BREVET DE TECHNICIEN SUPÉRIEUR

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE

Option A – Informatique et Réseaux

Épreuve E4

ÉTUDE ET CONCEPTION DE RÉSEAUX INFORMATIQUES

SESSION 2026

_____

Durée : 6 heures
Coefficient : 4

_____

Matériel autorisé

L'usage de calculatrice avec mode examen actif est autorisé.
L'usage de calculatrice sans mémoire, « type collège », est autorisé.

Tout autre matériel est interdit.

Chaque candidat remettra deux copies séparées : une copie « domaine professionnel » dans laquelle seront placés les documents réponses DR-Pro1 à DR-Pro8 et une copie « domaine de la physique ».

Ce sujet comporte :

Présentation	PR1 à PR9
Sujet	
Questionnaire domaine professionnel	S-Pro1 à S-Pro19
Questionnaire domaine de la physique	S-Ph1 à S-Ph13
Documentation technique	DOC1 à DOC16
Document réponses à rendre avec la copie	
Document réponses domaine professionnel	DR-Pro1 à DR-Pro8

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

PRÉSENTATION DU SYSTÈME

CISS CASHLESS ONLINE

1. Présentation

La société CISS propose des bornes interactives sur des stands de distribution de boissons et de snacks avec une solution de paiement sans contact appelée Cashless Online. Cette solution est utilisée dans le cadre de festivals, d'évènements sportifs ou culturels…

Elle permet aux participants de payer leurs consommations durant tout l'évènement avec une monnaie dématérialisée. L'argent est sur un bracelet sans contact. Un exemple de bracelet et de stand de distribution est donné figure 1.

L'intérêt de ce principe réside dans l'absence d'échange monétaire ou d'encaissement à partir de carte bancaire en dehors des stands de recharge des bracelets.

Figure 1 : bracelet de paiement sans contact et stand de distribution

On retiendra les termes suivants :

- festivalier qui est un participant à un évènement ;
- bénévole qui est une personne intervenant sur un stand pour le compte du gestionnaire ;
- gestionnaire qui est la structure organisant l'évènement. Cette organisation se décline avant, pendant et après.

La société CISS et son système Cashless Online sont sollicités pour un festival à Lyon qui se déroulera du 3 au 6 septembre 2026.

2. Organisation d'un festival

L'organisation du festival est gérée par un site Internet offrant plusieurs fonctionnalités.

Les inscriptions des bénévoles se font via ce site.

Le gestionnaire utilise ce site pour définir le nombre de stands et leur type. Il affecte les bénévoles dans chaque stand. Ce fonctionnement est présenté figure 2.

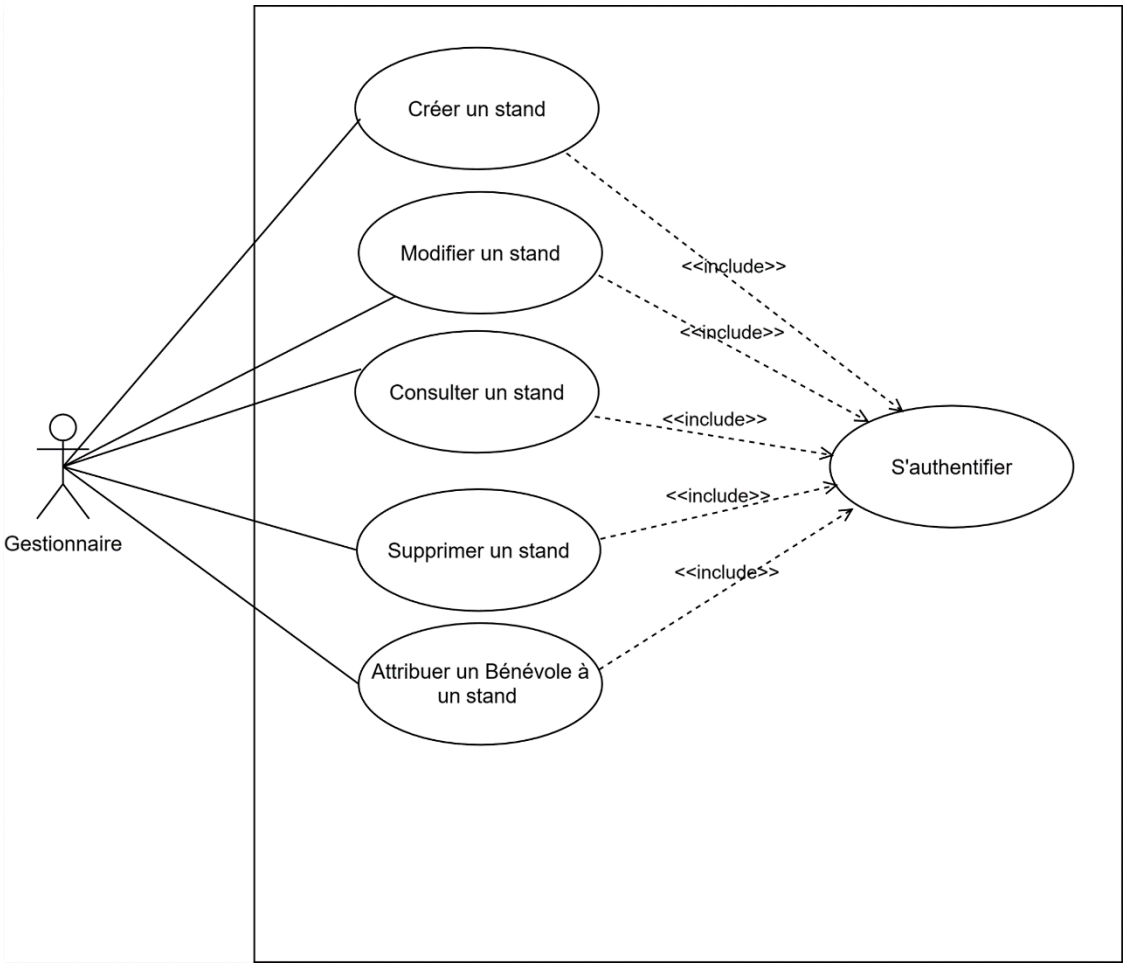


Figure 2 : administration du festival

Lors de la création du compte par le festivalier, il peut associer sa carte bancaire, définir son login et son mot de passe. Le bracelet du festivalier est associé à ce compte.

Une fois le bracelet associé au compte, le festivalier peut consulter le solde de son compte et ses achats.

Le jour de l'évènement, comme le représente la figure 3, le festivalier se voit remettre un bracelet et le crédite au stand de rechargement.

Figure 3 : ajout de crédit sur le bracelet

Ces bracelets sont l'unique moyen de paiement sur les stands de distribution. La figure 4 présente le paiement validé par le smartphone utilisé en tant que terminal Cashless.

Figure 4 : achat d'une boisson

3. La gestion du festival

Au festival, deux stands sont prévus pour assurer la recharge des bracelets et sept stands sont équipés de terminaux Cashless pour les achats. Les festivaliers y trouveront boissons et snacks.

Les emplacements des différents stands sont visibles sur la topologie du site illustrée en figure 5.

