunications) qui a été établi pour **permettre l'activation, la gestion et la terminaison d'une session média**.

Il définit en plus tout une **gamme de protocoles** qui servent à fournir **tout type de communication multimédia** dans les réseaux.

Le protocole **SIP** remplace progressivement le protocole **H.323** car il est **plus simple d'utilisation**.

# Couche Applications

## Voix sur IP Protocoles – Signalisation

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **SIP** – *Session Initiation Protocol*

Le protocole est un protocole de **gestion de session de communication en multimédia**. Il est **ouvert, standard** et c'est le **protocole principal** utilisé pour la signalisation en VoIP. Il est **aussi utilisé pour la visiophonie**, pour la **messagerie instantanée**, ...

En VoIP c'est donc ce protocole qui **permet la gestion des appels**.

Par exemple, c'est grâce à SIP que le **poste peut s'enregistrer auprès de l'IPBX**.

C'est aussi grâce à SIP que le poste peut indiquer à **l'IPBX quand l'utilisateur appui sur les touches du clavier**. Il permet aussi à l'IPBX de **faire sonner un poste**, de **mettre en relation deux téléphones**, ...

# Couche Applications

## Voix sur IP Protocoles – Signalisation

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **SIP – Session Initiation Protocol**  
C'est donc lui qui est au **cœur des infrastructures de VoIP**.  
Toutefois, ce n'est pas **SIP** qui **permet le transport de la voix**.  
Il ne sert qu'à la **signalisation**.  
SIP utilise le **port 5060 en UDP**.  
Il est **indépendant des autres protocoles** des couches inférieures. SIP **fonctionne de manière similaire à HTTP**.  
Il réutilise de nombreux en-têtes ainsi que des règles d'encodage et des codes de statut de HTTP.
- ;

# Couche Applications

## Voix sur IP Protocoles – Transport

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **RTP** – *Real-Time Transport Protocol*

Le transport de l'information permet notamment de **transporter la voix numérisée grâce aux codecs**, sur le réseau.

C'est ici le **protocole RTP** qui est utilisé.

Le protocole RTCP peut aussi **être utilisé pour contrôler la qualité et demander de renégocier les codecs** si la **bande passante disponible change**.

RTP est un **protocole situé au-dessus d'UDP**, permettant le transport de données ayant des **contraintes de temps réelles**. Il est principalement **utilisé pour les flux audio et vidéo**.

# Couche Applications

## Voix sur IP Protocoles – Transport

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **RTP – Real-Time Transport Protocol**  
RTP **ajoute une entête spécifique à UDP** pour plusieurs raisons.
  - Premièrement, il **numérote les paquets**, pour **gérer les pertes et le dé-séquencement** (c'est-à-dire les paquets qui arrivent dans le mauvais ordre).
  - Ensuite, il ajoute une **information d'horloge pour gérer la gigue** (c'est-à-dire la variation de latence entre plusieurs paquets).

Il permet aussi de **spécifier le type de données transportées (audio, vidéo, image, texte, ...)**.

Il y a encore d'**autres informations complémentaires** dans l'en-tête.



# Couche Applications

## Voix sur IP Protocoles – Transport

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **RTCP** – *Real-Time Transport Control Protocol*

En complément de RTP, on utilise **RTCP pour contrôler la qualité de la transmission**.

Il **fonctionne aussi avec UDP**.

RTCP ne **transporte pas l'information finale**. Il est simplement utilisé en **contrôle**. À l'aide de **statistiques sur la transmission** (paquet perdu, gigue, délai, ...), il est **possible d'estimer la qualité de service**.

C'est grâce à RTCP que l'on peut **renégocier le codec** pour s'adapter à la bande passante nécessaire.

Les paquets de contrôle sont **envoyés à tous les participants de la session**.

# Couche Applications

## Voix sur IP Protocoles – Transport

Les **principaux protocoles** rencontrés pour la Voix sur IP sont ...

- **RTCP** – *Real-Time Transport Control Protocol*  
RTCP n'offre pas de **garantie de livraison** des paquets.  
Pour cela, il faut, employer un **protocole de réservation de type RSVP** ou bien **s'assurer que les liens de communication utilisés sont correctement dimensionnés** par rapport à l'utilisation qui en est fait.  
Il existe donc trois principales fonctions de RTCP ...
  - **Fournir des informations sur la qualité de session ;**
  - **Contrôler le débit** auquel les participants à une session RTP transmettent leurs paquets RTCP ;
  - **Transmettre des informations de contrôle** de session.

# Couche Applications

## Voix sur IP

### Codecs

Un codec est un **algorithme capable de compresser un signal numérique**. Le but est que ce **signal soit moins lourd** pour le **transport** ou le **stockage**.

En télécommunication, on cherche toujours à **compresser la voix et la vidéo**. Sur un **réseau interne**, on a en général **beaucoup de bande passante à disposition**.

À moins de passer beaucoup d'appels simultanés, on n'aurapas de problème.

En revanche, sur une **connexion internet qui possède une bande passante plus faible**, même quelques appels simultanés peut **causer des problèmes**.

# Couche Applications

## Voix sur IP Codecs



Il existe de très nombreux codecs, qui ont chacun leurs caractéristiques telles que :

- Taux de compression ;
- Vitesse de compression ;
- Vitesse de décompression ;
- Consommation processeur/mémoire ;
- Qualité du signal de sortie.

# Couche Applications

## Voix sur IP

### Codecs

Il faut donc faire notre **choix parmi les codecs existants**, tout en tenant compte des **attributs de chaque codec**.

En règle générale, on utilise des **codecs à compression légère en interne** et des **codecs à forte compressions** pour les **appels transitant sur le WAN**.

# Couche Applications

## Voix sur IP Codecs

Voici une **liste non exhaustive** des codecs disponibles pour la voix en VoIP.

Codec	Débit	MOS
G.711	64 Kbps	4,1
G.729	8 Kbps	3,92
G.729a	8 Kbps	3,7
G.723.1 MP-MLQ	6,3 Kbps	3,9
G.723.1 ACELP	5,3 Kbps	3,65
G.726	32 Kbps	3,85
G.728	16 Kbps	3,61
G.722	64 Kbps	4,13
ILBC	15,2 Kbps	4,1

# Couche Applications

## Voix sur IP

### Codecs

Pour le codec G.711, il existe les **Lois A et  $\mu$**  (A-law et  $\mu$ -law). La **loi A** est principalement utilisée en **Europe et en Afrique**, alors que la **loi  $\mu$**  est principalement utilisée en **Amérique du nord** et **au Japon**.

Les deux sont **toutefois très proches**.

Le **champ MOS** – *Mean Opinion Score* est une **note subjective sur la qualité du signal après passage dans le codec**.

La note va de **1 à 5**.

**Au-delà de 4**, il est **presque impossible de faire la distinction** avec un **signal non-compressé**.

En général, on utilise **principalement G.711 et G.729**. **G.711 en interne** et sinon **G.729**.