DOCUMENTATION

DT1 - SQL on MySQL

Créer une table tbl :	`CREATE TABLE tbl ( id INT PRIMARY KEY, ... )`
Supprimer une base de données :	`DROP DATABASE ...`
Sélectionner les informations de la table :	`SELECT ...`
Écrire une nouvelle entrée dans la table :	`INSERT INTO ...`
Modifier une table :	`UPDATE ...`
Supprimer une entrée dans la table :	`DELETE ...`

Type champs les plus fréquents dans une base de données :

- NUMERIC (numérique), cela comprend les types INT, FLOAT, DOUBLE, BOOL...
- STRING (Caractère) correspond à VARCHAR(n) variable jusqu'à n caractères
- DATE contient date et heure (exemple de format date "2018-09-24 22:21:20")
- BOOLEAN : TRUE / FALSE

Jointure : sélection sur plusieurs tables

```
SELECT * FROM table1, table2
WHERE table1.attribut1 = table2.attribut2 ;

SELECT * FROM table1 JOIN table2
ON table1.attribut1 = table2.attribut2 ;

DELETE table1 FROM table1 JOIN table2
ON table1.attribute_name = table2.attribute_name WHERE condition ;
```

MySQL supports foreign keys, which permit cross-referencing related data across tables, and foreign key constraints, which help keep the related data consistent.

A foreign key relationship involves a parent table that holds the initial column values, and a child table with column values that reference the parent column values. A foreign key constraint is defined on the child table.

The essential syntax for defining a foreign key constraint in a CREATE TABLE or ALTER TABLE statement includes the following:

```
[CONSTRAINT [symbol]] FOREIGN KEY
    [index_name] (col_name, ...)
    REFERENCES tbl_name (col_name,...)
    [ON DELETE reference_option]
    [ON UPDATE reference_option]

reference_option:
    RESTRICT | CASCADE | SET NULL | NO ACTION | SET DEFAULT
```

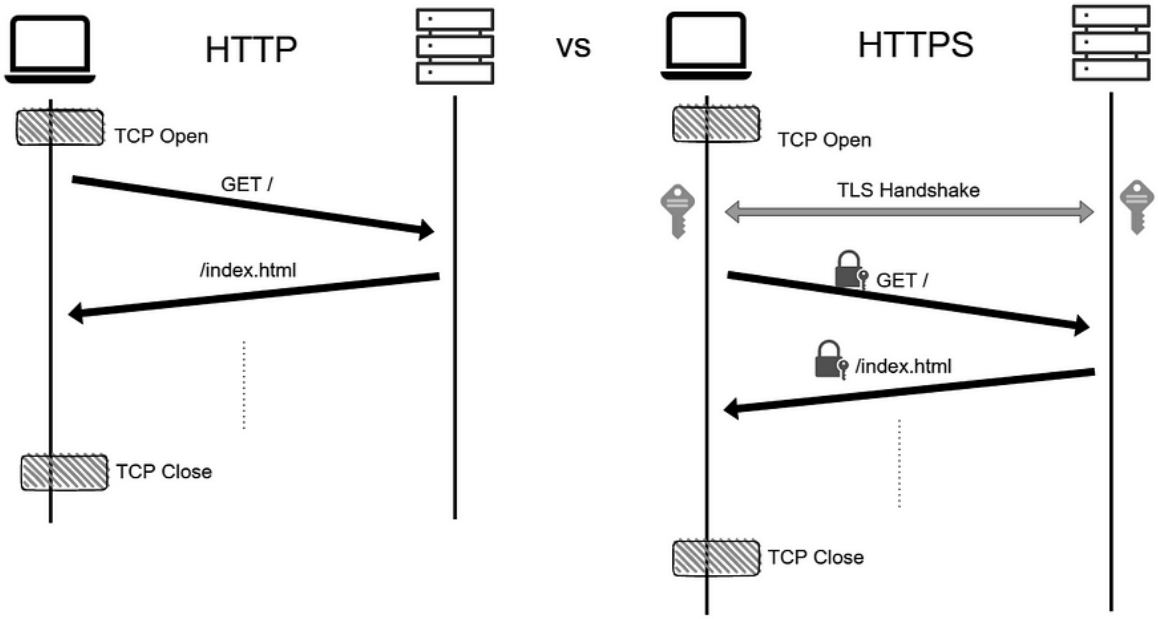
DT2 - Documentation WLC3504

Le Cisco WLC3504 est un contrôleur sans fil conçu pour fournir un contrôle, une gestion et un dépannage centralisés des réseaux sans fil dans les petites et moyennes entreprises. Il s'agit d'une plateforme compacte, hautement évolutive et riche en fonctionnalités, capable de prendre en charge les réseaux de génération 802.11ac Wave 2.

