LES PROTOCOLES RESEAU

DEFINITION :

Un protocole réseau est un protocole de communication mis en œuvre sur un réseau informatique ou un réseau de télécommunications.

Il est fréquent que plusieurs protocoles réseau forment des couches de protocoles.

v · m	Couches du modèle OSI [masquer]
7. Application	BGP · DHCP · DNS · FTP · FTPS · SFTP · FXP · Gemini · Gopher · H.323 · HTTP · HTTPS · IMAP · IPP · IRC · LDAP · LMTP · MODBUS · NFS · NNTP · POP · RDP · RTSP · SILC · SIMPLE · SIP · SMB-CIFS · SMTP · SNMP · SOAP · SSH · TCAP · Telnet · TFTP · VoIP · World Wide Web · WebDAV · XMPP
6. Présentation	AFP · ASCII · ASN.1 · HTML · MIME · NCP · TDI · TLS · TLV · Unicode · UUCP · Vidéotex · XDR · XML
5. Session	AppleTalk · DTLS · NetBIOS · RPC · RSerPool · SOCKS
4. Transport	DCCP · RSVP · RTP · SCTP · SPX · TCP · UDP
3. Réseau	ARP · Babel · BOOTP · CLNP · ICMP · IGMP · IPv4 · IPv6 · IPX · IS-IS · NetBEUI · NDP · RIP · EIGRP · OSPF · RARP · X.25
2. Liaison	Anneau à jeton (token ring) · Anneau à jeton adressé (Token Bus) · ARINC 429 · AFDX · ATM · Bitnet · CAN · Ethernet · FDDI · Frame Relay · HDLC · I²C · IEEE 802.3ad (LACP) · IEEE 802.1aq (SPB) · LLC · LocalTalk · MIL-STD-1553 · PPP · STP · Wi-Fi · X.21
1. Physique	4B5B · ADSL · BHDn · Bluetooth · Câble coaxial · Codage bipolaire · CSMA/CA · CSMA/CD · DSSS · E-carrier · EIA-232 · EIA-422 · EIA-449 · EIA-485 · FHSS · HomeRF · IEEE 1394 (FireWire) · IrDA · ISDN · Manchester · Manchester différentiel · Miller · MLT-3 · NRZ · NRZI · NRZM · Paire torsadée · PDH · SDH · SDSL · SONET · SPI · T-carrier · USB · VDSL · VDSL2 · V.21-V.23 · V.42-V.90 · Wireless USB · 10BASE-T · 10BASE2 · 10BASE5 · 100BASE-TX · 1000BASE-T
Articles liés	Pile de protocoles · Modèle Internet · Couche 8

LES PROTOCOLES RESEAU

LE PROTOCOLE **ARP** (**A**ddress **R**ésolution **P**rotocol)

Définition :

L'Address resolution protocol (ARP, protocole de résolution d'adresse) est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse ethernet), ou même de tout matériel de couche de liaison. Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

Il a été défini dans la RFC 826 : An Ethernet Address Resolution Protocol.

Le protocole ARP est nécessaire au fonctionnement d'IPv4 utilisé au-dessus d'un réseau de type ethernet. En IPv6, les fonctions de ARP sont reprises par le Neighbor Discovery Protocol (NDP).

Remarque :

Le protocole ARP a été conçu sans souci particulier de sécurité. Il est vulnérable à des attaques locales sur le segment reposant principalement sur l'envoi de messages ARP erronés à un ou plusieurs ordinateurs. Elles sont regroupées sous l'appellation ARP poisoning (pollution de cache ARP). La vulnérabilité d'un ordinateur à la pollution de cache ARP dépend de la mise en œuvre du protocole ARP par son système d'exploitation.

