Les Technologies sans fils

1) Généralités
2) Les différentes normes sans fil
3) Etude d'une norme particulière : 802.11

Généralités

But : Communiquer avec différents systèmes sans utiliser de liaison filaire

Plusieurs normes concurrentes :

- IrDA,
- liaison hertzienne, GSM, GPRS, UMTS, LTE , 5G …
- 802.11, 802.15, 802.16,…

Chaque norme correspond à une application bien spécifique.

WLAN : Wireless Local Area Network *a été défini par*

WECA : Wireless Ethernet Compatibility Alliance

(3com, Apple, Compaq, Dell, Lucent Technologies, Nokia, ….)

Généralités

Objets communicants:

• Vers 1960, Création du port RS232 pour relier **deux** systèmes , un maître, un esclave

• Evolution logique vers le sans-fil, -> **IrDA**

•Pb : permet seulement la communication entre deux systèmes

•Evolution logique vers les ondes radio, -> Bluetooth v1.0 → Bluetooth v5.0

Norme :

802.15.1 : Bluetooth v1.0 ⇒ **WPAN** : Wireless Personal Area Network

802.15.2 : Amélioration de la norme pour l'interopérabilité

802.15.3 :WPAN, haut débit : Augmentation du débit et de la portée
(> 20 Mbps et 10m, BP : 2,4 Ghz)

802.15.4 : WPAN, faible débit pour réseau ZigBee ou 6LowPan
(< 250 kb/s)

Généralités

Norme 802.16 alias Wimax:

- Réseau sans fil à large Bande
- Utilisation de la technologie BWA (Broadland Wireless Access)
- Débit jusqu'à 70Mb/s sur de grandes distances (20 km), BP de 2 à 11 Ghz
- Technique MIMO (Multiple Input/Multiple Output) -> plusieurs antennes en émission et en réception

Consortium WiMax

(*Worldwide Interoperability for Microwave Access)*

Définition de la norme 802.16a, b, i, ….m

But : au départ, relier les villages ne pouvant bénéficier de l'ADSL (Boucle Local Radio), puis 802.16d pour concurrencer Wifi/3G/4G.

La norme 802.16d est considérée comme norme autorisé 4G.

Jusqu'à présent, 2 licences WiMax par région + 1 nationale

- deux choisis par l'ARCEP (auvergne : Maxtel et Bollore)
- une appartenant à Altitude Telecom (racheté par Iliad (free))

Généralité (suite)

- Wimax
  - Bollore a racheté de nombreuses régions pour assurer une diffusion sur la France (une licence par région)
  - Actuellement quelques offres subsistent → concurrente de l'ADSL ou de la 4G
    - Mais très concurrencé par la fibre, et obsolète par rapport à 5G
  - Débit allant de 2 à 70 Mb/s
    - Tarif environs 40 €/mois (max 10 Go consommation)
- Fin Wimax Français
  - → bande passante rendue de 3410 à 3490 Mhz
  - Redistribution en 2026… vers la 5G

La norme 802.11

La norme **802.11** définit la couche 1 et 2 pour une liaison sans fil utilisant des ondes électromagnétiques :

- La couche physique
  - codage DSSS, FHSS, IrDA
- La couche Liaison de données
  - couche LLC et couche MAC

Cette norme permet d'avoir un débit de 1 ou 2Mb/s et elle utilise un accès au médium par compétition (méthode CSMA/CA)
(CA : Collision Avoidance)

Mais, évolution de cette norme

Wi-Fi (Wireless Fidelity)

Wi-Fi

Nom norme	Nom	Description
802.11a	Wifi 2	Débit : 54Mb/s, 8 canaux radio dans la bande de fréquence des 5 Ghz.
802.11b	Wifi 1	Débit : 11Mb/s, portée 300m, 3 canaux radio dans la bande de fréquence des 2,4 Ghz
802.11c	Pontage	Etablissement d'un pont pour la norme 802.11d
802.11d	International	Etablit les règles à respecter entre les différents pays pour transporter les données 802.11
802.11f	Roaming	Interopérabilité entre les différents points d'accès pour permettre l'itinérance (définition de l'IAPP)
802.11g	Wifi 3	Débit : 54MB/s, portée 300m, compatible avec 802.11b
802.11i	WPA2	Amélioration de la sécurité pour les normes a, b et g.
802.11n	Wifi 4	Débit max : 300 Mb/s, bande fréquence 2,4 ou 5Ghz
802.11ac	Wifi 5	Débit 1gb/s, Bande fréquence 5 Ghz
802.11ax	Wifi 6	Débit 10gb/s, Bande fréquence entre 2,4, 5 et 6 Ghz
802.11be	Wifi 7	Débit 25 gb/s, Bande fréquence entre 2,4, 5 et 6 Ghz, personne presque fixe
802.11bn	Wifi 8 (2028)	Débit 100 gb/s, Bande fréquence entre 2,4, 5 et 6 Ghz

Topologies

- **Mode Infrastructure (ou hotspot)**

  le plus courant

  • Au minimum , 1 AP + postes sans fil

  BSS : Basic Service Set

  - identifié par un BSSID (abrégé en SSID -> Service Set Identifier)