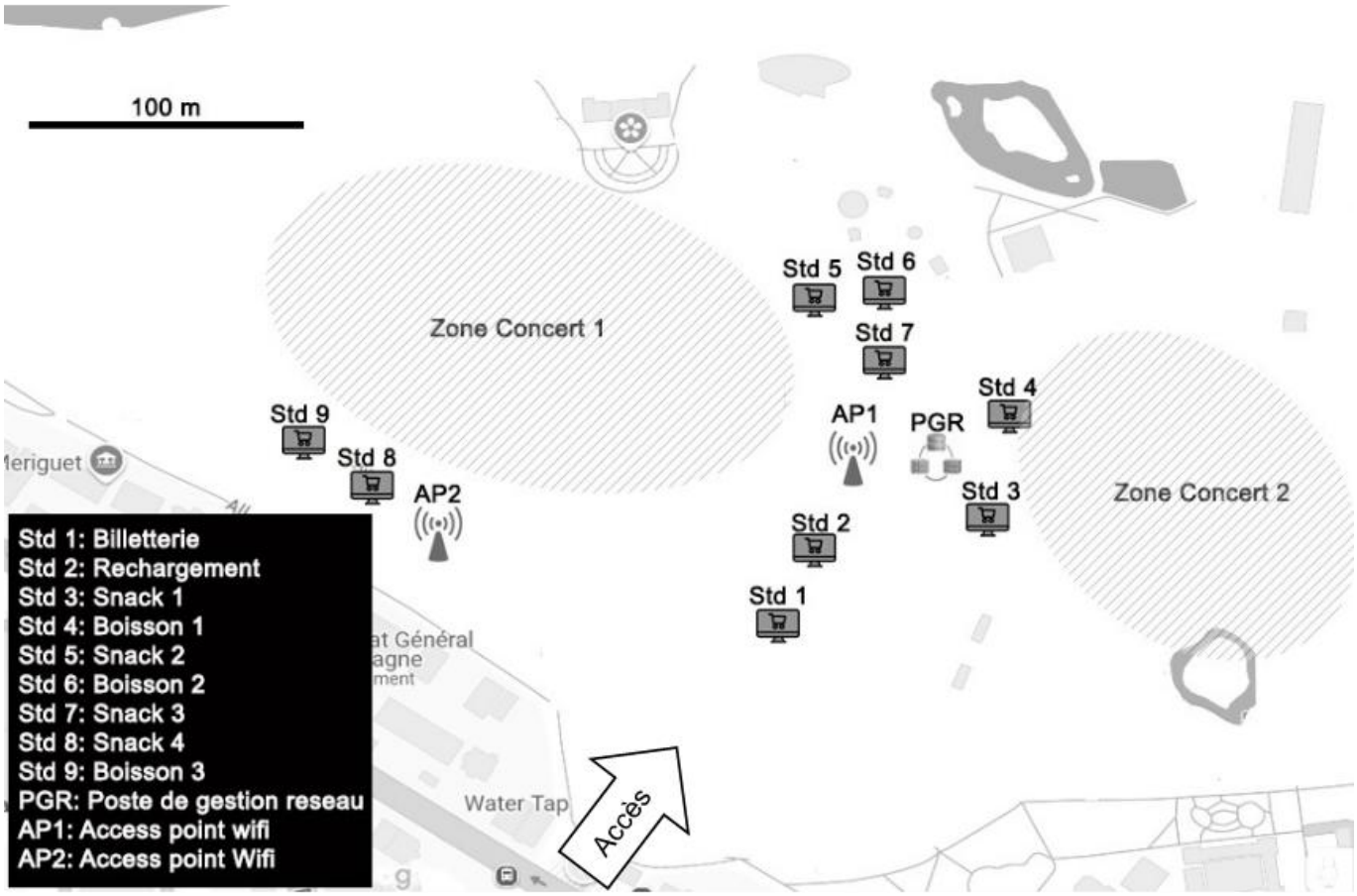


Figure 5 : topologie du festival

Les terminaux Cashless sont des smartphones dotés de la fonctionnalité NFC. Pour la suite du sujet, le terme terminal sera utilisé pour désigner ce téléphone portable.

L'App Mobile Cashless Online est installée sur chaque terminal. C'est une application qui échange avec le serveur d'APIs de Cashless Online.

Le diagramme de déploiement de la figure 6 donne le détail des divers composants de l'application Cashless Online.

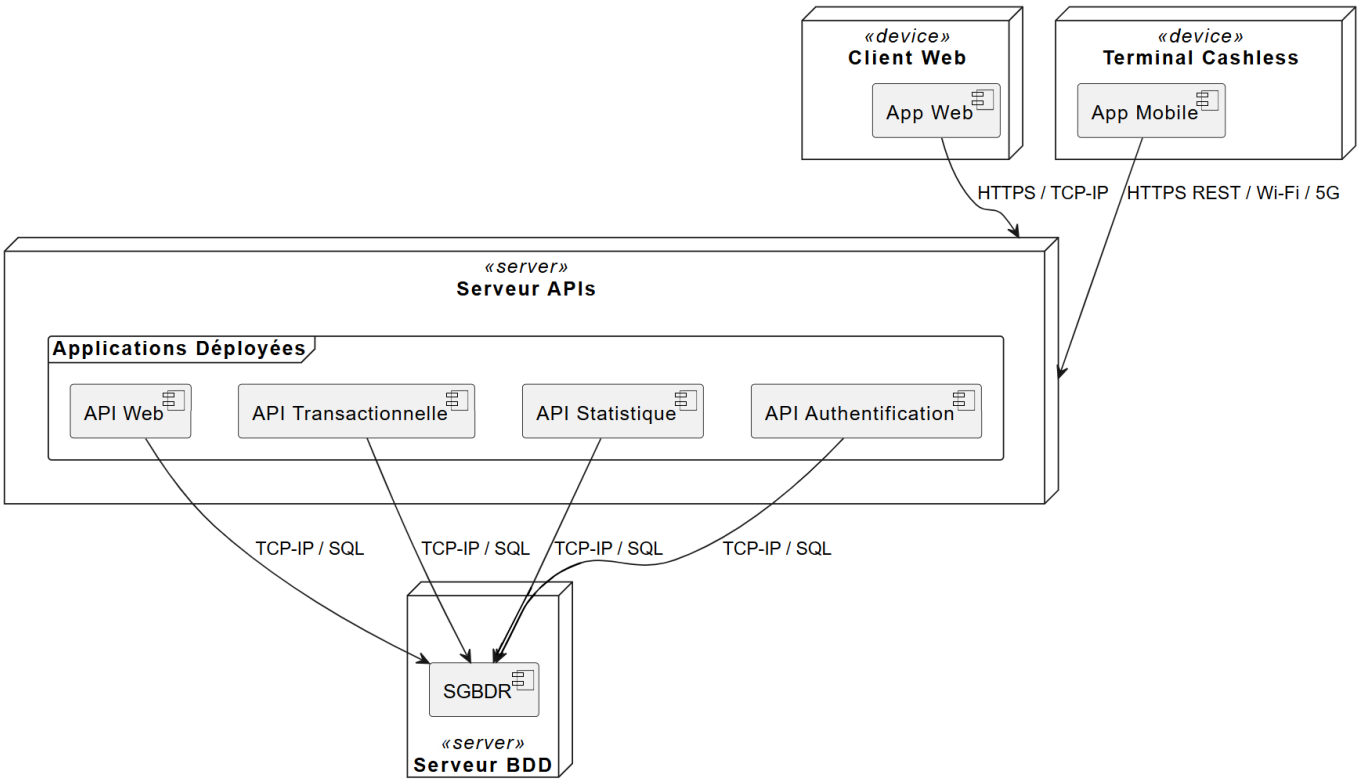


Figure 6 : diagramme de déploiement de la solution

4. Problématique

L'entreprise CISS a mené une enquête auprès de tous ses clients sur la satisfaction de son produit et des améliorations possibles.

Les gestionnaires soulignent souvent qu'à un moment du festival, un stand de distribution se retrouve saturé de festivaliers, au point que les bénévoles ne parviennent plus à suivre le rythme.

Il est difficile pour les gestionnaires de trouver plus de bénévoles pour tenir les stands de distribution. Ils aimeraient avoir une proposition pour résoudre ce problème.

L'entreprise CISS a développé un système de distribution de boisson automatique autonome.

Ce système est doté :

- d'une machine de tirage à boisson ;
- d'un terminal de paiement Cashless intégré.

Le festivalier se sert et règle sans l'intervention d'un bénévole. Le festivalier approche son bracelet du lecteur NFC du terminal. Le système vérifie alors auprès du serveur d'API que le crédit disponible est suffisant. Le festivalier choisit ensuite le volume de boisson souhaité. Le système contrôle automatiquement si la quantité restante le permet (en évaluant le poids du bac).

Si c’est le cas, il sert la boisson et débite le montant correspondant. Le synoptique de la figure 7 présente ces éléments. Pour la suite du sujet, le terme stand de service autonome est utilisé.

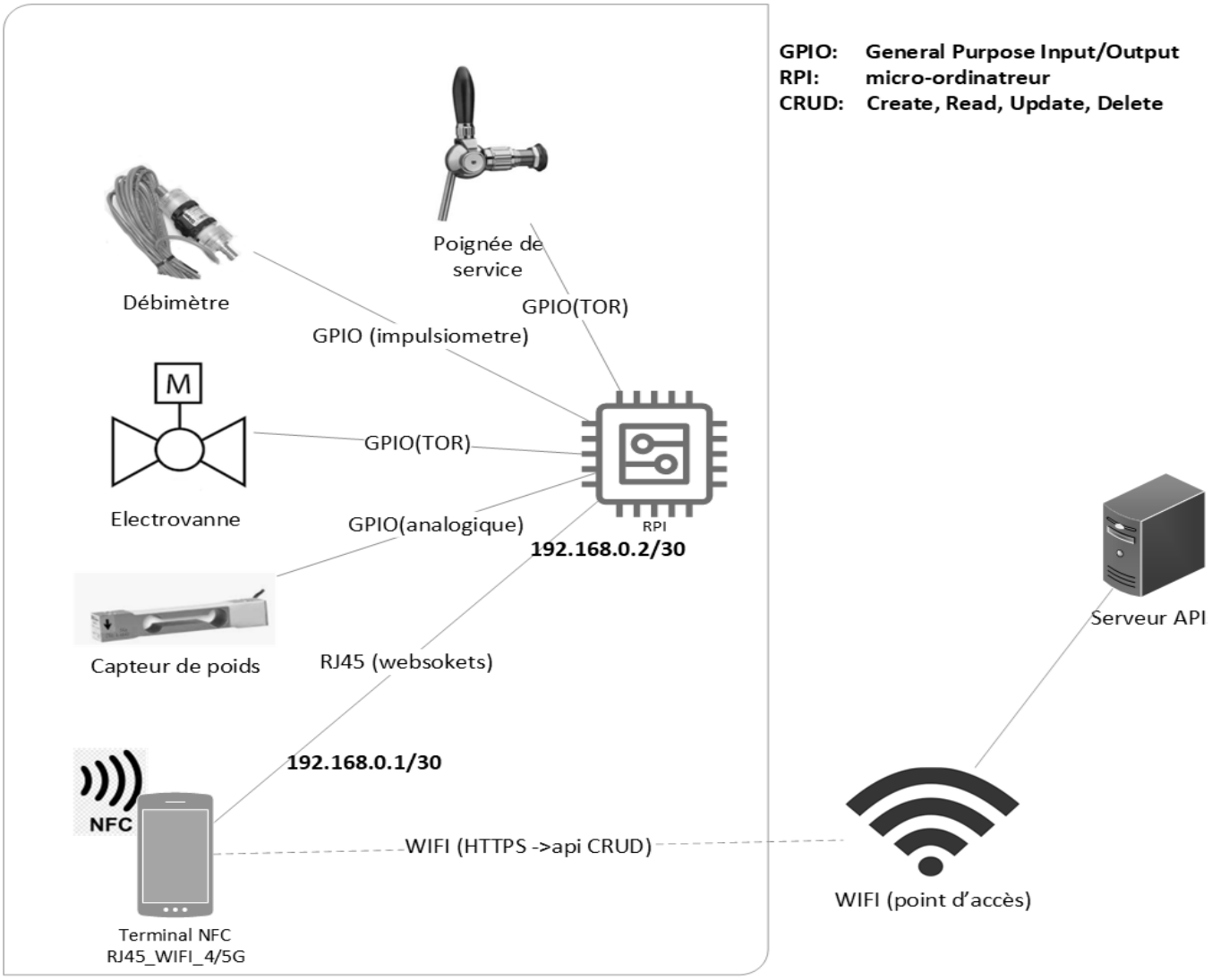


Figure 7 : synoptique d’un stand de service autonome

Avec l'ajout d'un stand de service autonome, l'intervention d'un technicien de la société est nécessaire pour installer et configurer le dispositif.