- évolutivité et performance :
    - débit de 4 Gbps ;
    - 150 points d’accès ;
    - 3000 clients ;
    - 1 interface Ethernet Multigigabit (jusqu'à 5 Gigabit), + 4 interfaces Gigabit ;
    - 4096 VLANs.
- configurations groupées : le WLC3504 permet la configuration groupée des points d’accès, facilitant ainsi le déploiement et la gestion des réseaux sans fil à grande échelle. Les administrateurs peuvent appliquer des paramètres communs à plusieurs points d’accès simultanément, réduisant ainsi les efforts de configuration ;
- band steering : cette fonctionnalité dirige automatiquement les clients vers la bande de fréquence 5 GHz, permettant une répartition plus équilibrée de la charge et une performance améliorée pour les utilisateurs finaux ;
- load balancing : le WLC3504 équilibre la charge des clients entre les points d'accès, assurant une utilisation optimale des ressources réseau et une meilleure expérience utilisateur ;
- WPA3 et 802.1X : le WLC3504 supporte les dernières normes de sécurité, y compris WPA3 pour le chiffrement des données et 802.1X pour une authentification sécurisée des utilisateurs. Ces technologies assurent une protection avancée contre les menaces et les attaques ;
- détection des intrusions : le contrôleur dispose de mécanismes de détection des intrusions, alertant les administrateurs en cas d’activités suspectes sur le réseau et contribuant à maintenir la sécurité de l’infrastructure sans fil ;
- redondance des points d'accès : si un point d'accès échoue, le contrôleur peut réaffecter automatiquement les utilisateurs à d'autres points d'accès disponibles, garantissant ainsi une continuité de service et une disponibilité élevée du réseau.