LES PROTOCOLES RESEAU

LE PROTOCOLE **ARP** (**A**ddress **R**ésolution **P**rotocol)

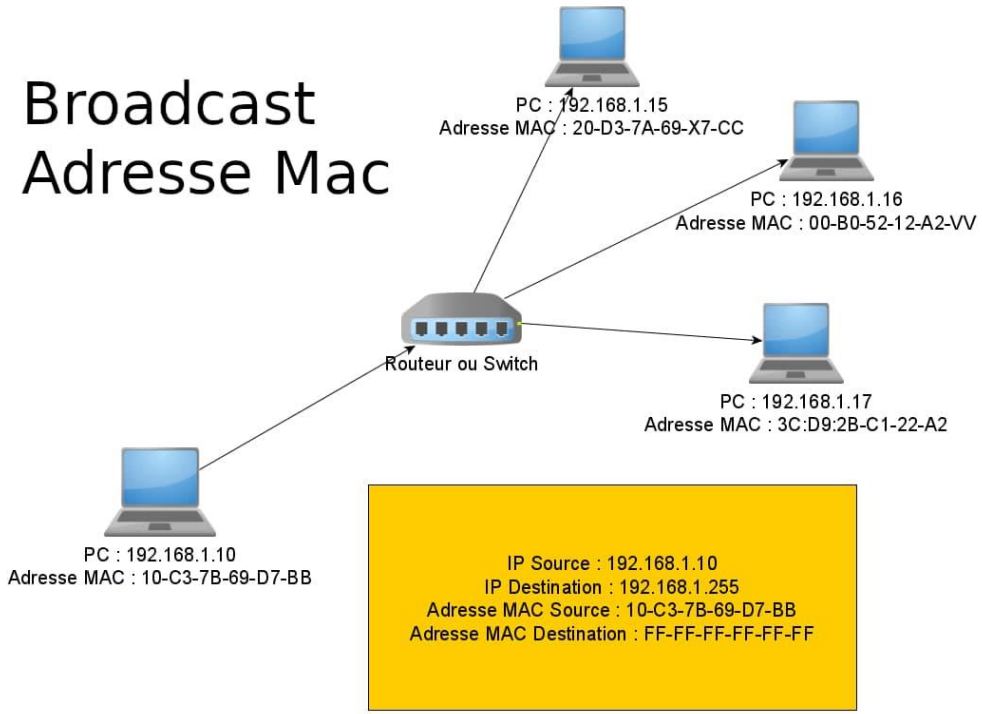
Mode de fonctionnement:

Imagions un réseau local LAN composés deux PC (PC1 et PC2) connectés en Ethernet.
Le PC1 a un paquet à envoyer à PC2.
Par une résolution DNS, il détermine que le PC2 a l'adresse IP 192.168.0.15.

Pour envoyer le message, il nécessite également de connaître l'adresse MAC de PC2.
Tout d'abord, PC1 utilise une table ARP cache pour rechercher 192.168.0.15 pour tout enregistrement existant de l'adresse MAC de PC2 (20:D3:7A:69:X7:CC).

Si l'adresse MAC est trouvée, elle envoie un cadre Ethernet avec l'adresse de destination 20:D3:7A:69:X7:CC, contenant le paquet IP sur le lien.

Si le cache n'a pas produit de résultat pour 192.168.0.15, Le PC1 doit envoyer un message de demande ARP diffusé sur le broadcast (destination FF: FF: FF: FF: FF ADRESSE MAC), qui est acceptée par tous les ordinateurs sur le réseau local, demandant une réponse pour 192.168.0.15



LES PROTOCOLES RESEAU

- LES PROTOCOLES **TCP (T**ransmission **C**ontrol **P**rotocol**)** et **UDP** (**U**ser **D**atagram **P**rotocol)

Définition :

TCP comme UDP s'exécute au-dessus de IP et se fonde sur les services fournis par ce dernier.

TCP assure un service de transmission de données fiable avec une détection et une correction d'erreurs de bout en bout

UDP offre un service de transmission de datagrammes sans connexion.

Avec TCP/UDP, il est possible de remettre des données à des processus d'application s'exécutant sur une machine distante. Ces processus d'application sont identifiés par numéros de port. Une Socket (historiquement développé dans UNIX BSD) est un point de communication par lequel un processus peut émettre été recevoir des informations. C'est la combinaison d'une adresse IP et d'un numéro de port. La combinaison des deux sockets définit une connexion TCP ou un échange UDP.

La RFC 1060 définit les ports prédéfinis pour les services :

Exemple :

20 = FTP 25 = SMTP 69 = TFTP 443 = HTTPS

23 = Telnet 53 = DNS 80 = HTTP 3389 = RDS etc.