Un nouveau technicien découvre l'ensemble du système. Après une brève présentation faite par son responsable, il est invité à l'explorer d'abord en tant qu'utilisateur.

Dans un premier temps, il travaille sur l'ancienne version de CASHLESS Online, c'est-à-dire sans le stand autonome, et réalise différents tests pour en comprendre le fonctionnement et en acquérir la maîtrise.

Dans un second temps, il configure et intègre le stand de service autonome au système CASHLESS.

Son responsable lui fournit plusieurs éléments essentiels :

- l'architecture réseau de la figure 8 ;
- les tables de la base de données de la figure 9 ;
- des bracelets ;
- des terminaux.

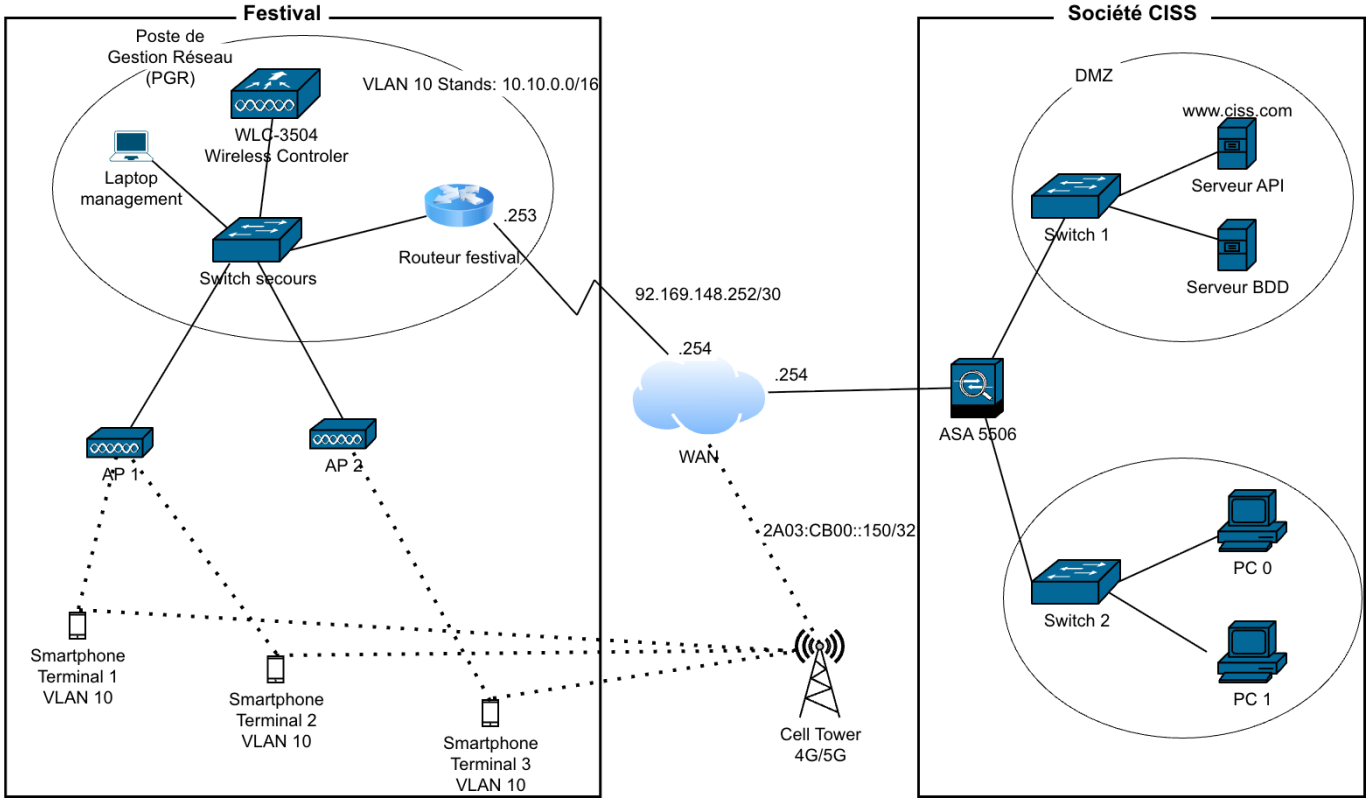


Figure 8 : architecture réseau du système

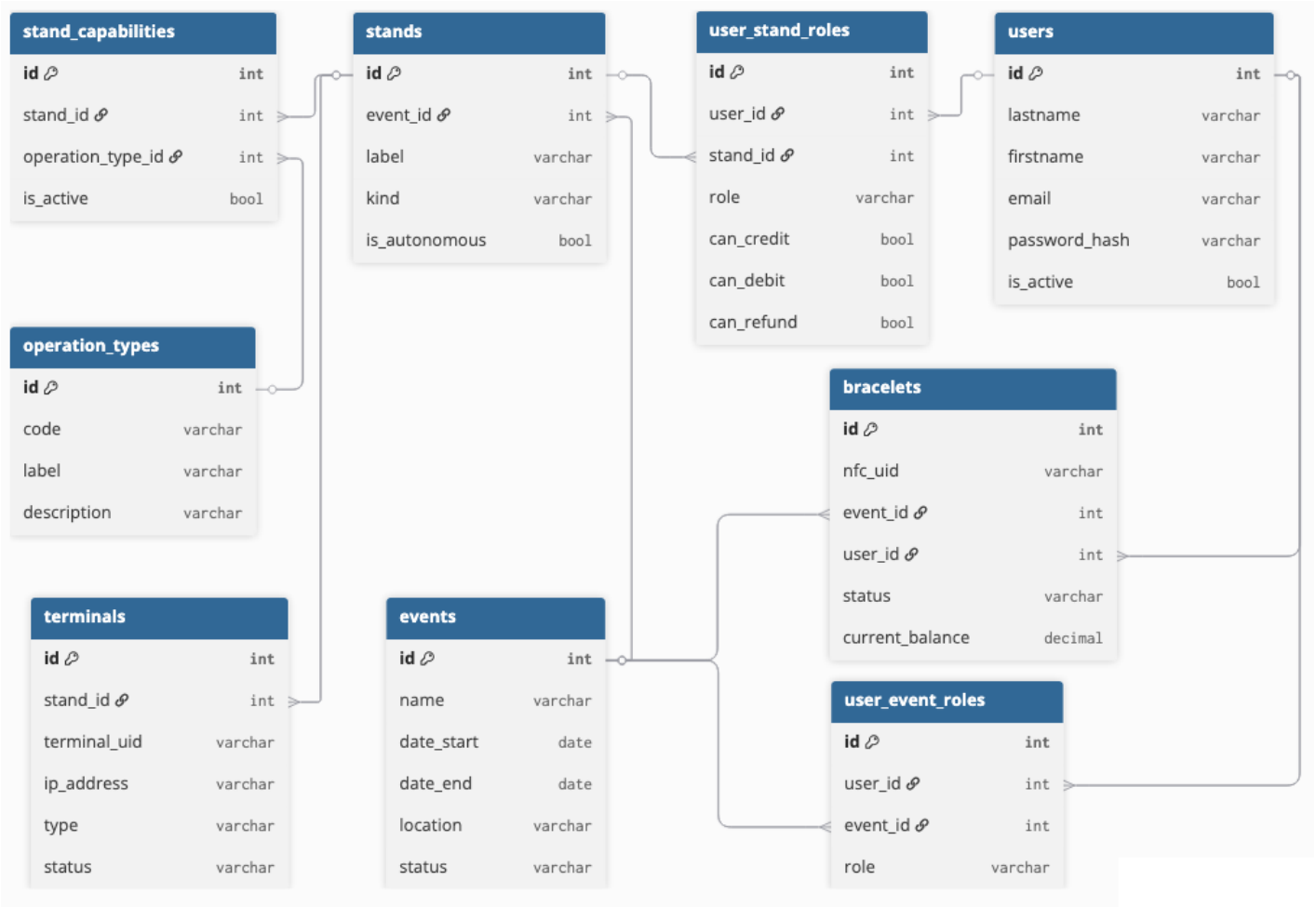


Figure 9 : schéma partiel des tables de la base de données

La table `users` regroupe toutes les personnes du système : organisateurs, bénévoles, techniciens ou administrateurs. Elle constitue la base centrale des comptes utilisateurs.

La table `events` stocke l'ensemble des évènements (festivals, soirées, salons). Chaque évènement possède ses propres stands, ses bracelets et ses rôles associés.

La table `stands` décrit les différents stands d'un évènement : stand de crédit, bar, restauration, stand autonome ou stand d'information. La colonne `kind` distingue leur type, et `is_autonomous` indique si le stand fonctionne sans opérateur humain.

La table `terminals` correspond au matériel utilisé sur les stands, comme les téléphones NFC ou les bornes fixes. On y retrouve notamment l'identifiant matériel `terminal_uid`, l'adresse IP pour la supervision du terminal `ip_address` et le stand auquel il est affecté `stand_id`.