- **Mode Ad-Hoc**

  • Aucun AP, que des postes sans fil

  IBSS : Independant Basic Service Set

  - identifié par un SSID

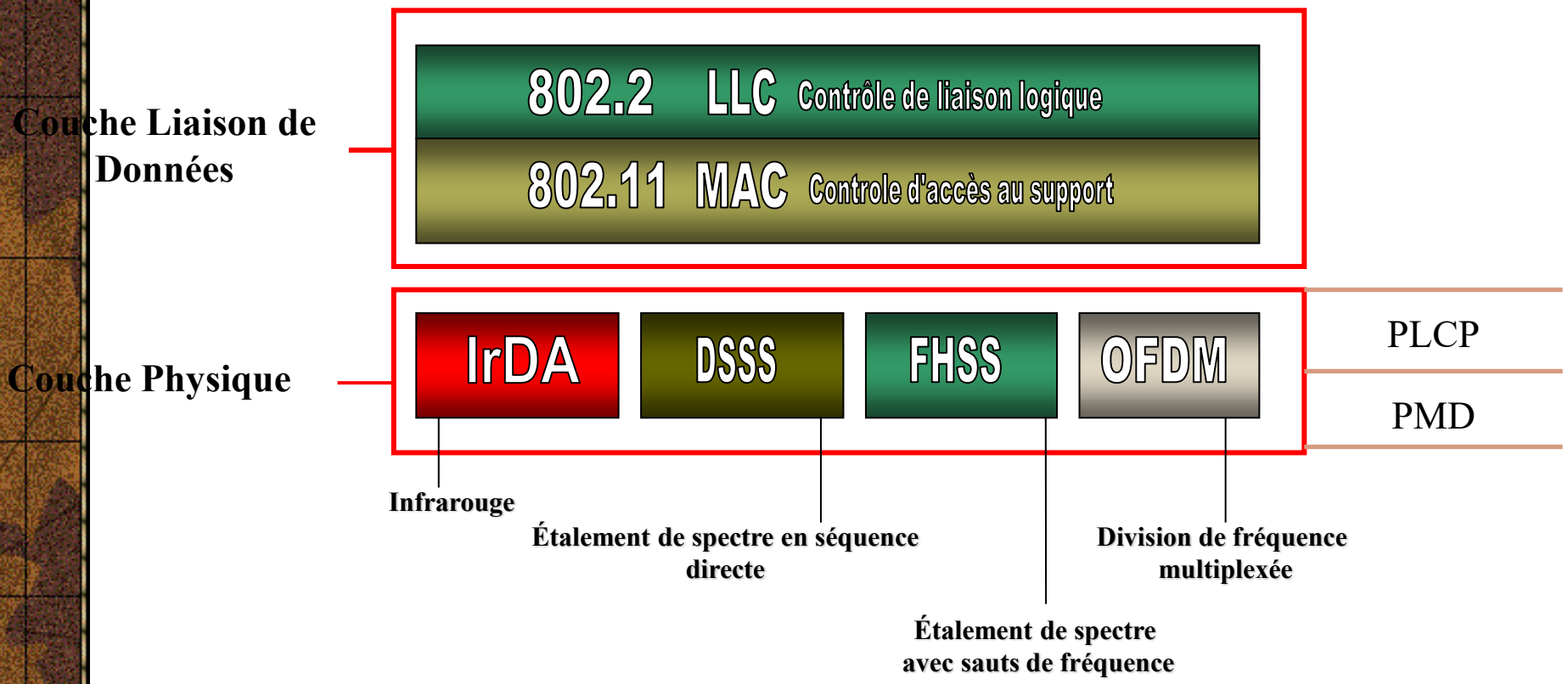
Tout le monde doit voir tout le monde
ou
Pc configuré comme routeur

Architecture en couches

- **WiFI**

PLCP : Physical Layer Convergence Procedure

PMD : Physical Medium Dependant



Physique - OFDM

- **OFDM : Orthogonal Frequency Division Multiplexing**

• Basé sur les différentes fréquence utilisées (2,4 Ghz , 5 Ghz, …)
• Division du canal principal en sous canaux utilisés en parallèle
• Un canal principal de x Mhz est divisé en y canaux de 300 Khz
• Modulation différente pour chacun des canaux.

•Très utilisé pour le 802.11a, ac
norme a :8 canaux de 20 Mhz entre 5,15 Ghz et 5,35 Ghz
norme ac : 8 canaux de 80 Mhz entre 5,17 Ghz et 5,83 Ghz

Utilisation de la norme **OFDMA** (… Multiple Access) pour le 802.11ax, be
Déjà présent dans la 5G

Couche liaison de données

La couche MAC

- Similaire à la couche Mac ethernet
- ***Fonctionnalité***
  - Contrôle d'accès au support
  - Contrôle d'erreur par CRC
  - Fragmentation et réassemblage
  - Gestion de l'énergie
  - Gestion de la mobilité
- ***Deux méthodes d'accès pour le 802.11a, b, g***
  - **DCF** (Distributed Coordination Function) : utilisation pour les données asynchrones, collisions possibles
  - **PCF** (Point Coordination Function) : utilisation pour les données synchrones, pas de collision.

Distributed Coordination Function

◆ DCF

• **Basé sur un accès CSMA/CA**

Pour émettre :

- On écoute le support (ondes)
- Si libre pendant un temps donné (*DIFS*, Distributed Inter Frame Space)

-> transmission d'une trame Ready To Send (RTS) contenant les informations sur le volume de données et la vitesse de transmission (optionnel)

-> réception d'un Clear To Send (CTS) (optionnel)

-> envoie des données

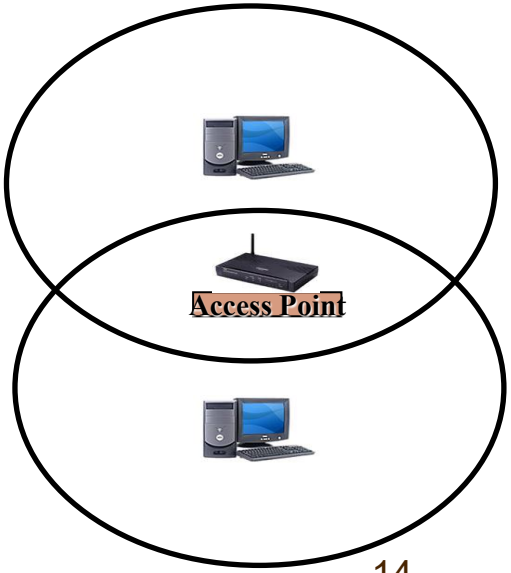
-> récupération d'un ACK pour chaque trame

Une station qui veut émettre doit attendre la libération du support.

(NAV : Network Allocation Vector)

Un ACK pour chaque trame car

2 stations peuvent vouloir émettre en même temps sans se voir.