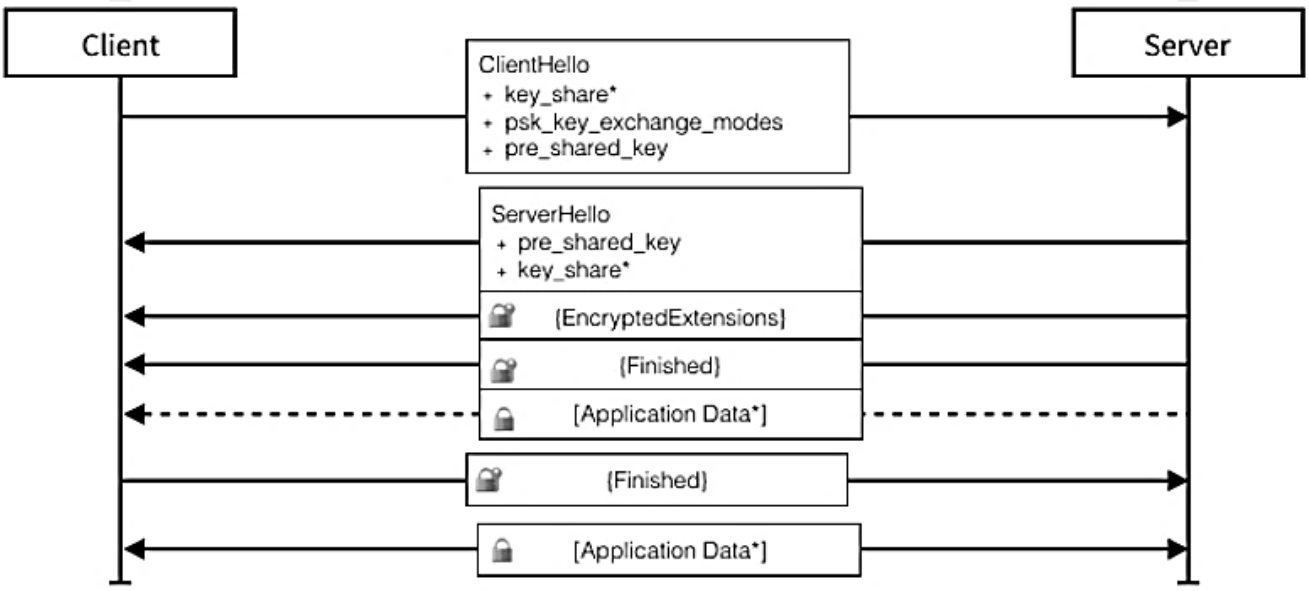
DT3 - Présentation http/https

- Requête HTTP, les échanges ne sont pas chiffrés.
- Dans HTTPS, les échanges sont chiffrés à l'aide d'une clé partagée.

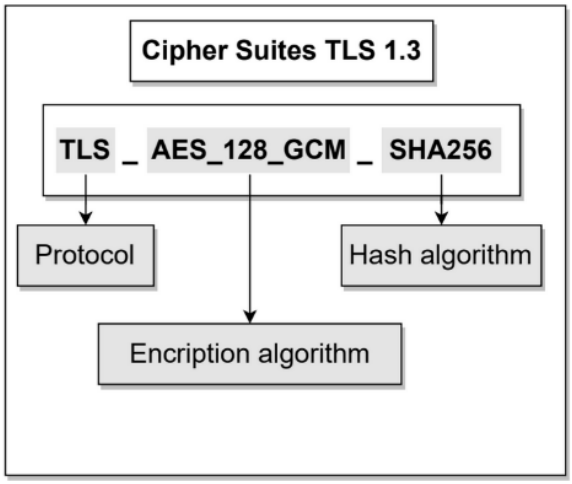


- <u>Diagramme de séquence TLS v1.3 « reprise de session » ou « reprise avec un PSK»</u>

  Comme le serveur s'authentifie via une clé PSK, il n'envoie pas de certificat ni de message CertificateVerify. Lorsqu'un client propose une reprise via une clé PSK, il doit également fournir une extension « key_share » au serveur pour permettre à ce dernier de refuser la reprise et de revenir à une négociation complète, si nécessaire. Le serveur répond avec une extension « pre_shared_key » pour négocier l'utilisation de l'établissement de clé PSK et peut répondre avec une extension « key_share » pour effectuer l'établissement de clé (EC)DHE sans retransmission du certificat.



- **Suite de chiffrement TLS v1.3**



Suite de chiffrement	Clé AES	Hachage	Sécurité estimée	Durée théorique de résistance aux attaques par force brute
TLS_AES_128_GCM_SHA256 (0x13, 0x01)	128 bits	SHA-256	2^{128}	**10^7 ans** (actuellement inviolable avec des ressources actuelles)
TLS_AES_256_GCM_SHA384 (0x13, 0x02)	256 bits	SHA-384	2^{256}	**10^{77} ans** (pratiquement inviolable)
TLS_AES_128_CCM_SHA256 (0x13, 0x04)	128 bits	SHA-256	2^{128}	**10^7 ans** (similaire à AES-128-GCM)
TLS_AES_128_CCM_8_SHA256 (0x13, 0x05)	128 bits	SHA-256	2^{128}	**10^7 ans** (similaire à AES-128-GCM, mais le tag réduit peut affecter la sécurité)

DT4 - Documentation ASA5506

Le Cisco ASA 5506 est un pare-feu de nouvelle génération qui fait partie de la série ASA 5500-X. Il est conçu pour fournir une protection avancée des réseaux, notamment pour les petites et moyennes entreprises (PME).

Il utilise un niveau de sécurité associé à chaque interface. Il s'agit d'un nombre compris entre 0 et 100 qui définit la fiabilité du réseau auquel l'interface est connectée ; plus le nombre est élevé, plus la confiance accordée au réseau est élevée. La mise en place de ces niveaux de confiance est nécessaire pour la création d'une DMZ.