LES PROTOCOLES RESEAU

LES PROTOCOLES **TCP (T**ransmission **C**ontrol **P**rotocol**)** et **UDP** (**U**ser **D**atagram **P**rotocol)

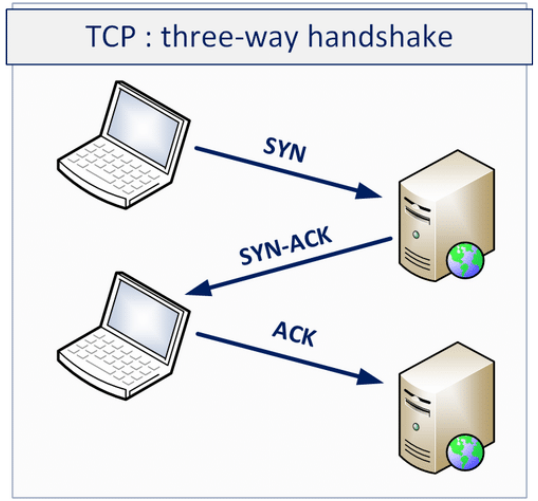
Le protocole TCP :

Une session TCP fonctionne en trois phases :

- l'établissement de la connexion : Ouverture d'une Socket, échange initial avec synchro des numéros de séquence entre les deux parties
- Les transferts de données : Pendant la phase de transferts de données, certains mécanismes clefs permettent d'assurer la robustesse et la fiabilité de TCP. En particulier, les numéros de séquence sont utilisés afin d'ordonner les segments TCP reçus et de détecter les données perdues, les sommes de contrôle permettent la détection d'erreurs, et les acquittements ainsi que les temporisations permettent la détection des segments perdus ou retardés.
- la fin de la connexion : La phase de terminaison d'une connexion utilise un handshaking en quatre temps, chaque extrémité de la connexion effectuant sa terminaison est de manière indépendante.

liste de quelques protocoles populaires qui s'appuient sur TCP :

- Les protocoles HTTP et HTTPS, notamment pour charger le contenu des sites Internet
- Le protocole SMTP pour envoyer des e-mails
- Le protocole NFS pour transférer des données (sur certaines versions uniquement)
- Le protocole SMB pour transférer des données
- Les protocoles SSH et Telnet pour la gestion à distance d'un équipement
- Le protocole RDP pour l'administration d'un hôte via le Bureau à distance
- Le protocole LDAP pour interroger un annuaire comme l'Active Directory



LES PROTOCOLES RESEAU

- LES PROTOCOLES **TCP (T**ransmission **C**ontrol **P**rotocol**)** et **UDP** (**U**ser **D**atagram **P**rotocol)

Le protocole UDP :

le protocole UDP est utilisé pour transporter les données, il va envoyer les données d'un hôte source vers un hôte de destination, sans chercher à savoir si l'hôte de destination a bien reçu l'ensemble des données. Autrement dit, il n'y a pas de vérification des erreurs : si l'on envoie un fichier via UDP, on ne sait pas si l'hôte distant a reçu entièrement ce fichier ou s'il l'a reçu partiellement.

Puisque l'on ne vérifie pas que l'hôte distant a bien reçu les données, on économise des ressources, mais aussi du temps, donc le protocole UDP est plus rapide que le protocole TCP.

L'en-tête d'un segment UDP contient très peu de champs : le port source, le port de destination, la longueur totale du segment, la somme de contrôle (pour vérifier l'intégrité du segment envoyé par le réseau) et les données.

quelques exemples de protocoles qui utilisent UDP comme protocole de transport, tout en sachant que cette liste n'est pas exhaustive.

- Le protocole DNS pour la résolution des noms (même si TCP peut être utilisé dans de rares cas)
- Le protocole SNMP pour la supervision des équipements
- Le protocole NTP pour la mise à jour de la date et l'heure via le réseau
- Le protocole TFTP pour le transfert de fichiers simplifié

LES PROTOCOLES RESEAU

- LES PROTOCOLES **HTTP** (**H**yper **T**ext **T**ransfer **P**rotocol) et **HTTPS** (**H**yper **T**ext **T**ransfer **P**rotocol **S**ecure)