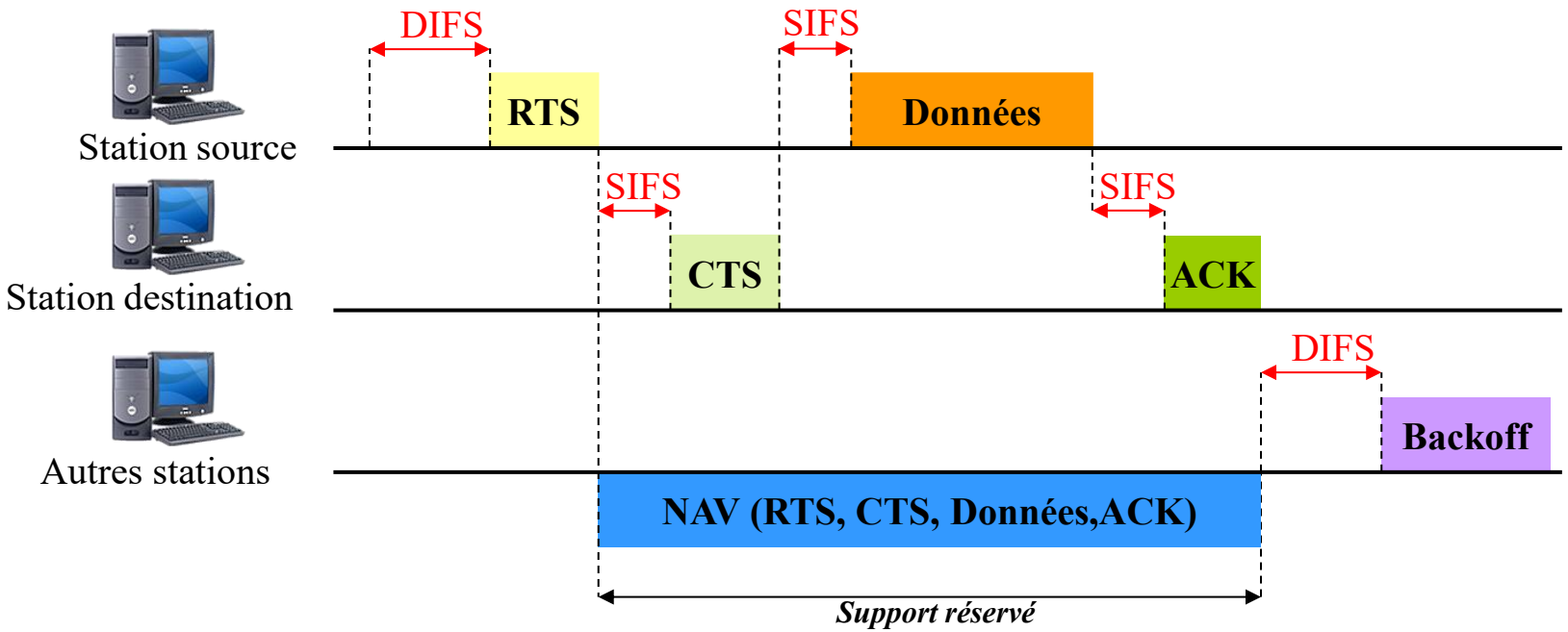


Distributed Coordination Function

◆ DCF

• *Exemple de dialogue*

SIFS : Short Inter Frame Space < **PIFS** : Prioritary < **DIFS** < **EIFS** (Extented)



Backoff : temps d'attente aléatoire pour que toutes les stations n'émettent pas en même temps.

Les Trames WiFI (1)

- **3 types de trames**
  - Trames de *données*
  - Trames de *contrôle* (RTS, CTS, ACK)
  - Trames de *gestion*

- **Structure d'une trame WIFI:**

PLCP : Physical Layer Convergence Procedure
-> renseigne sur la composition de la trame

Le préambule et le PLCP varie en fonction de l'interface physique utilisée
(FHSS, DSSS, IrDA, OFDM, OFDMA)

Les Trames WiFI (2)

- **Couche MAC pour les trames de données**

Contrôle de trame 2 octets	Durée/ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	Séquence 2 octets	Adresse 4 6 octets

Corps de la trame 0 à 2312 octets	CRC 4 octets

Contrôle de trame

Version (2 bits)	Type (2 bits)	Sous-Type (4 bits)	To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

Version : actuellement, 00
Type : 3 types, plusieurs sous-types (00 : gestion, 01:contrôle, 10 : données)
To DS ou From DS : trame vers ou en provenance du système de distribution
More fragment : 1, trame fragmentée et pas dernier fragment, 0 sinon
Retry : 1 , retransmission
Power management : 1 , économie d'énergie, 0 actif
More Data : 1 si d'autres données à faire parvenir à la station
WEP : trame chiffrée ou non
order : Trame ordonnée ou non

Les Trames WiFI (3)

- **Couche MAC pour les trames de données**

Champ *« durée/ID »* : identifiant pour des trames polling de contrôle, ou durée pour calculer le NAV

Champ «*Adresse* » : même format que les adresses Mac (6 octets)

- DA : Destination Adresse : destination de la trame : individuelle ou groupe
- SA : Source Adresse : source de la trame : individuelle
- RA : Receiver Adresse : réception des données : Point d'accès récepteur
- TA : Transmitter Adresse : transmission des données : Point d'accès émetteur
- BSSID : soit adresse MAC de l'AP, soit @MAC du IBSS.

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4	
0	0	DA	SA	BSSID	Aucune	Ad-hoc
0	1	DA	BSSID	SA	Aucune	
1	0	BSSID	SA	DA	Aucune	Normal
1	1	RA	TA	DA	SA	Entre 2 PA

Champ « *contrôle de séquence* » : numérotation des trames

Les Trames WI-FI (4)

- **Couche MAC pour les trames de contrôle**

Trame RTS

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	TA 6 octets	FCS 2 octets

Trame CTS

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	FCS 2 octets

Trame ACK

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	FCS 2 octets

La Sécurité (1)

- **Les types d'attaque :**
  - Ecoute passive ou active → permet l'interception de données
    → facile à réaliser car les données sont émises dans un rayon, difficilement détectable
  - Intrusion réseau (intrusion, usurpation)
    par les employés, par virus,…
  - Le brouillage radio (facilement détectable, mais très efficace)
  - Les dénis de services
  - Attaque Man In the Middle via ARP spoofing, ARP poisoning…

La Sécurité (2)