La table `bracelets` représente les bracelets NFC. Chaque bracelet est lié à un évènement et à un festivalier. Le solde courant est stocké dans `current_balance` pour éviter des recalculs fréquents.

La table `operation_types` définit les types d'actions possibles : crédit, débit, remboursement ou consultation. Elle permet de faire évoluer facilement le système.

La table `stand_capabilities` précise les actions qu'un stand peut réaliser. Par exemple, un stand de crédit peut effectuer un crédit, un bar peut effectuer un débit, et un stand autonome peut cumuler plusieurs capacités selon sa configuration.

La table `user_event_roles` indique le rôle d'un utilisateur pour un évènement donné, comme organisateur, technicien ou superviseur.

Enfin, la table `user_stand_roles` décrit les rôles attribués à un utilisateur sur un stand précis. Elle gère aussi les droits opérationnels, comme la possibilité d'effectuer un crédit, un débit ou un remboursement. Cela permet de contrôler précisément qui peut faire quoi sur chaque stand.

Le sujet comporte les six parties indépendantes suivantes :

- partie 1, traitant de l'analyse de structures matérielles et logicielles ;
- partie 2, traitant de la conception de structures matérielles et logicielles ;
- partie 3, traitant la validation du choix du débitmètre ;
- partie 4, traitant la détection des fûts de boisson vides ;
- partie 5, traitant la caractérisation du protocole de communication NFC ;
- partie 6, traitant du choix des antennes.

SUJET

Option A Informatique et Réseaux

Domaine professionnel

Durée 4 h 30

Partie 1 - Analyse du système informatique

Le technicien crée un compte festivalier sur le site web. Il renseigne ses informations en indiquant entre autres son login et son mot de passe. Bien que ce ne soit pas obligatoire, il saisit les informations d'une carte bancaire, pour pouvoir faire un rechargement en ligne. Il analyse ses interactions avec le système.

Q1. **Compléter** sur le document réponse DR-Pro1 le diagramme des cas d'utilisation en spécifiant les relations entre les cas d'utilisation « Créer son Compte », « Ajouter sa carte bancaire », « Recharger son bracelet en ligne » et « S'authentifier ».

Le technicien clique sur le lien « consulter ses achats et le solde restant ». Le solde est de 0 €, aucune transaction n'a été effectuée.

Q2. **Compléter** le document réponse DR-Pro2 pour ajouter au diagramme « Consulter ses achats » et « Consulter le solde restant ». **Spécifier** les éventuelles liaisons avec les acteurs et les cas d'utilisation existants.

Q3. À partir de la figure 5 et 6 (document présentation du système), **compléter** le document réponse DR-Pro3 pour spécifier les liaisons entre les nœuds du système. **Préciser** les supports et les cardinalités.

Le terminal communique avec les bracelets grâce à un lecteur NFC présent et obligatoire sur le terminal.

Q4. Sur le document réponse DR-Pro4, **entourer** les avantages et les inconvénients pour chaque matériel informatique.

L'App Mobile communique avec l'API Transactionnelle. Le technicien se focalise sur l'architecture réseau du système et plus précisément sur la connexion entre les divers éléments informatiques.

Q5. Avec l'aide de la figure 8, **compléter** le document réponse DR-Pro5 en indiquant le protocole de la couche physique utilisé pour établir une communication entre les terminaux et le serveur d'APIs.

Q6. **Compléter** le document réponse DR-Pro6 en indiquant les protocoles de couche supérieure nécessaires entre les terminaux et le serveur d'APIs. **Préciser** le nom de la couche correspondante dans le modèle OSI.

Le diagramme partiel entités/relations de la base de données Cashless Online est présenté en figure 9.

Q7. **Indiquer** si un utilisateur peut avoir plusieurs bracelets, **justifier** la réponse.

Q8. Grâce à la documentation technique DT1**, rédiger** la création de la table `stands`.

Q9. **Donner** la requête SQL qui permet d'afficher la liste des adresses IP des terminaux affectés aux stands autonomes.

Sur la figure 8, un réseau 4/5G et un réseau Wi-Fi sont représentés. Il est indiqué que les terminaux utilisés lors de l'évènement peuvent fonctionner soit sur le réseau 4/5G, soit sur le réseau Wi-Fi. Il est également précisé que le réseau 4/5G du festival n'est pas maîtrisé par l'entreprise. Il faut donc s'assurer que le réseau Wi-Fi soit suffisamment performant.

La solution doit bénéficier d'une une sécurité renforcée. La solution Wi-Fi doit privilégier la bande des 5GHz. Il faut pouvoir centraliser la gestion des points d'accès. La solution doit permettre de répartir les connexions sur les différentes bornes pour éviter une surcharge de connexions.

Q10. À l'aide de la documentation technique DT2, **justifier** le choix du contrôleur WLC3504.

Une capture de trames réalisée avec Wireshark est étudiée. Cette capture est présentée dans la figure 10. Une trame Ethernet retient particulièrement l'attention du technicien, elle concerne une reprise de session et du TLS 1.3, protocole devant assurer la confidentialité des échanges avec le serveur. Les documents fournissent également le détail de certaines trames, notamment la trame n°4, reproduite dans la figure 11, et la trame n°6, présentée dans la figure 12.

No	Time	Source	Port src	Destination	Port dst	Protocol	Info
1	0.000000	51.159.173.20	49246	10.69.1.123	443	TCP	49246 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=62365468 TSecr=0
2	0.000051	10.69.1.123	443	51.159.173.203	49246	TCP	443 → 49246 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=121598498 TSecr=62365468
3	0.000123	51.159.173.20	49246	10.69.1.123	443	TCP	49246 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSval=62365468 TSecr=121598498
4	0.000210	51.159.173.20	49246	10.69.1.123	443	TLSv1.3	Client Hello
5	0.000402	10.69.1.123	443	51.159.173.203	49246	TCP	443 → 49246 [ACK] Seq=1 Ack=2855 Win=64128 Len=0 TSval=121598498 TSecr=62365468
6	0.000415	10.69.1.123	443	51.159.173.203	49246	TLSv1.3	Server Hello, Change Cipher Spec, Application Data
7	0.000562	51.159.173.20	49246	10.69.1.123	443	TLSv1.3	Change Cipher Spec
8	0.000703	51.159.173.20	49246	10.69.1.123	443	TLSv1.3	Application Data
9	0.000850	10.69.1.123	443	51.159.173.203	49246	TCP	443 → 49246 [ACK] Seq=2855 Ack=64128 Win=64128 Len=0 TSval=121598498 TSecr=62365473
10	0.000913	10.69.1.123	443	51.159.173.203	49246	TLSv1.3	Application Data
11	0.001054	51.159.173.20	49246	10.69.1.123	443	TCP	49246 → 443 [ACK] Seq=2855 Ack=64128 Win=64128 Len=0 TSval=62365468 TSecr=121598498
12	0.001132	51.159.173.20	49246	10.69.1.123	443	TLSv1.3	Application Data

Figure 10 : trames Wireshark de l'échange TLS Cashless

```
Frame 4: 2241 bytes on wire (17928 bits), 2241 bytes captured (17928
bits) …
Ethernet II, Src: HP_bb:d2:1f, Dst: Ubiquiti_43:1f:60
Internet Protocol Version 4, Src: 10.69.1.223, Dst: 51.159.173.103
Transmission Control Protocol, Src Port: 54926, Dst Port: 443, Seq: 1,
Ack: 1…
Transport Layer Security
    TLSv1.3 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 2170
        Handshake Protocol: Client Hello
            Handshake Type: Client Hello (1)
            Length: 2166
            Version: TLS 1.2 (0x0303)
            Random:
6afde7269528826859ef58ce931ca7939887bb0a7de9fbb4ccdfd839302e571d
            Session ID Length: 32
            Session ID:
7749b3bdefa5cc93e1402d4fda6ec8a35442436a715174223e9516b662b7852a
            Cipher Suites Length: 32
            Cipher Suites (16 suites)
            Compression Methods Length: 1
            Compression Methods (1 method)
            Extensions Length: 2061
            Extension: Reserved (GREASE) (len=0)
            Extension: encrypted_client_hello (len=282)
            Extension: signed_certificate_timestamp (len=0)
            Extension: psk_key_exchange_modes (len=2)
            Extension: key_share (len=1263) Unknown (4588), x25519
            Extension: ec_point_formats (len=2)
            Extension: session_ticket (len=0)
            Extension: extended_master_secret (len=0)
            Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
            Extension: status_request (len=5)
            Extension: compress_certificate (len=3)
            Extension: renegotiation_info (len=1)
            Extension: supported_groups (len=12)
            Extension: application_settings (len=5)
            Extension: application_layer_protocol_negotiation (len=14)
            Extension: server_name (len=39) name=desktop-api-
int.paiement.solutions
            Extension: signature_algorithms (len=18)
            Extension: Reserved (GREASE) (len=1)
            Extension: pre_shared_key (len=331)
```

Figure 11 : détails trame n° 4 de la figure 10

```
Frame 6: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits…
Ethernet II, Src: Ubiquiti_43:1f:60, Dst: HP_bb:d2:1f
Internet Protocol Version 4, Src: 51.159.173.103, Dst: 10.69.1.223
Transmission Control Protocol, Src Port: 443, Dst Port: 54926, Seq: 1,
Ack:…
Transport Layer Security
    TLSv1.3 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 128
        Handshake Protocol: Server Hello
            Handshake Type: Server Hello (2)
            Length: 124
            Version: TLS 1.2 (0x0303)
            Random:
fd0ea24311c55c5db0001981a03ee3d86061d0c59214800e4996aa90b1387f55
            Session ID Length: 32
            Session ID:
7749b3bdefa5cc93e1402d4fda6ec8a35442436a715174223e9516b662b7852a
            Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
            Compression Method: null (0)
            Extensions Length: 52
            Extension: supported_versions (len=2) TLS 1.3
            Extension: key_share (len=36) x25519
            Extension: pre_shared_key (len=2)
            [JA3S Fullstring: 771,4866,43-51-41]
            [JA3S: 2253c82f03b621c5144709b393fde2c9]
    TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher
Spec
    TLSv1.3 Record Layer: Application Data Protocol: Hypertext
Transfer Protocol
    TLSv1.3 Record Layer: Application Data Protocol: Hypertext
Transfer Protocol
```

Figure 12 : détails trame n° 6 de la figure 10

Q11. À l'aide des éléments fournis dans la documentation technique DT3, des figures 11 et 12, **démontrer** que les trames fournies figure 10 représentent bien un échange TLS v1.3 avec reprise PSK.