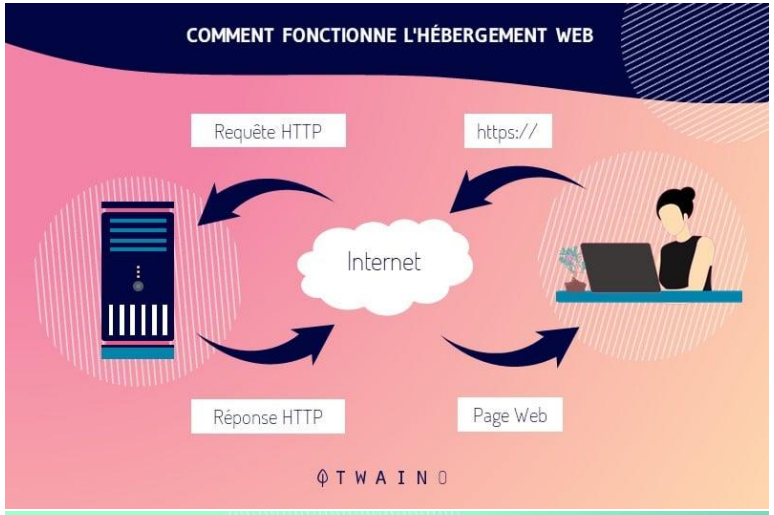
Définition :

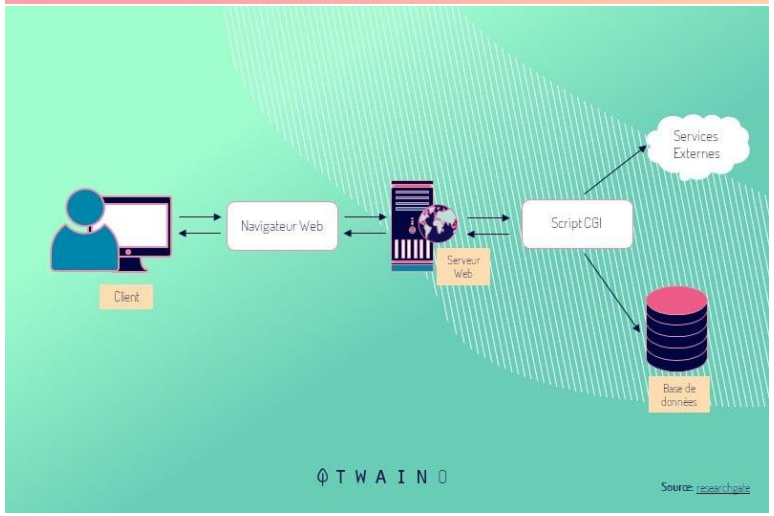
L'HyperText Transfer Protocol, généralement abrégé HTTP, littéralement « protocole de transfert hypertexte », est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (avec S pour secure, soit « sécurisé ») est la variante sécurisée par le chiffrement et l'authentification.

HTTP est un protocole de la couche application dans le modèle OSI. Il peut fonctionner sur n'importe quelle connexion fiable. Dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).

Les clients HTTP les plus connus sont les navigateurs Web. Il est aussi utilisé dans des interfaces de programmation d'application (API) pour accéder aux données d'un serveur ainsi que des systèmes pour récupérer automatiquement le contenu d'un site tels que les aspirateurs de site Web et les robots d'indexation.

Le protocole HTTPS (Hyper Text Transfer Protocol Secure) est une extension sécurisée du protocole HTTP, le « S » pour « Secured » (sécurisé) signifie que les données échangées entre le navigateur de l'internaute et le site web sont chiffrées et ne peuvent en aucun cas être espionnées (confidentialité) ou modifiées (intégrité). Obtenir le sacro-saint « S » passe par l'acquisition et l'installation d'un certificat SSL/TLS auprès d'une Autorité de Certification reconnue. Cela affichera ainsi le HTTPS, le cadenas vert et le mot « Sécurisé » dans la barre d'adresse du navigateur.