Les contres mesures

- Limiter la puissance d'émission des bornes si possible
  éviter d'arroser le quartier
- Désactivation des services d'administration disponible (passwd admin) ou fermeture de port pour limiter les accès
  changement des mots de passes par défaut
- Changement de SSID par défaut (attribution d'un SSID)
  mais transmis en général par AP ou en méthode Ad-Hoc ➔ Pb
- Désactivation du Broadcast du SSID
  mais visible dans les trames lors de l'association
- Filtrer les adresses MAC : utilisation des ACL (Access LISTS) des clients RLAN au niveau des bornes d 'accès
  mais possibilité de « voler » une adresse MAC (MAC Spoofing)
- Chiffrer les données (avec un bon cryptage…)

La Sécurité (3)

Couche MAC pour la sécurité

Le cryptage

- Utiliser un chiffrement pour les données

- l 'implémentation WEP (Wired Equivalent Privacy) (clé sur 40 bits / 104bits) donnée par les utilisateurs auquel est rajouté un vecteur d'initialisation (24 bits).

Fonctionnement : chiffrement RC4 en utilisant clé + vecteurs d'initialisation (IV)

message envoyé = (M.c(M)) xor RC4(IV . K)

{ c(M) = cheksum de M et K = clé
{ le RC4 donne des séquences pseudo-aléatoires

Le vecteur d'initialisation change à chaque trame envoyée, on lui rajoute 1

(assez facilement crackable si on connaît le 1er octet de M et IV)

Pb : faiblesse d'implémentation dans IV commencent à 0 puis incrémentés de 1 à chaque envoi, vecteurs faibles ….

Actuellement, quelques dizaines de minutes pour cracker clé WEP 128 bits

Si utilisation de WEP, alors codage supplémentaire : ssl, Ipsec, ssh,…

La Sécurité (4)

Couche MAC pour la sécurité

Le cryptage (suite)

- Utiliser la norme 802.1x ou 802.11i (WPA : Wifi protected Access ou WPA2)

=> concerne spécifiquement l'authentification

- 3 acteurs :
  - -> le client (demandeur ou supplicant)
  - -> le point d'accès relais (NAS : Network Access Server)
  - -> le serveur d'authentification = serveur RADIUS

codage en utilisant les trames EAP : Extensible Authentication Protocol

- Pour le chiffrement : remplacement de WEP par TKIP

Temporal Key Integrity Protocol (changement de clé souvent)

(cela ne sert à rien de décrypter une clé si elle n'est plus utilisée)

Le roaming

- **But** : permettre à un appareil sans fil qui se déplace de rester connecté
  - protocole IAPP : Inter-Access Point Protocol (norme 802.11F)
    -Utilisation de 4 ou 5 trames pour changer de AP
    - Pb : aucune sécurité

Latence trop longue lors d'une authentification 802.1X

Nouvelle norme : 802.11r

Fast Basic Service Set Transition

idée : les clés de chiffrement sont mises en cache dans les AP

→ gain de temps

VoIP (Voix sur IP)

- Généralités
- Un protocole particulier : SIP
- un exemple d'IPBX :
  - Asterisk

La voix sur IP (1)

• **Définition :**

Le principe est de faire circuler sur Internet, grâce au protocole IP, les paquets de données correspondant à des échantillons de voix numérisée.

• **Fonctionnement :**

La conversation analogique est encodée dans un format numérique, avec compression possible, et encapsulée dans des paquets IP pour être transportée sur le réseau WAN/LAN

La VoIP consiste à intégrer la voix et les données dans un même réseau :

➡ ce qui permet de réaliser des économies car maintenance d'un seul réseau, c'est **la convergence** voix et donné

La voix sur IP (2)

Quelques problèmes

- Un réseau unique et en cas de panne, des conséquences plus graves
- Une fiabilité des réseaux de données moins bonne que celles des réseaux voix (➔ perte des paquets)
- Présence d'une latence dans le réseau
  - 0 à 300 ms , acceptable pour la plupart des conversations
  - 300 à 700 ms, devient pratiquement une conversation half duplex
  - > 700 ms, inutilisable
- Notion de Qos (Quality of Service)

Terminologie (1)

Terminologie

- VoIP: Voix sur IP (Voice over IP)
  La voix circule sur le réseau IP et aussi sur le réseau RTC

- ToIP : Téléphonie sur IP (Telephony over IP)
  La voix ne circule que sur le réseau IP

- IP Phone : Un téléphone se branchant sur le réseau
  téléphone analogique + adaptateur téléphonique analogique = ip phone

- Softphone : Un logiciel faisant office de téléphone
  (nécessite la configuration de la carte son → x-lite, msn, skype, …)

- IPBX : Autocommutateur logiciel travaillant avec communications IP (voire des communications RTC)

Terminologie (2)

Terminologie

- PABX : Private Automatic Branching eXchange
  nom commun donné pour un autocommutateur

- PSTN : Public Switched Telephone Network
  nom anglais du RTC

- PoE : Power Over Ethernet (norme 802.3af)
  ➔ permet d'amener le courant électrique via la prise ethernet
  (utilisé pour les téléphones, les points d'accès, les capteurs,…)

- FXO/FXS : Foreign eXchange Office / Foreign eXchange Service
  Fxo : prise terminal (exemple téléphone)
  Fxs : prise fournissant le courant

Comment ça marche ?

VoIP n'est pas un protocole

- La voix sur IP est un nom générique regroupant un ensemble de protocoles et de méthodes permettant d'encoder, de transporter et de "router" des appels audios.

- **Plusieurs étapes**
  - La voix est échantillonnée et codée sur 8 bits
  - Le signal est compressé (utilisation des codecs de compression)
  - Mise en relation des différentes entités
    couche session : H323, SIP, propriétaire…
  - Chaque paquet est envoyé sur le réseau
    Problème : le réseau n'utilise que très peu de contraintes temporelles
    nouveaux protocoles : RTP, RTcP
  - etc …

Codec

- Codec :
  - Compresseur / Décompresseur
    Codeur / Décodeur
    } ?