Q12. **Donner** la suite de chiffrement utilisée à partir de la trame de la figure 12 et de la documentation technique DT3. **Préciser** la fonction de hachage.

Q13. **Expliquer** quelle est la différence entre hachage et chiffrement.

Lors de la mise en place de chaque stand, il est nécessaire d'y affecter des terminaux. Ces terminaux permettent de réaliser les paiements.

Lors de l'installation de l'App Mobile Cashless Online sur le terminal, un numéro unique est défini. Il permet d'identifier de manière unique chaque terminal grâce à son numéro de série : Android UID.

Une fois l'installation faite, chaque terminal s'initialise et se configure auprès du serveur d'API de la société CISS. Pour cela chaque terminal échange un certain nombre d'informations avec le serveur.

Plusieurs échanges initiés par le terminal vers le serveur d'API de la société CISS sont présentés ci-dessous.

Échange 1 : requête en POST envoyée par un terminal (client) vers le serveur d'API.

```
http://ciss.fr/cashlessonline/tpe/init/

{"Initialization":{"Stand":8, "License":"542",
"Row":"001","SerialNumber":"9dbca32c-b3f2-4844-9372-39069f3acfcc"}}
```

Q14. **Indiquer** le nom du domaine du site internet.

Q15. **Donner** les méthodes HTTP possibles pour transmettre les informations dans une API REST.

Q16. **Donner** au moins une information qui a été envoyée dans le body.

Q17. **Indiquer** quel est le nom du point de vente concerné par cette requête.

Q18. **Indiquer** à quoi correspond `SerialNumber`.

Réponse du serveur d'API

```
HTTP/1.1 200 OK

{
 "OK": 1,
 "Msg": "OK",
 "UserId": 11,
 "APIKey": "9dbca473-ae33-4f55-95d7-8123675a3741",
 "Display": " SUCCES\n Initialisation\n terminee\n"
}
```

Q19. **Indiquer** le rôle du chiffre 200.

Q20. **Indiquer** à quoi correspond la valeur de l'`APIKey` de la réponse présentée.

La société CISS gère plusieurs festivals et chaque festival comporte plusieurs stands. Les messages suivants sont échangés par le stand d'un même festival.

Échange 2 : requête en GET envoyée par un terminal (client) vers le serveur d'API

```
http://ciss.fr/cashlessonline/tpe/sessionjs/11/1733296780821/ab9d5a980
f3554cbff724237ebeceb2ee479b6a9157d5501d0d33cd9bc7b274eb33de029225554c
b792f8ae84715438d5eab6906e078db24bd7d36a4a3ff3338?NumSerie=9dbca32c-
b3f2-4844-9372-39069f3acfcc%40myterminal-
desktop&AppVersion=myTerminal%404.15.1 HTTP/1.1
```

Q21. Le numéro 1733296780821 est un `timeStamp`, **définir** ce terme.

Réponse du serveur d'APIs

```
HTTP/1.1 200 OK

{
   "OK": 1,
   "Msg": "OK",
   "Session": "9dbca4f9-bb0d-487f-b3e2-bc99d07326c7",
   "Code": "200"
 }
```

L'attribut Session correspond au token de session.

Q22. **Donner** le rôle d'une session sur un serveur web.

Échange 3 : requête en POST envoyée par un terminal (client) vers le serveur d'API

```
http://ciss.fr/cashlessonline/tpe/teleparametrage/WEB002/800792
```

```
{"RemoteConfiguration":{"SerialNumber":"9dbca32c-3f2-4844-9372-
39069f3acfcc"}}
```

Réponse du serveur

```
HTTP/1.1 200 OK
```

```
     {
        "OK": 1,
        "Msg": "OK",
        "HeaderOffline": "Caisse 2",
        "WebSite": "ciss.fr",
        "CallTime": "2235",
        "Currency": {
          "Name": "Euro",
          "Symbol": "€",
          "Decimals": 2
       },
       "Stand": {//info point de vente
       "Label": "Caisse 2",   "Url": null,
       "Location": {
          "AddressLine1": "Fête de la coquille St-Jacques",
          "PostalCode": "38250",
          "City": "Villard-de-Lans",
          "Country": "France"
        }
     }
```

Le schéma des tables de la base de données est donné par la figure 9.

Q23. L'échange 3 correspond à la lecture de la configuration enregistrée dans la base pour un terminal. **Donner** le nom des tables utilisées par le serveur pour générer cette réponse.

Le festival est programmé du 03/09/2026 au 06/09/2026 à Lyon.

Q24. À l'aide de la documentation technique DT1**, donner** la requête SQL permettant d'ajouter dans la table `events` le festival avec le statut `"programmé"`. La clé primaire est auto-incrémentée.

Q25. À l'aide de la documentation technique DT1, **donner** la requête SQL permettant de récupérer la valeur de la clé primaire du festival dont le statut est `"programmé"`.

Le terminal actuellement affecté à la « Fête de la coquille St-Jacques », doit être affecté au festival.

Q26. **Donner** le champ ou l'attribut à mettre à jour dans la base pour affecter ce terminal au stand snack 3 du festival.

Partie 2 – Conception d'un système informatique

À ce stade, le technicien maîtrise pleinement le système Cashless Online. L'ensemble des fonctionnalités est compris et le travail se concentre désormais sur le stand de service autonome.

Le synoptique du stand de service autonome est présenté dans la figure 7.

La fabrication d'une grande partie du système a été sous-traitée à une entreprise selon un cahier des charges, à l'exception du terminal, choisi par CISS.

Le terminal utilisé dans le stand de service autonome est équipé :

- d'un lecteur NFC ;
- d'un port RJ45 ;
- d'un port Wi-Fi ;
- d'un accès data 4/5G.

Ce terminal est géré par la société CISS, tout comme la partie logicielle, développée et installée par cette dernière.

Le premier modèle de stand de service autonome est livré par l'entreprise sous-traitante. C'est ce modèle qui est installé au festival.

La conformité du matériel doit être validée, le terminal doit être ajouté, et l'ensemble des tests d'intégration doit être réalisé.

La partie réseau du stand de service autonome doit être configurée et validée afin d'assurer la communication avec le terminal et l'intégration complète dans le système actuel.

L'architecture réseau est présentée figure 8.

Q27. À l'aide de la documentation technique DT4 du pare feu ASA5506, **indiquer** quelles fonctionnalités le système utilise pour créer une zone DMZ.

Les éléments de configuration de l'ASA5506 sont présentés ci-dessous.

```
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address 96.31.56.253 255.255.255.252
 !
 interface GigabitEthernet1/2
  nameif dmz1
  security-level 50
  ip address 192.168.1.1 255.255.255.0
 !
 interface GigabitEthernet1/3
  nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0
```

Q28. Sur le document réponse DR-Pro7, à l'aide des informations ci-dessus, **compléter** les configurations des interfaces de l'ASA. En **déduire** les adresses et les masques des réseaux correspondants.

Il est demandé au technicien de modifier, pour cet événement, la stratégie du contrôleur Wi-Fi WLC-3504 selon les spécifications suivantes :

- au moins trois sous-réseaux différents (VLAN 10, VLAN 20, VLAN 99) doivent être définis ;
- pour des raisons de sécurité, le nombre de machines dans chaque sous-réseau doit être limité à 30, le terme machine incluant l'ensemble des terminaux ainsi que la passerelle par défaut ;
- le réseau 192.168.69.0/24 est découpé en sous-réseaux ;
- pour les VLAN 10 et VLAN 20, les deux premiers sous-réseaux possibles sont retenus ;
- pour le VLAN 99, le dernier sous-réseau possible est retenu ;
- la stratégie DHCP est appliquée de manière similaire à tous les sous-réseaux : l'intégralité des adresses est rendue disponible, à l'exception de la dernière, réservée pour la passerelle par défaut.

Q29. **Proposer** une segmentation en sous-réseau en tenant compte des contraintes ci-dessus. **Compléter** le document réponse DR-Pro8.

Dans le cadre de la politique de cybersécurité de la société CISS, le technicien procède à une cartographie des mécanismes de sécurité mis en place, en les corrélant aux couches du modèle OSI, afin d'évaluer leur couverture fonctionnelle et d'identifier d'éventuelles lacunes de protection.

Q30. **Compléter** le document réponse DR-Pro9 en positionnant SSID, HTTPS, sous-réseau, VLAN.

Q31. À l'aide de la topologie du système présentée figure 5, **déterminer** la distance entre AP2 et PGR. En **déduire**, à l'aide de la documentation technique DT5, la ou les technologies possibles pour établir une liaison directe.