Voici un aperçu de ses spécifications et de ses fonctionnalités :

Caractéristiques techniques

- Ports et Interfaces :
    - interfaces Ethernet : 8 ports Gigabit Ethernet, avec des configurations pouvant inclure des ports SFP pour la connectivité en fibre ;
    - port de gestion : port dédié pour la gestion administrative du pare-feu.
- Performance :
    - débit de pare-feu : jusqu'à 300 Mbps pour le trafic de pare-feu ;
    - débit VPN : prend en charge jusqu'à 100 Mbps pour le trafic VPN, offrant une bonne performance pour les connexions sécurisées ;
    - connexions simultanées : capable de gérer jusqu'à 100 000 connexions simultanées.
- Caractéristiques de sécurité :
    - inspection des paquets : inspection approfondie des paquets pour détecter les menaces et bloquer les attaques ;
    - contrôle d'accès : politiques de contrôle d'accès basées sur l'utilisateur et l'application ;
    - détection des menaces : capacités de prévention des intrusions (IPS) et intégration avec Cisco Firepower pour une détection avancée des menaces ;
    - access Control Lists (ACL) et Network Address Translation (NAT) : pour une DMZ à trois interfaces.

Fonctionnalités Avancées

- VPN :
    - prise en charge des VPN IPsec et SSL, permettant des connexions sécurisées pour les utilisateurs distants ;
    - fonctionnalité de tunnel split pour la gestion des connexions.
- Gestion et surveillance :
    - cisco ASDM : interface graphique pour une configuration et une gestion simplifiée ;
    - syslog et notifications : intégration avec des systèmes de gestion des événements pour le suivi et l'alerte.
- Filtrage de contenu :
    - capacité de filtrage d'URL pour bloquer l'accès à des sites non sécurisés ou inappropriés ;
    - contrôle des applications pour gérer l'utilisation des applications web.

Scalabilité et Extensibilité

- mises à jour de licences : les fonctionnalités peuvent être étendues grâce à des mises à jour de licences, permettant d'adapter le pare-feu aux besoins croissants de l'entreprise ;
- modules d'extension : possibilité d'ajouter des modules pour des fonctionnalités supplémentaires, comme l'IPS ou le filtrage avancé.

Déploiements typiques

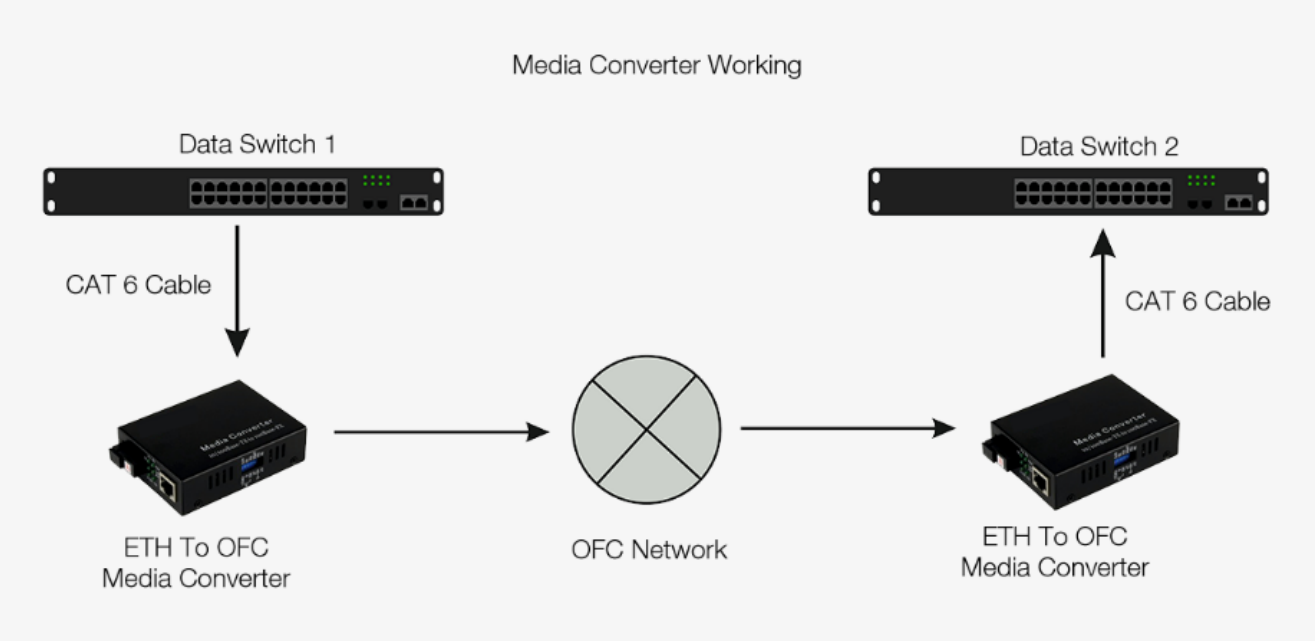
- sécurisation des bureaux distants : idéal pour les environnements de travail à distance, offrant des connexions VPN sécurisées ;
- protection des réseaux internes : renforcement de la sécurité des réseaux internes contre les menaces externes ;
- conformité réglementaire : aide à répondre aux exigences de conformité pour des secteurs comme la finance, la santé ou l'éducation.