• G. 711 (alias PCM Pulse Code Modulation)
-> Codage de la voix sur 8 bits, 8000 fois par seconde
-> autrement nommé : u-law (en Amérique) et a-law (reste du monde)

•G. 723.1 : débit de 5,3kb/s ou 6,3 kb/s
-> compatible avec le protocole H323
-> licence protégée par brevet

•G. 729 : -> débit 8 kb/s , codage CS-ACELP , licence protégée par brevet

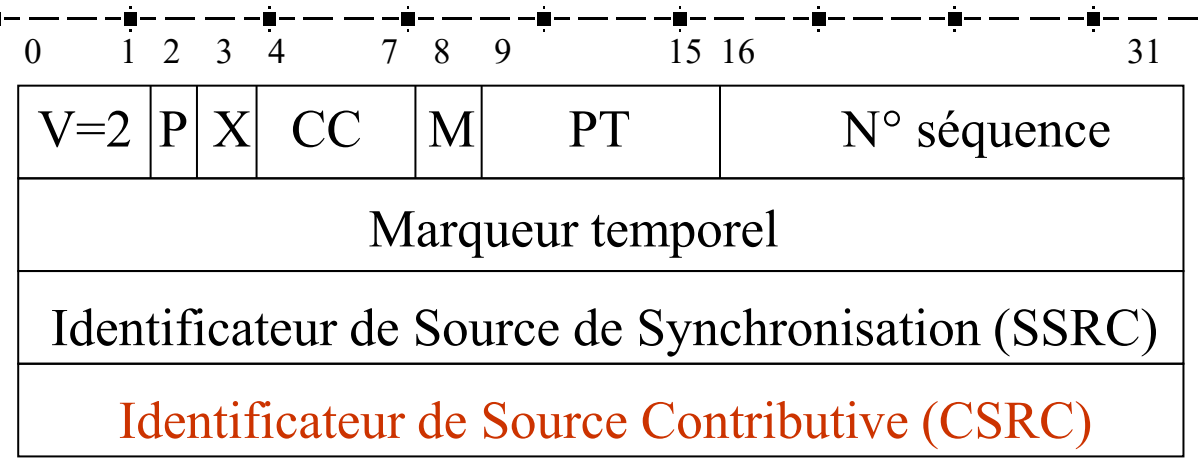
•GSM : débit 13 kb/s
-> moins bon que le reste, mais gratuit

RTP

- **RTP : Real Time Protocol**
  - RFC 3550, 3551
  - Protocole de transfert de données en temps réel pour l'audio et la vidéo
  - Au-dessus de la couche 4 (utilisation d'UDP ou de TCP)
  - Permet
    - de reconstituer une base de temps
    - le séquencement des paquets
    - l'identification des contenus

RTP s'appuie sur RTCP (Real Time Control Protocol) pour le contrôle de flux et la QoS.

En-tête RTP (1)



v = version (actuellement 2)

P : padding → existence de bourrage à la fin du paquet ? 0=non

X : extension de l'entête : 0 = non, 1 = oui

CC : nombre de CSRC (généralement 0)

M : Marquage → à 1, après un silence (reprise de parole)

Pt : Payload = type de codec utilisé ex : G711 a-law =8, u-law=0, G729=18

N° séquence : permet de repérer le paquet (augmente de 1 à chaque fois)

Marqueur temporel : permet la gestion des tampons et de la gigue du réseau, augmente de 1

SSRC : Nombre aléatoire désignant la source du paquet RTP (ce nombre ne change pas)

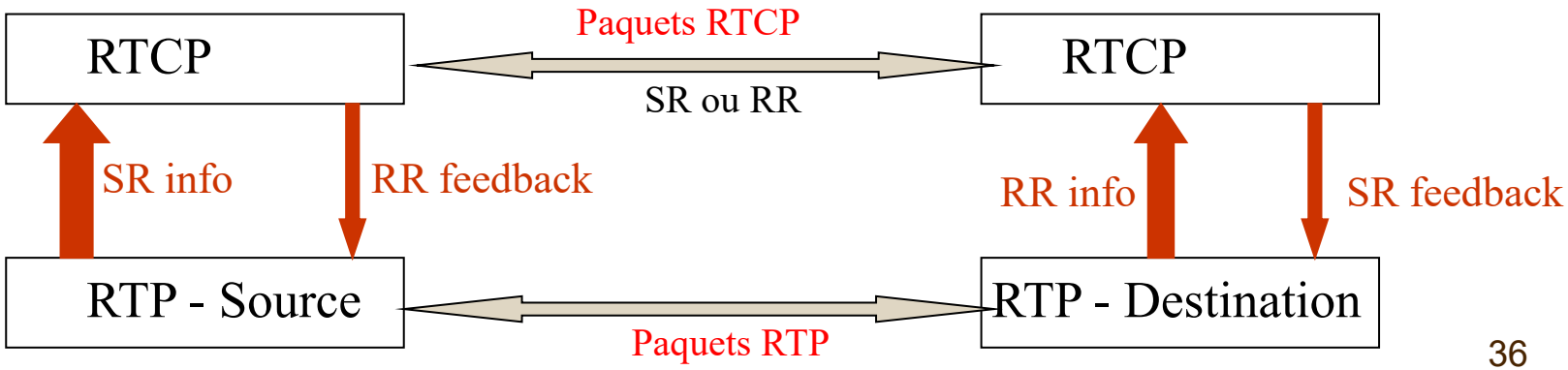
RTCP (1)

- RTCP permet d'assurer une QoS à RTP (trame de contrôle de RTP, mais optionnel)

- En général, RTCP utilise le port juste au-dessus de RTP
  exemple : RTP : 6066 <-> 12567 RTCP: 60767 <-> 12568

- 2 sortes de paquets :
  - SR : Sender Report
  - RR : Receiver Report

- Utilisation d'une horloge NTP pour synchroniser RTP



SIP (1)

SIP (Session Initiation Protocol)

- Concurrent direct de H 323, mais au départ plus simple
- créé par l'IETF, RFC 3261
  - mais des extensions -> RFC 3262 à 3265
  - d'autres protocoles :
    - SDP Session Description Protocol (RFC 2327)
    - RSVP : utilisé pour la qualité de service
    - RTP/RTCP : pour faire transiter les données

Attention, SIP ne prend pas en charge le transfert des données ….