Pour améliorer les échanges du système et la montée en puissance des stands de service autonome, il faut que le technicien propose un devis pour utiliser la fibre optique.

Q32. À l'aide de la documentation technique DT6 et de la figure 8**, compléter** sur le document-réponse DR-Pro10 le tableau du coût financier de la partie étudiée afin d'obtenir la solution la plus économique qui répond aux contraintes énoncées.

Pour le festival, un stand de service autonome avec une seule ligne de service de boisson est mis en service.

Le MLD de la base de données concernant les lignes autonomes est présenté figure 13.

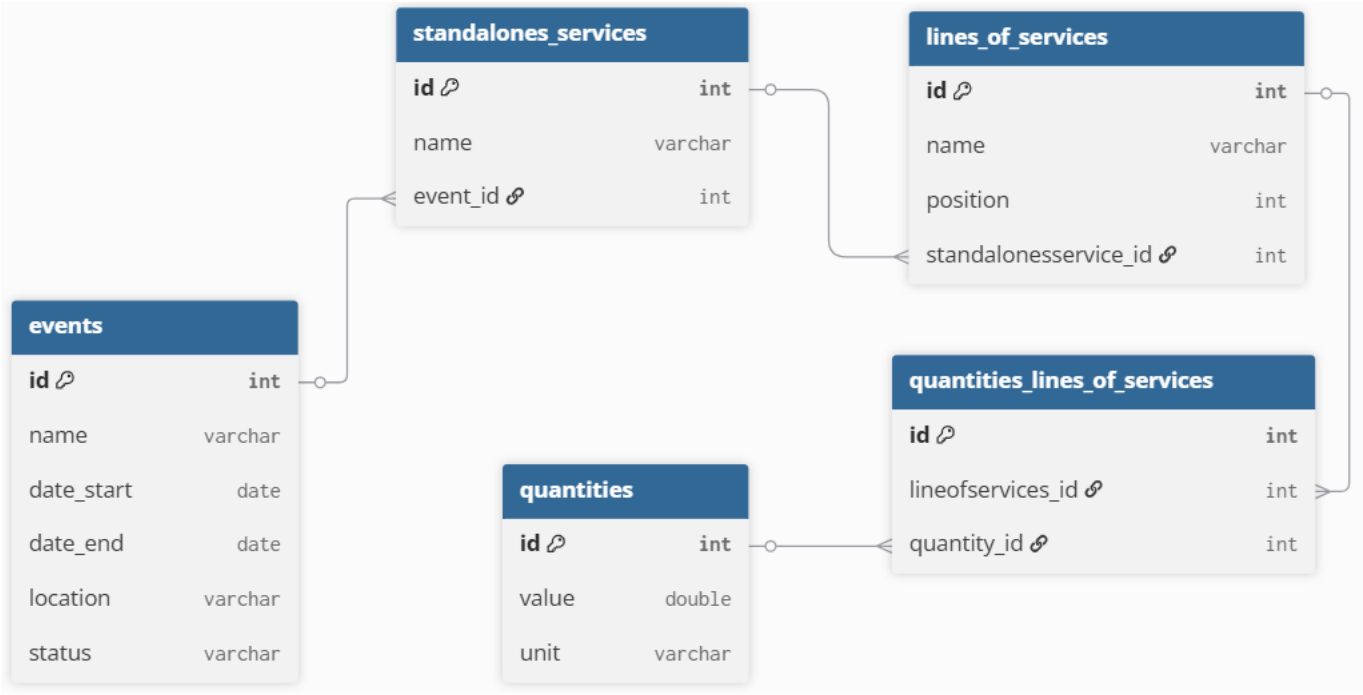


Figure 13 : schéma partiel des tables du stand de service autonome

Q33. À l'aide de la documentation technique DT1**, écrire** la ou les requêtes SQL permettant d'insérer les quantités de 25 cL, 33 cL et 50 cL dans la table `quantities` de la figure 13. La clé primaire est auto-incrémentée.

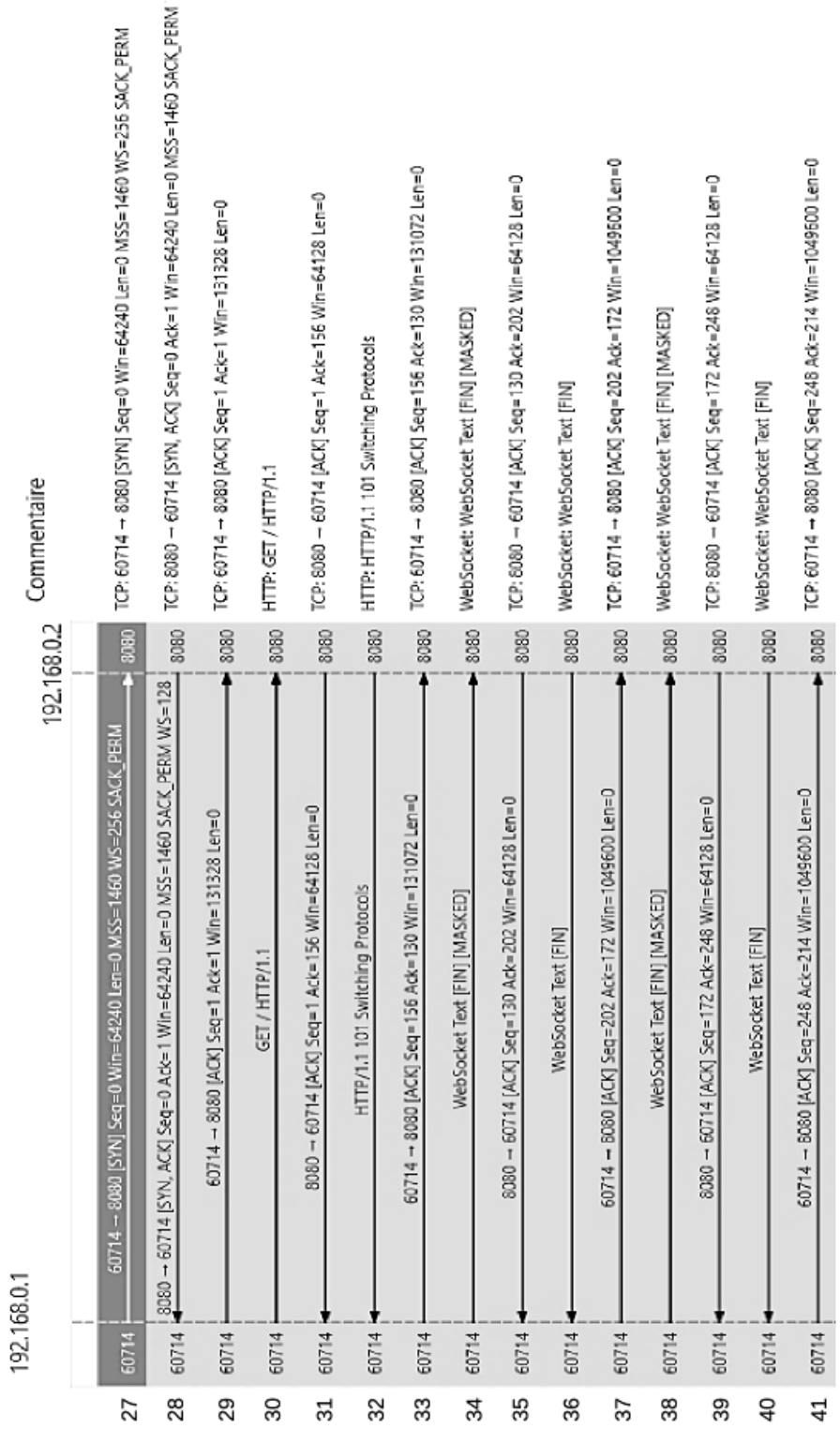


Figure 14 : échanges réseaux

Une adresse IP est fixée sur le terminal. Le terminal a le rôle de client. Il communique avec le serveur RPI du stand autonome, l'échange entre ces équipements est présenté figure 14.

Q34. À l'aide de la figure 14, **compléter** le tableau sur le document réponse DR-Pro11**.**

Q35. À l'aide de la figure 14, **compléter** le document réponse DR-Pro12 et **identifier** les numéros des lignes pour :

- la phase de connexion de TCP ;
- le changement de protocole HTTP $\rightarrow$ WS ;
- un acquittement TCP du serveur RPI ;
- un acquittement TCP du client terminal.

Trame web Socket émise par le client :

```
81 a8 1d aa c3 26 66 88 b5 49 71 df ae 43 42 c9
af 04 27 9f f3 0a 3f ce b6 54 78 cf 9c 42 74 d9
b7 54 74 c8 b6 52 74 c5 ad 04 27 9c f3 5b
```

Q36. Le principe du masking websocket de la RFC6455 est présenté dans la documentation technique DT7. La valeur du volume demandé est représentée par les 14^{éme} et le 15^{éme} octets du payload. **Donner** le masque. **Donner** la valeur du volume, rappel `0x30` en ASCII correspond au caractère '0'.

Il a été indiqué par le responsable qu'il est impératif de valider la durée de remplissage. À partir du moment où la carte est passée sur le lecteur et où la commande est validée, le festivalier est servi de manière autonome.

Un analyseur de trames Wireshark a été connecté au stand de service autonome. Wireshark a été lancé afin d'enregistrer les trames entre le terminal et le RPI. Une commande de boisson a ensuite été effectuée, comme par un festivalier.

La figure 15 présente la trace Wireshark obtenue. Le débit du distributeur du stand de service autonome de boissons doit permettre aux utilisateurs de remplir leur verre en moins de 11 secondes pour un verre de 25 cL.