DT5 - Technologies de connexions réseau

Technologie	Type de connexion	Distance maximale	Caractéristiques principales
Fibre optique monomode	Fibre optique	Jusqu'à 80 km (ou plus avec des équipements spécifiques)	Conçue pour la transmission de données sur de longues distances avec faible atténuation. Utilise un seul mode de lumière.
Fibre optique multimode	Fibre optique	Jusqu'à 300 mètres (en général)	Idéale pour des distances plus courtes, comme dans les bâtiments. Utilise plusieurs modes de lumière, ce qui peut entraîner une dispersion.
RJ45 (Ethernet)	Câble cuivre (TP)	100 mètres (norme 100BASE-TX)	Utilisé pour les réseaux locaux, avec des vitesses allant jusqu'à 1 Gbps (ou plus avec des normes avancées).
Wi-Fi (802.11ac/ax)	Sans fil	Environ 30 à 100 mètres (en fonction des conditions)	Connexion sans fil pour les réseaux locaux, avec des vitesses pouvant atteindre plusieurs Gbps dans les normes récentes. Sensible aux interférences et aux obstacles.

DT6 - Documentation coût des ressources

OFC : Optical Fiber Communication



SFP Module :

Réf : MGBSX1	**Réf : MGBT1**	**Réf : MGBLX1**
Module SFP 1000BASE-SX 850nm 550m DOM LC Duplex MMF	Module SFP 1000BASE-T en Cuivre RJ-45 100m	Module SFP 1000BASE-LX/LH 1310nm 10km DOM LC Duplex MMF/SMF
		
Distance de Transfert Maxi. : 550m sur OM2 MMF Longueur d'Onde 850nm	- RJ-45 - Cat 5e/6/6a (UTP) - 2 x 1000Base-T RJ-45 - 1 x console RJ-45	Longueur d'Onde : 1310nm Distance de Transfert Maxi. :10km@SMF
7€ HT	28€ H.T	8€ H.T

Convertisseurs (réf 5618) lot de 2

	• SFP non inclus. • Convertisseur Fibre Ethernet, Convertisseur RJ45 Gigabit / Module mini-GBiC SFP Multimode-Monomode/0.55-20km. Conforme aux normes IEEE 802.3ab et IEEE 802.3z Ports : 1 Gigabit SFP port ; 1, 10M/100M/1000M RJ45 port (Auto MDI/MDIX). • Extension de la distance de la fibre optique jusqu'à 550 mètres en multimode et 20 km en monomode. • Network Media 1000BASE-X : Multi-mode/Single-mode SFP module. • Network Media 1000BASE-T : UTP category 5, 5e, 6 cable (maxium 100 m) ; EIA/TIA-568 100Ω STP (maximum 100 m). Port FX échangeable à chaud. • Prix 35.82€ HT

Switch

	S5810-28FS	S3410-24TS-P	S3910-24TS
			
Ports RJ45	8x 1G (8 Combo)	24x 1G	24x 1G
Ports SFP	28x 1G SFP	2x 1G SFP (Combo)	—
Ports SFP+	4x 10G SFP+	2x 10G SFP+	4x 10G SFP+
Ports 25G/40G/100G	—	—	—
Couche de Gestion	L3	L2+	L2+
Empilage de Matériel	Jusqu'à 8 Unités	Jusqu'à 4 Unités	Jusqu'à 4 Unités
Redondant Remplaçable à chaud 1+1	✓	✓	✓
QoS, IGMP Snooping, Agrégation de Liaison, IPv6, Routage Statique L3, RIP, OSPF	✓	✓	✓
Protocole de Routage Avancé (BGP/ISIS)	✓	—	—
Sécurité Avancée	✓	✓	✓
PoE	—	PoE/PoE+	—
Prix (HT)	1348	968	619

Lexique :

SFP (Small Form-factor Pluggable) ;
MMF (Multi-Mode Fiber) ;
SMF (Single-Mode Fiber) ;
PoE (Power over Ethernet) 15,4 watts par port ;
PoE+ (Power over Ethernet Plus) 25,5 watts par port ;
PoE++(Ultra PoE) : Jusqu'à 60 watts par port (PoE Type 3) ou 100 watts par port (PoE Type 4).