- Protocole tout IP
- Requête/ réponse très proche de HTTP ou SMTP
- Développé pour prendre en charge l'ouverture d'une session, puis de fournir une description du type de session demandée

Les entités SIP (1)

User Agent

Equipement terminal pour recevoir ou émettre

- UAC : User Agent Client
  -> initie les requêtes SIP
- UAS : User Agent Server
  -> réponse à la requête

SIP était à l'origine un protocole orienté point à point

→ Pour contacter UAS, besoin de connaître son @IP
impossible à généraliser

Registrar ou Registration Server

Enregistre dans une base de données les correspondances entre les adresses SIP (URI SIP sip:utilisateur@domaine.com) et IP

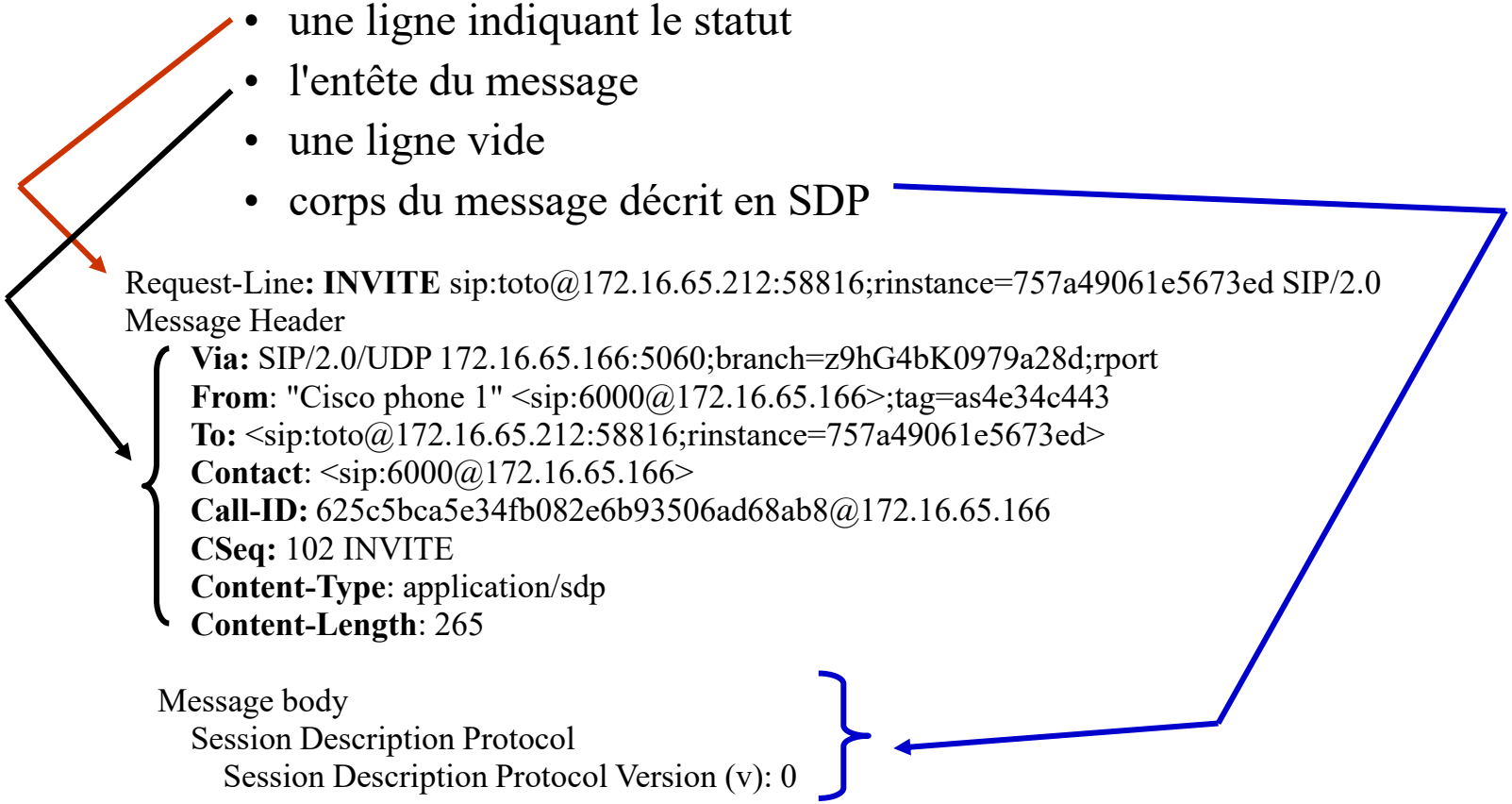
- Un UAC s'enregistre toujours dans un registrar

Les entités SIP (2)

- **Proxy SIP**
  - Prend en charge le routage des appels
  - Permet de trouver l'adresse du destinataire
    (peut utiliser des requêtes DNS)
  - Registrar et Proxy SIP sont en général très liés
- **Redirect Server**
  - permet de rediriger une adresse SIP vers une autre adresse SIP
- **Location Server**
  - interroge les registars pour trouver l'adresse IP

Les messages SIP

- SIP est un protocole client/serveur (comme http)
  - le client envoie une requête et attend une réponse
  - le chemin parcouru par les paquets est arbitraire (sur UDP)
  - les requêtes et les réponses ont la même structure :
    - une ligne indiquant le statut
    - l'entête du message
    - une ligne vide
    - corps du message décrit en SDP



SDP

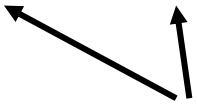
SDP Exemple 1

v=0
o=- 2 2 IN IP4 172.16.66.212
s=Counter Path X-lite
t=0 0
c=IN IP4 172.16.65.212
m=audio 49170 RTP/AVP 0 3

Champ	Description
Version	v=0
Origine	o=<username> <session id> <version> <network type> <address type> <address>
Nom de session	s=<session name>
Times	t=<start time> <stop time>
Connexion info	c=<network type> <address type> <connection address>
Media	m=<media> <port> <transport> <media format list>