Q37. En analysant la trame de la figure 15 ci-dessous, **démontrer** que la durée maximale de remplissage fixée dans le cahier des charges est bien respectée.

No	Time	Source	Port src	Destination	Port dst	Protocol	Info
10	7.568815	192.168.0.1	60714	192.168.0.2	8080	TCP	60714 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
11	7.569070	192.168.0.2	8080	192.168.0.1	60714	TCP	8080 → 60714 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
12	7.569108	192.168.0.1	60714	192.168.0.2	8080	TCP	60714 → 8080 [ACK] Seq=1 Ack=1 Win=131328 Len=0
13	7.593151	192.168.0.1	60714	192.168.0.2	8080	HTTP	GET / HTTP/1.1
14	7.593347	192.168.0.2	8080	192.168.0.1	60714	TCP	8080 → 60714 [ACK] Seq=1 Ack=156 Win=64128 Len=0
15	7.797334	192.168.0.2	8080	192.168.0.1	60714	HTTP	HTTP/1.1 101 Switching Protocols
16	7.851907	192.168.0.1	60714	192.168.0.2	8080	TCP	60714 → 8080 [ACK] Seq=156 Ack=130 Win=131072 Len=0
17	10.8429	192.168.0.1	60714	192.168.0.2	8080	WebSocket	WebSocket Text [FIN] [MASKED] **{"volume_cL":25,"distribution_duration":30}**
18	10.8431	192.168.0.2	8080	192.168.0.1	60714	TCP	8080 → 60714 [ACK] Seq=130 Ack=202 Win=64128 Len=0
19	17.3985	192.168.0.2	8080	192.168.0.1	60714	WebSocket	WebSocket Text [FIN] **{"status_code":1,"distributed_volume":100}**
20	17.4524	192.168.0.1	60714	192.168.0.2	8080	TCP	60714 → 8080 [ACK] Seq=202 Ack=172 Win=104960 Len=0
36	70.8583	192.168.0.1	60714	192.168.0.2	8080	WebSocket	WebSocket Text [FIN] [MASKED] **{"volume_cL":25,"distributed_volume":30}**
37	70.8586	192.168.0.2	8080	192.168.0.1	60714	TCP	8080 → 60714 [ACK] Seq=172 Ack=248 Win=64128 Len=0
45	77.3635	192.168.0.2	8080	192.168.0.1	60714	WebSocket	WebSocket Text [FIN] **{"status_code":1,"distributed_volume":100}**
46	77.4065	192.168.0.1	60714	192.168.0.2	8080	TCP	60714 → 8080 [ACK] Seq=248 Ack=214 Win=104960 Len=0

Figure 15 : capture Wireshark

Le débitmètre génère une impulsion tous les 2,5 mL. La figure 16 montre le taux de réussite du comptage des impulsions. Le verre de 25 cL doit être rempli en moins de 11 s.

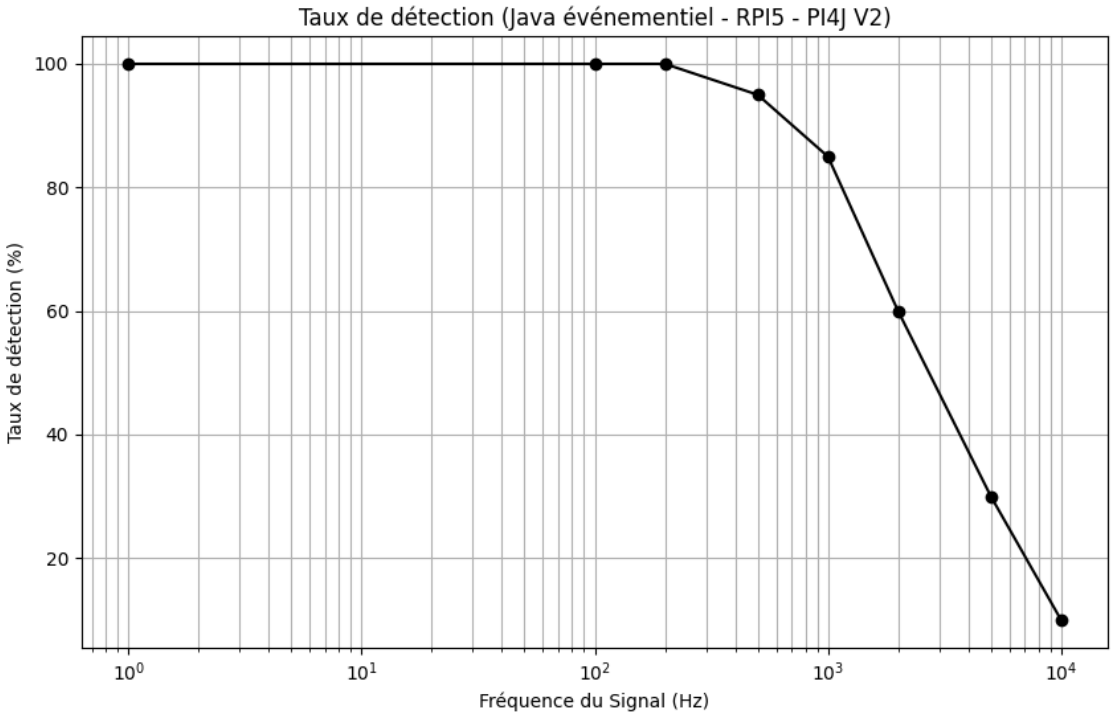


Figure 16 : taux de réussite du comptage des impulsions

Q38. **Calculer** le nombre d'impulsions générées pour un verre de 25cL. Grâce à la figure 16, **démontrer** que les performances permettent de rester en dessous de la durée maximale pour une durée de 11 s.

Q39. À partir de la figure 16, **calculer** la durée minimale pour le remplissage d'un verre de 50 cL avec un taux de traitement de 100 %.

Le diagramme de classe de l'application est présenté figure 17.

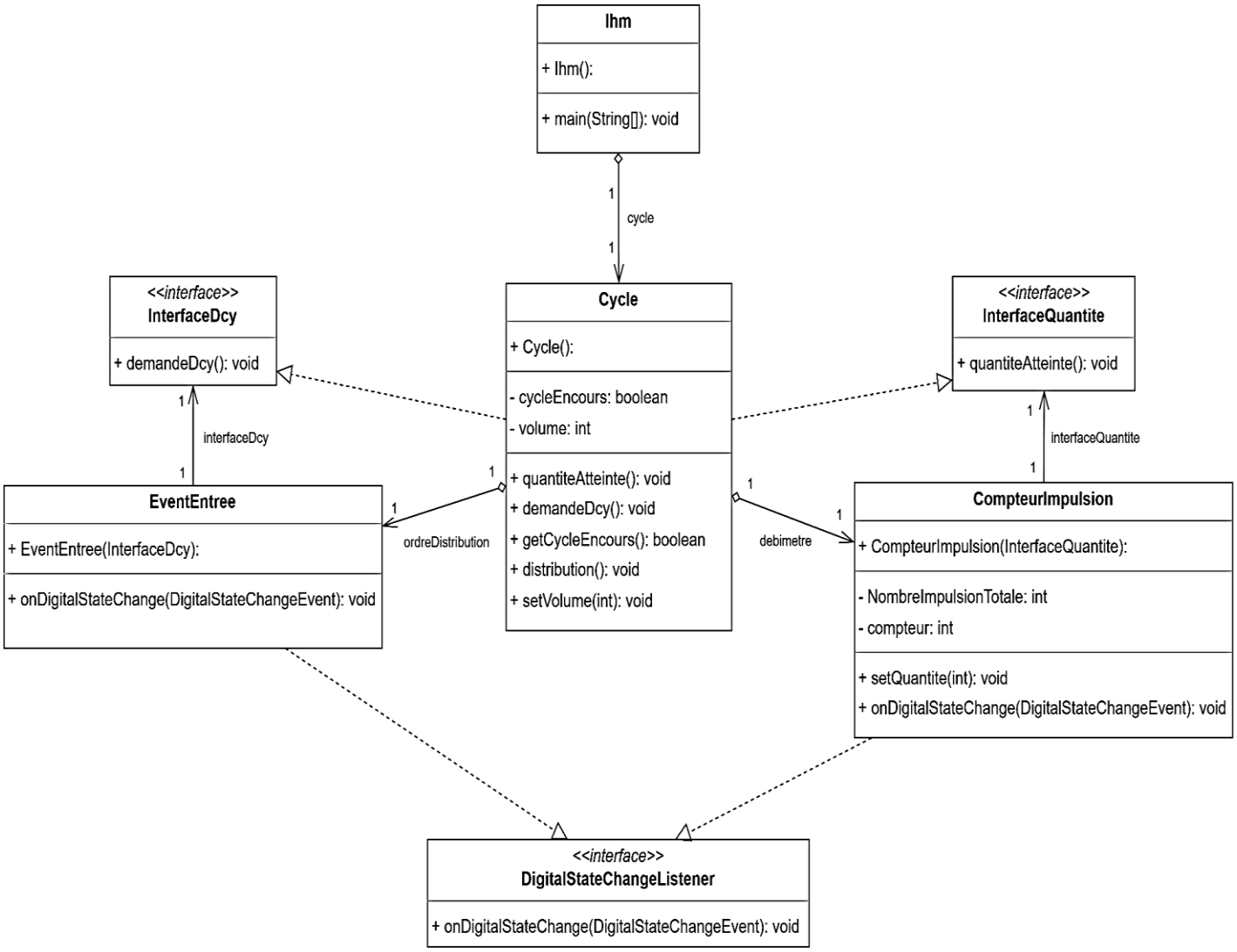


Figure 17 : diagramme partiel de classes

Q40. **Donner** la méthode de la classe `Cycle` qui émet une demande de cycle (dcy). **Préciser** si la classe `Ihm` y a accès, **justifier**.