Nous voulons justifier le coût d'une partie de l'infrastructure composée du switch du PGR et de la liaison entre ce dernier et AP2.
Le choix de la liaison physique entre le PGR et AP2, est l'utilisation d'une fibre multimode. La partie alimentation électrique de AP1 et AP2 n'est pas étudiée ici et ne doit pas être un critère de choix du matériel.

DT7 - RFC 6455, websocket

Norme RFC 6455 (web socket) :

Le « masking » est **obligatoire pour les clients** pour éviter les problèmes de sécurité liés à des proxys.

Principe du « Masking » RFC 6455 :

Pour chaque octet du message (payload) on fait un XOR avec l'octet de la clef de masquage qui lui correspond (4 octets), cette opération est répétée en boucle.

Format de la trame websocket RFC 6455

- 1 octet ***Opcode***= 0x81 ;
- 1 octet ***Length*** (payload) (b7=1, info length de b6->b0) ;
- 4 octets ***Masking*** ;
- N octets ***Payload***.

Trame web Socket= Byte_Opcode(1) + Byte_Length(1)+ Bytes_Masking_Key(4) + Byte(s)_Payload(n)

Exemple

Trame émise : `81 89 ff ab 89 cd ed 9f df b5 65 17 57 3d ed`

- 1 octet ***Opcode*** : 0x81 ;
- 1 octet ***Length*** (payload) (b7=1, info length de b6->b0)
  → `0x89` → 9 octets de payload
- ***Masking*** : `ff ab 89 cd`
- ***Payload*** : `12 34 56 78 9a bc de f0 12`

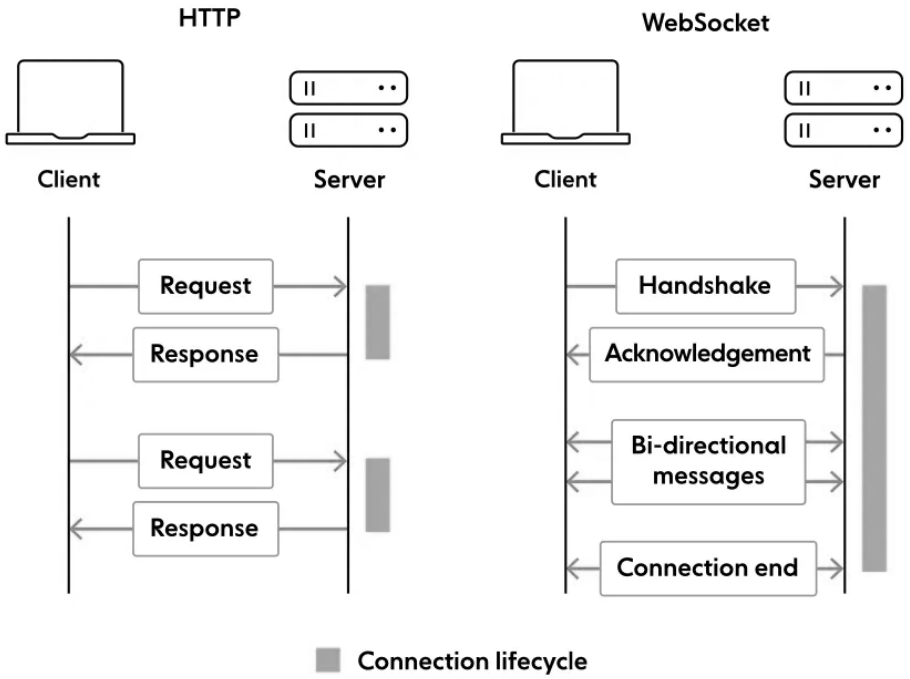
Payload	12	34	56	78	9a	bc	de	f0	12
Masking	ff	ab	89	cd	ff	ab	89	cd	ff
XOR	ed	9f	df	b5	65	17	57	3d	ed