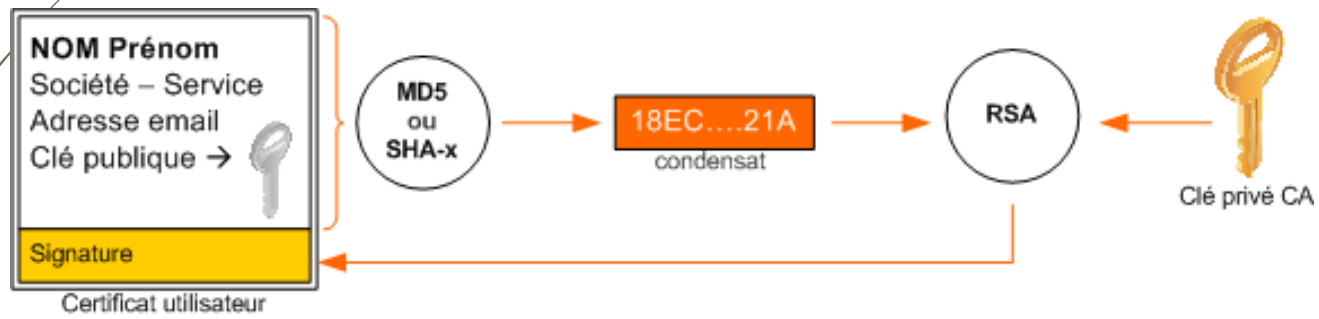
LES PROTOCOLES RESEAU

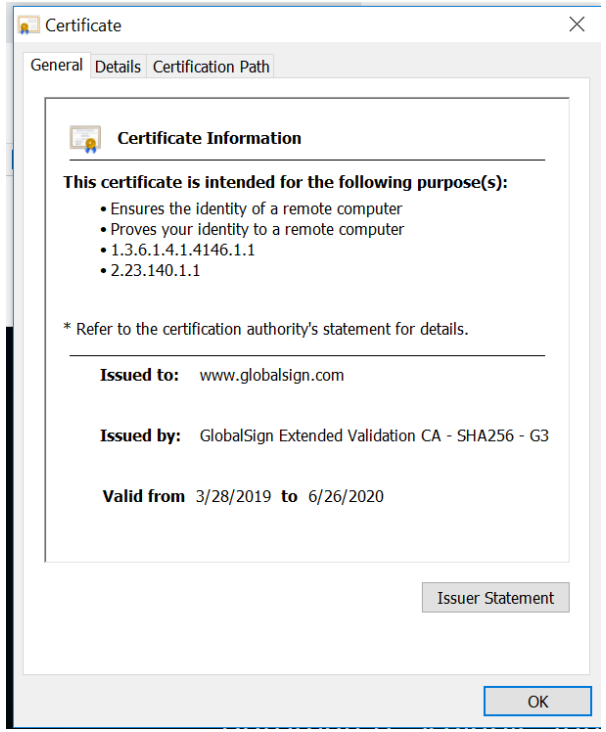
LES CERTIFICATS : Définition

Un **certificat électronique** (aussi appelé **certificat numérique** ou **certificat de clé publique**) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges.

Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique (virtuelle). Pour un site web il s'agit d'un certificat SSL.

Le standard le plus utilisé pour la création des certificats numériques est le X.509.





- infalsifiable : il est chiffré pour empêcher toute modification.
- nominatif : il est délivré à une entité (comme la carte d'identité est délivrée à une personne et une seule).
- certifié : il y a le « tampon » de **l'autorité** qui l'a délivré.