SDP Exemple 2

v=0
o=picard 124333 67895 IN IP4 uunet.com
s=Engage!
t=0 0
c=IN IP4 101.234.2.1
m=audio 3456 RTP/AVP 0 107 109 8 98 …



code pour le G.711

Les méthodes (1)

- Les méthodes sont spécifiées dans les premiers octets de chaque requête SIP, spécifiant ainsi le contenu du message

- Il y a deux types de requêtes :
  - celle initialisant le dialogue telle que INVITE ou SUBSCRIBE
  - celle à l'intérieur d'un dialogue et pouvant modifier la session actuelle, telle que BYE ou NOTIFY

- INVITE
  - initialise la session, "invite" un client à parler
  - paramètres de la session se trouve dans le corps de la requête

    (Media Description, Media Attribute,…)

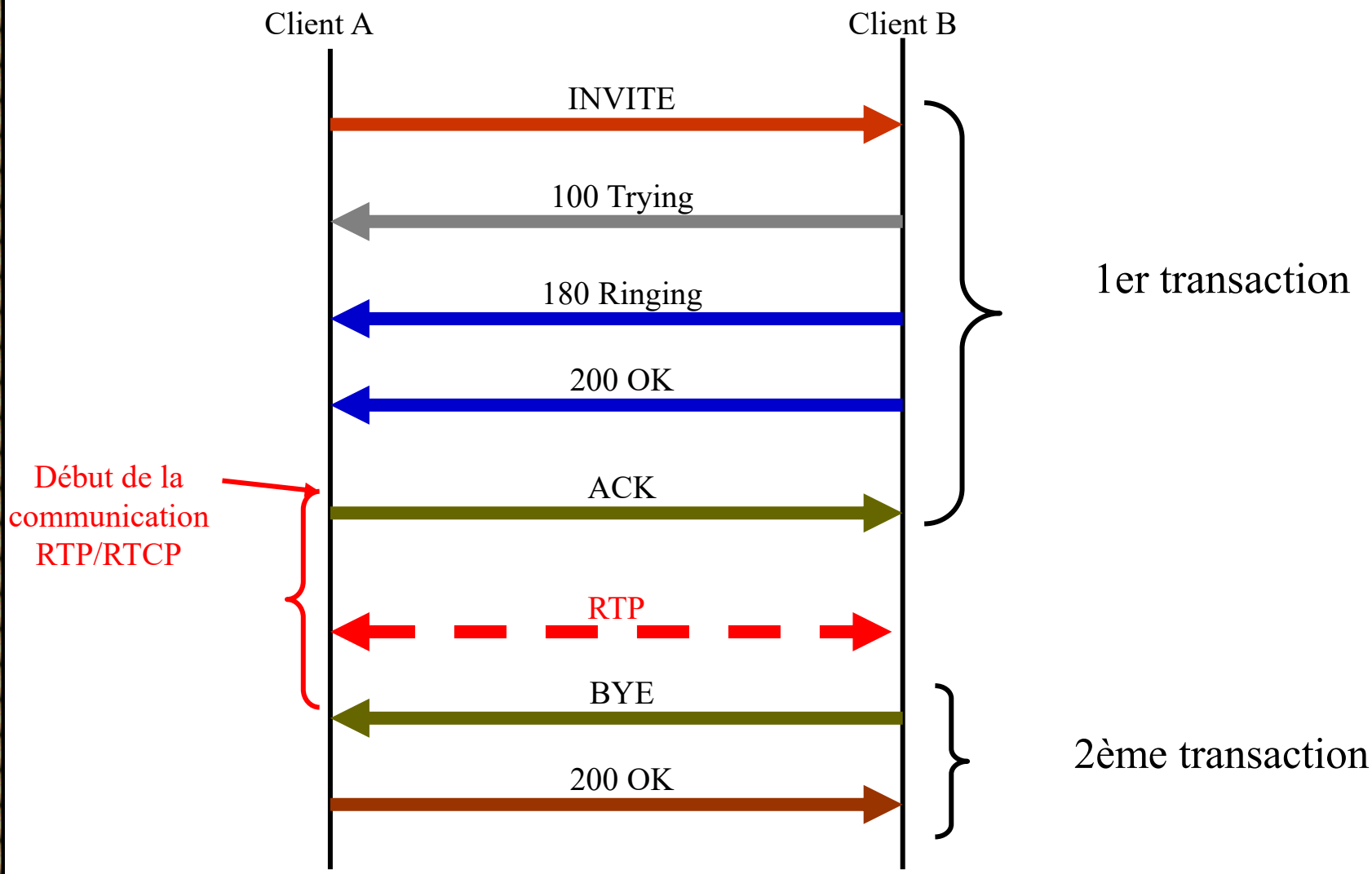
Les méthodes (2)

- ACK
  - confirme l'établissement d'une session (retour de INVITE)
- BYE
  - termine une session
- CANCEL
  - annule une transaction (exemple : INVITE)
- OPTIONS
  - permet de récupérer des informations sur le serveur
- REGISTER
  - permet de s'enregistrer auprès d'un registrar
- SUBSCRIBE
  - pour s'informer sur un agent, comme dans une messagerie instantanée
- NOTIFY
  - permet d'envoyer un événement dans la "messagerie instantanée"
- etc …

Les réponses

- Comme pour HTTP, les réponses sont des codes sur 3 chiffres
  - 1xx : Informational response
    - 100 : trying
    - 180 : ringing
  - 2xx : succès
    - 200 : OK
  - 3xx : Redirection response
    - 301 : moved permanently
  - 4xx : erreur client
    - 400 : Bad Request
    - 404 : Not found
    - 408 : Request Timeout
  - 5xx : server failure
    - 500 : internal error
  - 6xx : Global failures

Exemple de dialogue (1)



Problèmes SIP

Pare-feu et NAT

- SIP fonctionne en UDP sur le port 5060
  → simple pour un pare-feu

  MAIS session RTP sur un port quelconque….

- Problème d'adressage pour le NAT
  - présence de l'adresse non routable dans SDP
    ➡ impossible de faire un paquet retour

•Solution :

- STUN (RFC 3489) : (**Simple Traversal of UDP through NATs**)
  utilisation d'un serveur auxilliaire STUN
- ICE (**Interactive Connectivity Establishment)**
- TURN (**Traversal Using Relay NAT)**
- **IPv6** (sans NAT)

Asterisk (1)

- **Asterisk** est un PABX applicatif open source permettant d'interconnecter en temps réel des réseaux de voix sur IP et des réseaux de téléphonies classiques via des cartes d'interface téléphonique.