La formule est :

Octet masqué = Octet brut ⊕ Octet de masquage

Remarque ⊕ symbole de XOR (ou exclusif) : A ⊕ B

WebSocket



Use Case protocole WebSocket :

1. webSocket Handshake : Le client lance la négociation en envoyant une requête HTTP GET au serveur, comprenant les en-têtes « Upgrade » et « Connection », indiquant l'intention d'établir une connexion WebSocket. La requête contient également un en-tête Sec-WebSocket-Key, qui est une valeur aléatoire codée en base64 générée par le client. Cette valeur permet de garantir que le serveur gère et répond correctement à la demande d'établissement de liaison ;

2. dès réception de la requête, le serveur la traite et vérifie que le client est compatible avec le protocole WebSocket. Si le serveur prend en charge les connexions WebSocket, il répond avec un code d'état HTTP 101 Switching Protocols, ainsi que les en-têtes « Mise à niveau » et « Connexion ». Le serveur crée également une valeur Sec-WebSocket-Accept unique en hachant la clé Sec-WebSocket-Key du client avec un GUID fixe et la renvoie dans la réponse ;

3. trames WebSocket : Une fois la connexion établie, les données sont échangées entre le client et le serveur à l'aide de trames WebSocket. Une trame se compose d'un en-tête contenant des informations de contrôle, suivi de la charge utile. Les trames peuvent être des trames de contrôle ou de données, les trames de contrôle gérant la connexion et les trames de données transportant du texte ou des données binaires ;

4. communication WebSocket : la connexion WebSocket permet une communication bidirectionnelle en temps réel entre le client et le serveur. Les données peuvent être envoyées et reçues simultanément, réduisant ainsi la latence et améliorant les performances du réseau. La connexion reste ouverte jusqu'à ce qu'elle soit explicitement fermée par le client ou le serveur ou jusqu'à ce que la connexion soit interrompue en raison d'erreurs réseau ou d'autres problèmes.

DT8 - Rédiger un test unitaire

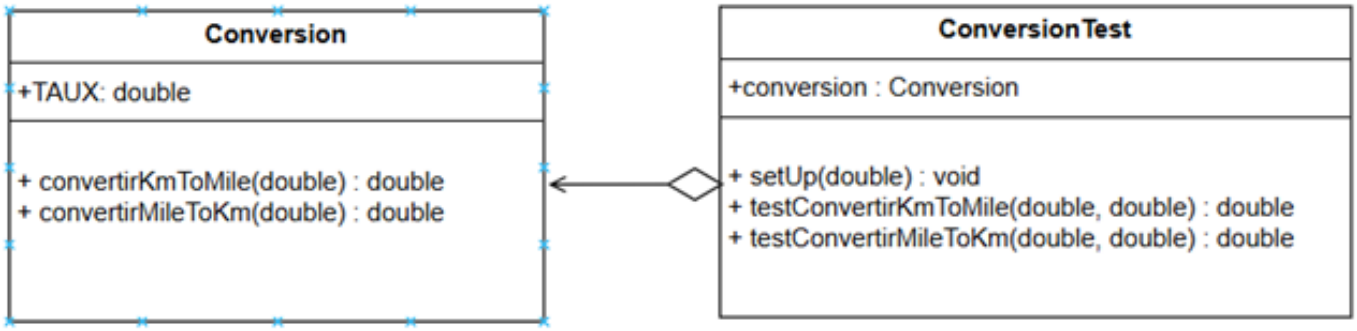


Diagramme de classes

Un test unitaire est fait sur la méthode convertirKmToMile() de la classe Conversion. Pour ce faire la classe ConversionTest permet d'effectuer des tests unitaires sur les méthodes de la classe Conversion.