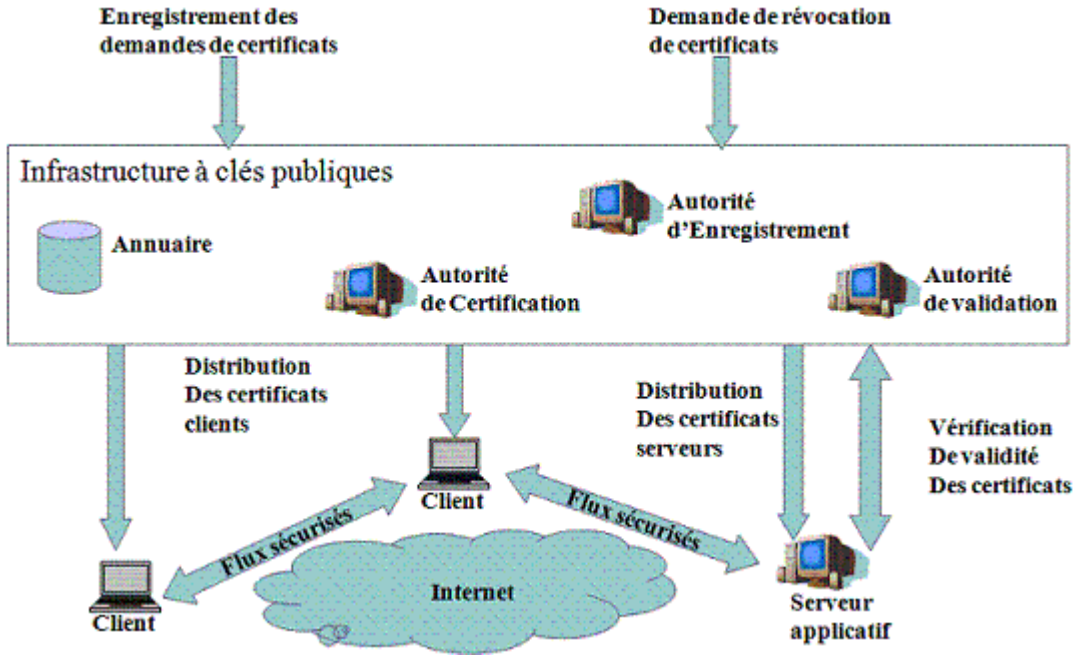
LES PROTOCOLES RESEAU

LES CERTIFICATS : **Les autorités de certification -** Public Key Infrastructure (PKI)

Les autorités de certification sont des organismes enregistrés et certifiés auprès d'autorités publiques et/ou de gouvernance de l'Internet qui établissent leur viabilité comme intermédiaire fiable.

Ces organismes diffusent leurs propres clés publiques. Étant certifiées fiables, ces autorités sont en contact direct avec les principaux producteurs de systèmes d'exploitation et de navigateurs web (tels que Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, etc.) qui incluent nativement les listes de clés des autorités de certification.

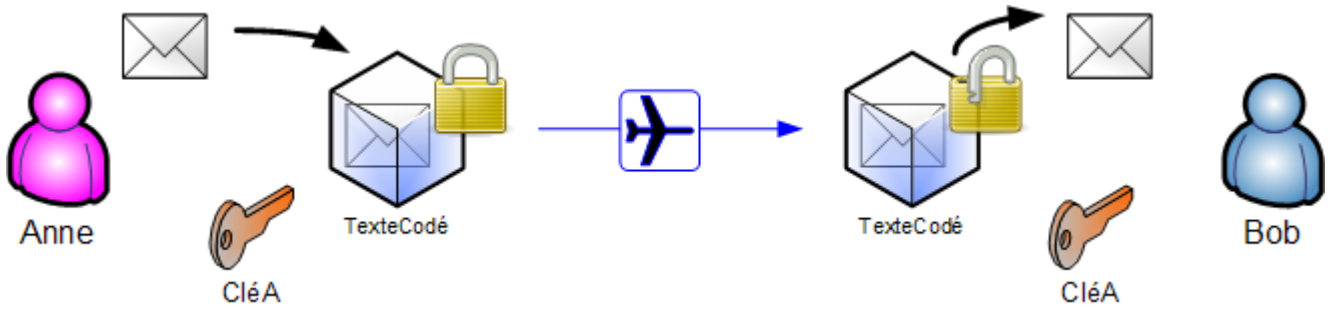
C'est cette relation qui est à la base de la chaîne de confiance. Ces clés sont appelées *clés publiques racines* ou *certificats racines* et sont utilisées pour identifier les clés publiques d'autres organismes.