- Protocoles implémentés:
  - IAX™ (Inter-Asterisk Exchange)
  - H.323
  - SIP (Session Initiation Protocol)
  - MGCP (Media Gateway Control Protocol)
  - SCCP (Cisco® Skinny®)

- Codecs:
  - ADPCM
  - G.711 (A-Law & µ-Law)
  - G.723.1 (pass through)
  - G.726
  - G.729 (through purchase of commercial license through Digium)
  - GSM
  - iLBC
  - Linear
  - LPC-10
  - Speex

NTP - Généralité

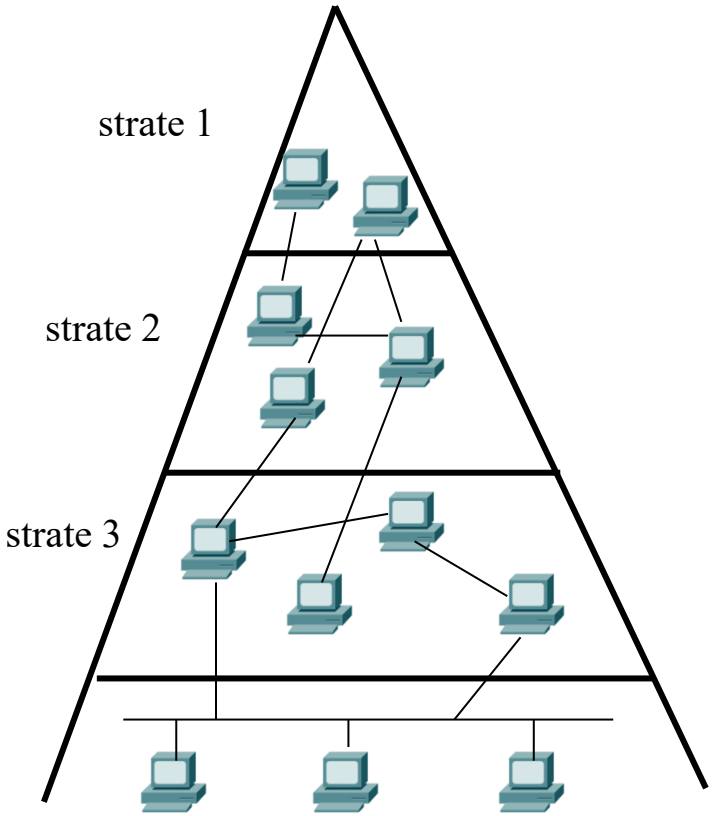
- NTP – Network Time Protocol
  - Protocole réseau permettant de mettre à jour son horloge en se synchronisant sur des serveurs de temps présents sur Internet.

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

-Contraintes :

- la différence entre deux machines doit être inférieure à une certaine valeur
- l'horloge d'une machine avance continûment dans le temps

NTP – Principe



Utilisation de la notion de strate

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

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

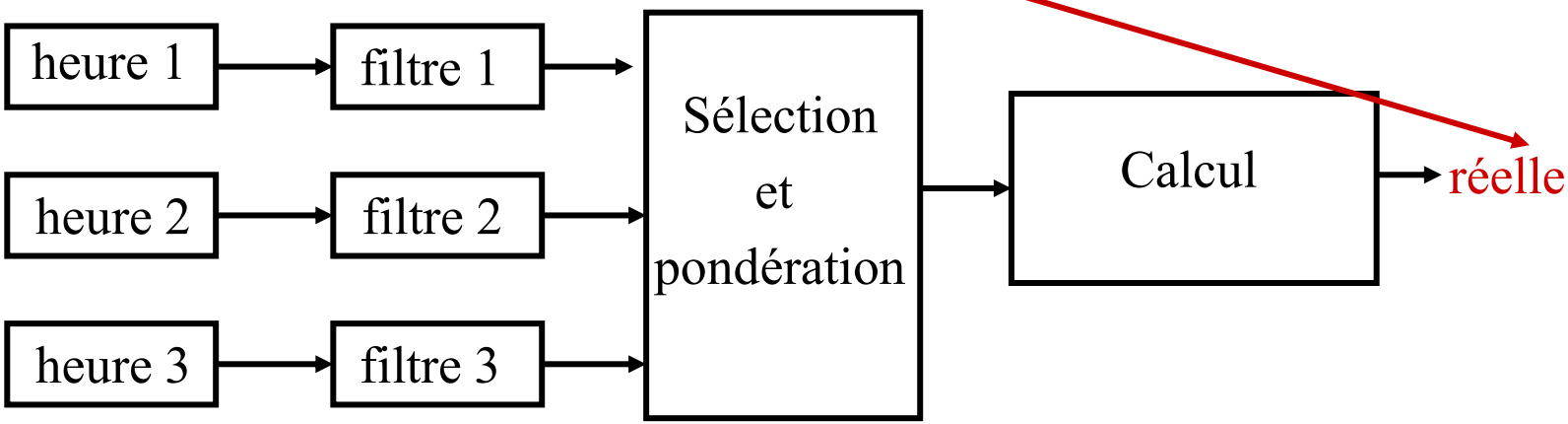
NTP –Synchronisation (1)

- Synchronisation

  → mise en place d'une variable d'ajustement

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

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



NTP –Synchronisation (2)

- Codage du temps sur 64 bits (Timestamp)
- Date du début du codage : 1 janvier 1900
- validité jusqu'en 2036… mais passage en version 128 bits.

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

  Hypothèse : temps aller = temps retour

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

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

NTP -configuration

- Sous linux
  - dans le fichier /etc/ntp.conf
    -- indiquer la liste des serveurs à utiliser

- Sous Windows XP
  - par ligne de commande
    - net time /setsntp:nom_serveur ntp
    - at 12:03 every:date net time /setsntp:nom_serveur ntp

  - graphiquement :
    - double-click sur l'heure, puis temps internet