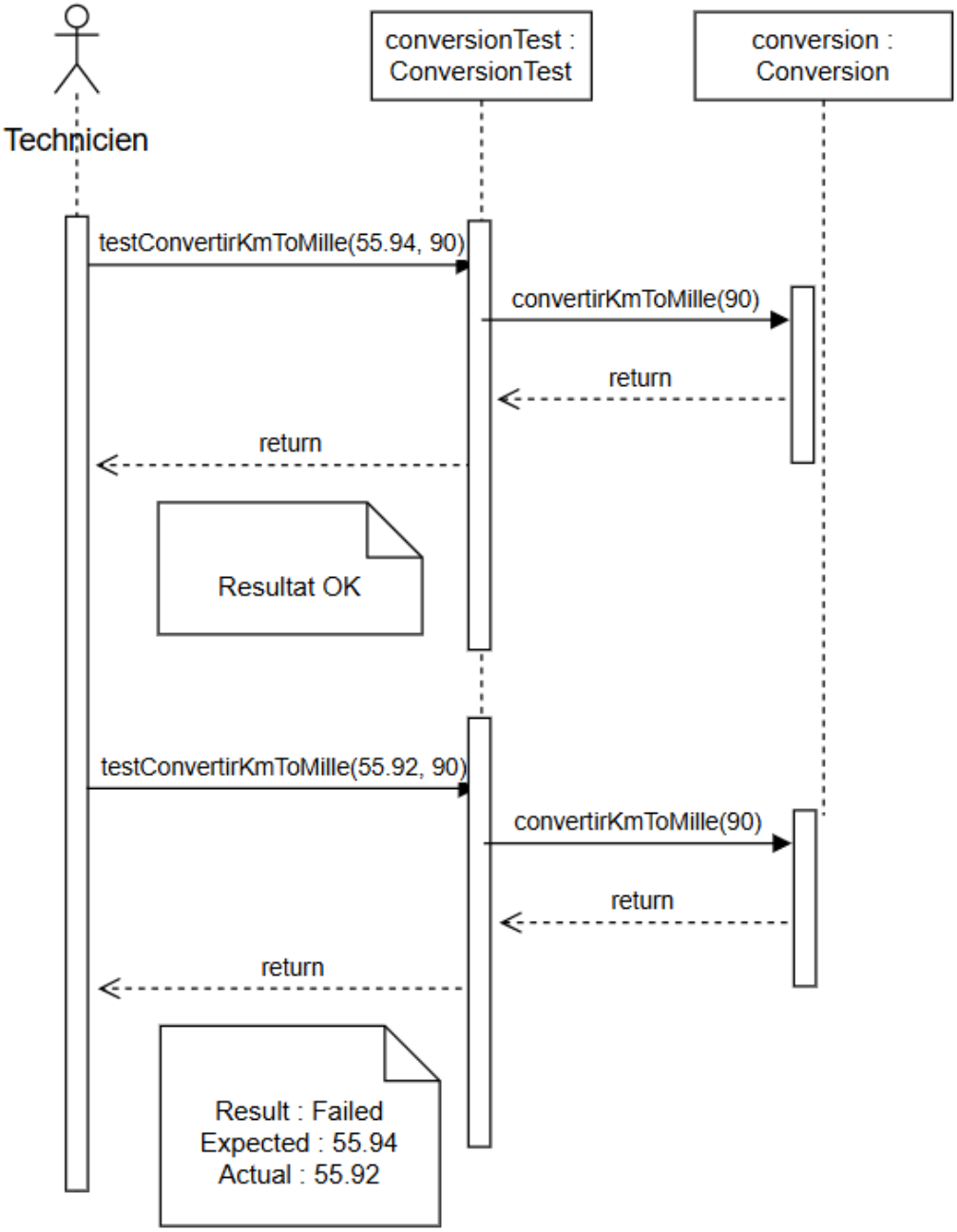
La méthode compare le premier paramètre et le résultat du deuxième paramètre.

Si les valeurs correspondent, le test passe.
Si les valeurs sont différentes, le test échoue.

Le diagramme de séquence ci-dessous déroule le test.

La première partie du diagramme est une séquence qui passe le test.

La deuxième partie du diagramme est une séquence qui ne passe pas le test.


Technicien
conversionTest : ConversionTest
conversion : Conversion
testConvertirKmToMille(55.94, 90)
convertirKmToMille(90)
return
return
Resultat OK
testConvertirKmToMille(55.92, 90)
convertirKmToMille(90)
return
return
Result : Failed
Expected : 55.94
Actual : 55.92

DT9 - Article 34 - Communication à la personne concernée d'une violation de données à caractère personnel

Source : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article34

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

   a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

   b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;

   c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.