LES PROTOCOLES RESEAU

- LES CERTIFICATS : **Chiffrement symétrique**

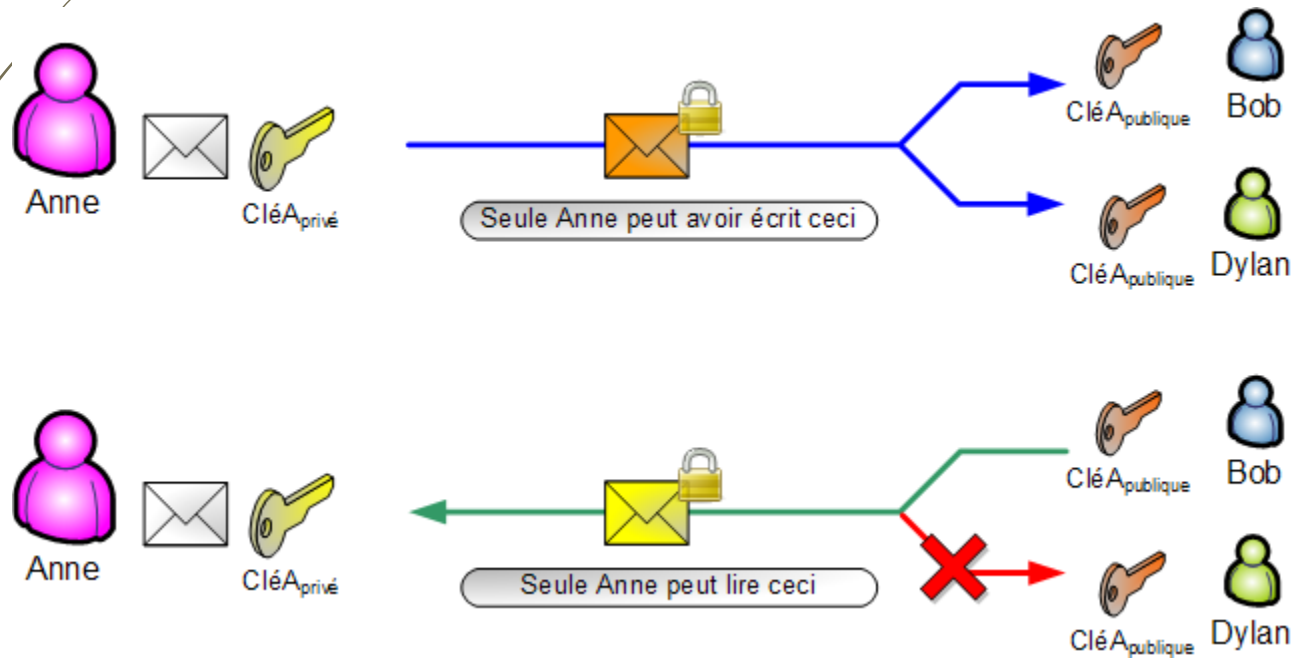
Cette méthode est la plus simple à comprendre : si Anne (A) veut envoyer un message chiffré à Bob (B) elle doit lui communiquer un mot de passe (clé de chiffrement). Comme l'algorithme de chiffrement est symétrique, on a la relation suivante :
TexteCodé = chiffrement du message par la clé

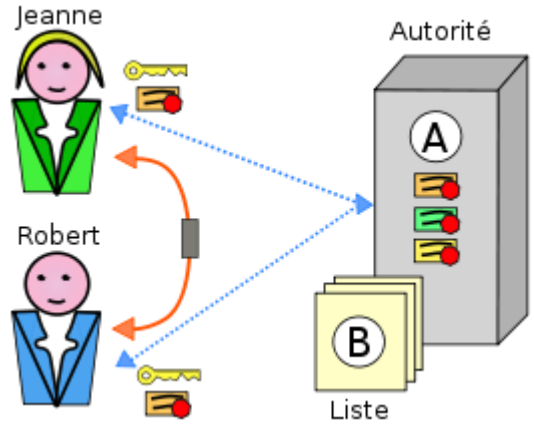


LES PROTOCOLES RESEAU

- LES CERTIFICATS : **Chiffrement Asymétrique**

La propriété des algorithmes asymétriques est qu'un message chiffré par une clé privée sera lisible par tous ceux qui possèdent la clé publique correspondante. À l'inverse, un message chiffré par une clé publique n'est lisible que par le propriétaire de la clé privée correspondante.





LES PROTOCOLES RESEAU

- LES PROTOCOLES **AS** (**A**ccess **S**tratum) et **NAS** (**N**on **A**ccess **S**tratum)

AS (Acces Stratum) : La strate d'accès fait références aux protocoles relatifs à l'accès radio qui permettent de gérer l'échange d'information (pour rappel signalisation et données) entre l'UE et coeur réseau de l'opérateur. L'AS fait référence aux couches basses de la pile protocolaire OSI.

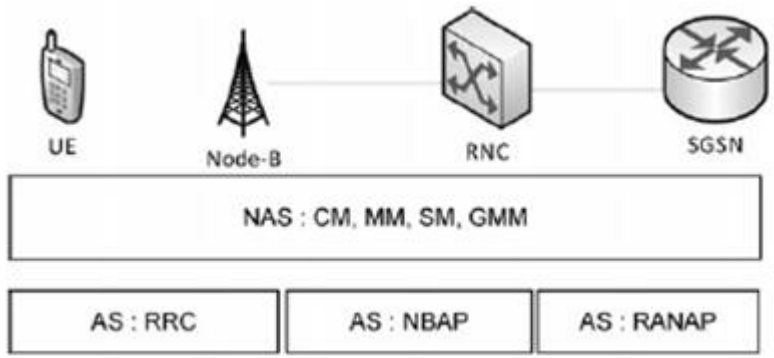
NAS (Non Acces Stratum) : Le NAS (strate de non-accès) représente un ensemble de protocoles qui s'établit entre l'UE et le réseau coeur. Le NAS permet l'échange d'information de contrôle ou de données quel que soit l'accès radio. Le NAS s'appuie donc sur l'AS pour transporter ses données.

Les rôles de la Strate d'Accès :
Les principales fonctions liées au réseau d'accès (UTRAN Universal Terrestrial Radio Access Network) sont les suivantes

- •Gestion des ressources radio
- •Handover
- •Chiffrement/Compression

Les rôles de la Non Strate d'Accès
La couche NAS a deux rôles essentiels

- •Gestion des sessions (et des appels pour la 3G)
- •Gestion de la mobilité.



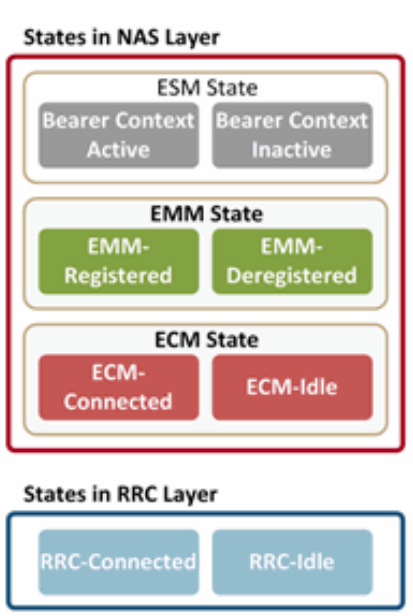
Réseau 3G

LES PROTOCOLES RESEAU

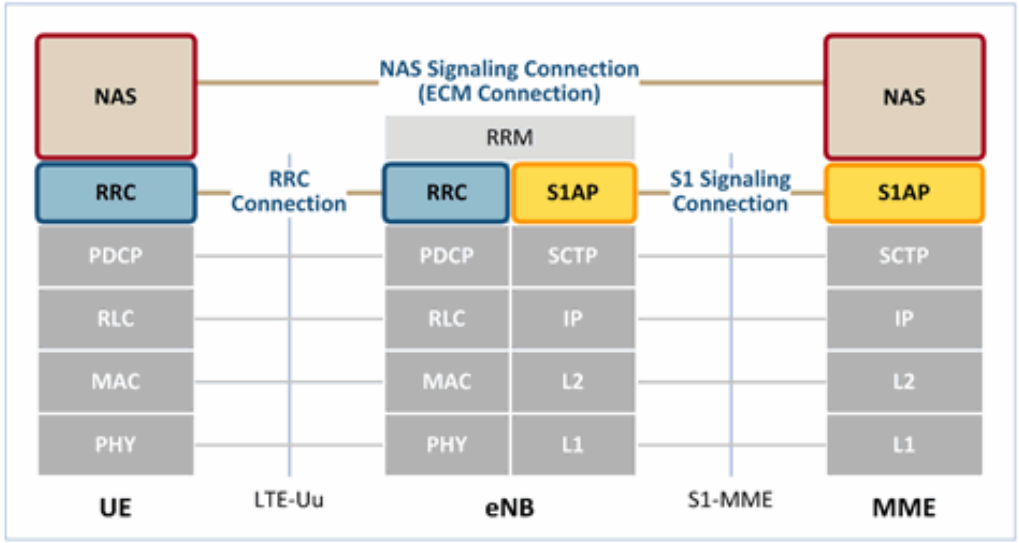
- LES PROTOCOLES **AS** (**A**ccess **S**tratum) et **NAS** (**N**on **A**ccess **S**tratum)

Pour le LTE, les protocoles se nomment:

- **ESM** : EPS Session Management
- **EMM** : EPS Mobility Management.



Réseau 4G



Les rôles de la Strate d'Accès : La strate d'accès regroupe donc les couches basses : RRC, PDCP, RLC, MAC et Phy. Les messages NAS, entre l'UE et le Nb ou eNb sont encapsulé dans les messages RRC.