Q41. **Préciser** si la classe `Ihm` a accès à l'attribut `compteur` de la classe `compteurImpulsion`, **justifier**.

Le diagramme ci-dessous de la figure 18 définit les deux classes qui vont permettre de faire des tests unitaires. Le contenu des classes est simplifié.

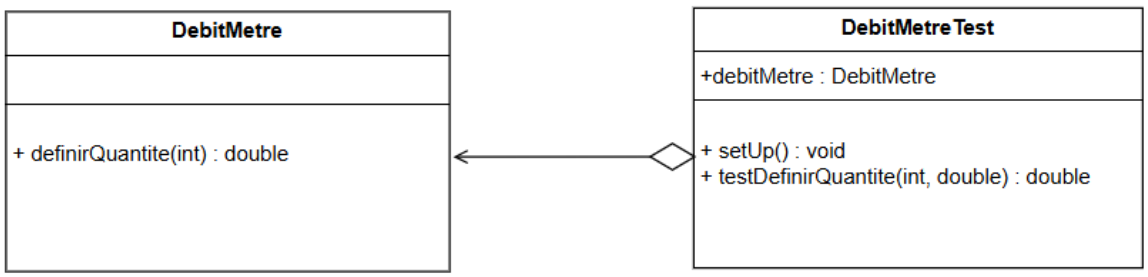


Figure 18 : diagramme partiel de classes

Pour rédiger les tests unitaires le format d'écriture utilisé est dans la documentation technique DT8.

Pour délivrer une quantité de boisson il faut définir un nombre d'impulsions à recevoir du débitmètre.

La classe `DebitMetre` possède une méthode : `definirQuantite(nb_impulsions)` qui, en fonction du nombre d'impulsions attendues, retourne une quantité de boisson en millilitre.

La classe `DebimetreTest` possède une méthode : `testDefinirQuantite(nb_impulsions, volume_cL )` qui teste la classe `DebitMetre`.

Le système délivre 25 cL, 33 cL ou 50 cL. Le nombre d'impulsions est de 100 pour 25 cL, 140 pour 33 cL et 200 pour 50 cL.

Le technicien fait un premier test, il saisit un nombre d'impulsions de 100. La méthode retourne une quantité de boisson de 250 mL, il saisit un nombre d'impulsions de 144 pour une quantité de boisson de 33 cL. La méthode lui retourne une quantité de boisson de 360 mL.

Q42. Sur le document réponse DR-Pro13, **compléter** les résultats des tests unitaires qui ont été effectués en utilisant la documentation technique DT8.

L'application Cashless fait l'objet d'une attaque informatique depuis un stand autonome et un accès frauduleux par injection SQL a été constaté sur la table `user_event_roles` exclusivement.

L'article 34 de la réglementation générale sur la protection des données personnelles (RGPD) impose la communication à la personne concernée d'une violation de ses données à caractère personnel.

Q43. Dans le cadre de cette compromission, à l'aide de la documentation technique DT9 et de la figure 9, **préciser** si la société CISS est tenue de communiquer auprès de l'ensemble des festivaliers et des bénévoles afin de les alerter. **Justifier** la réponse.

SUJET

Option A – Informatique et Réseaux

Domaine de la physique

Durée 1 h 30

Le sujet est composé de 4 parties indépendantes.

- Partie 3 : validation du choix du débitmètre.
- Partie 4 : détection des fûts de boisson vides.
- Partie 5 : caractérisation du protocole de communication NFC.
- Partie 6 : choix des antennes.

Présentation

Le responsable d'un festival à Lyon envoie un technicien supérieur afin de vérifier le choix et le bon dimensionnement de différents organes permettant le fonctionnement d'un débit de boisson automatisé (stand de service autonome).

Pour cela, le technicien supérieur est en charge de :

- vérifier le débitmètre à impulsions ;
- vérifier le capteur de force permettant de déterminer la masse des fûts de boisson afin de donner l'alerte pour un fût vide ;
- vérifier la transmission de données entre le lecteur et le tag NFC ;
- choisir les antennes permettant la collecte des données du lecteur NFC.

Partie 3 – Validation du choix du débitmètre

L'objectif de cette partie est de valider si les capacités de mesure du débitmètre OF-10 ZZT répondent aux contraintes.

Pour cela, les chronogrammes de fonctionnement du débitmètre, ainsi qu'un extrait de sa documentation, seront donnés au cours du questionnement.

Le débit de boisson automatisé possède un débitmètre à impulsions permettant d'ouvrir et fermer une électrovanne afin de remplir un verre de boisson. Le nombre d'impulsions est traité informatiquement.

Le technicien supérieur est en charge de vérifier les deux points suivants du débitmètre :

- le débitmètre doit être capable de mesurer le débit maximum de la boisson, qui est proche de 300 litres par heure, soit 300 000 cm^3 par heure ;
- un verre de boisson de 0,25 litre, soit 250 cm^3, doit être rempli en moins de 11 secondes.

Le débitmètre utilisé étant le OF-10 ZZT, celui-ci génère en sortie des impulsions ; celles-ci ont été enregistrées en fonction du temps par le technicien supérieur, sur la figure 19, pour un débit maximum.

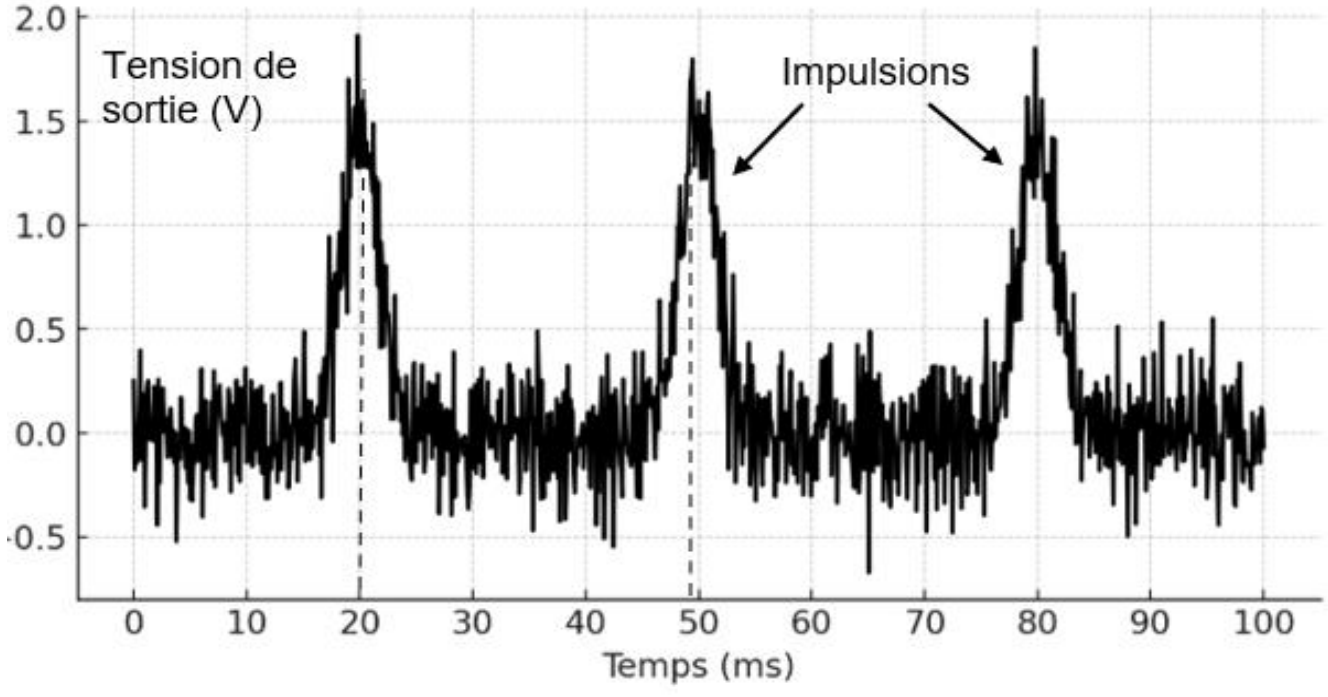


Figure 19 – Impulsions en sortie du débitmètre en fonction du temps pour le débit maximum

Q44. **Déterminer** la durée entre deux impulsions, notée ΔT_{min}, à la sortie du débitmètre.

Q45. **Calculer** le nombre d'impulsions en une heure, noté N_{I1}, dans le cas où le temps entre deux impulsions correspond à ΔT_{min}.

Une partie de la notice du débitmètre est donnée sur la figure 20.

Type	OF-05 ZAT-AO	OF-05 ZZT-AO	OF-10 ZAT-AO	OF-10 ZZT-AO
Code	782 105	782 205	782 110	782 210
Fluide	Kérosène Huile Gasoil	Eau Acides faibles Bases, solvants	Kérosène Huile Gasoil	Eau Acides faibles Bases, solvants
% E.M.	Précision ±2% de l'étendue de mesure, (±1 % : S/Dde)			
P /bar	5 bar maxi			
T°C	-10...+65 °C (T°C ambiante)			
Plages	0,3...0,8 cPo 0,8...2,0 cPo 2,0...5,0 cPo 5,0...200 cPo	5,0...50 l/h 3,0...50 l/h 1,0...50 l/h 0,5...50 l/h	0,3...0,8 cPo 0,8...2,0 cPo 2,0...5,0 cPo 5,0...200 cPo	40...300 l/h 20...300 l/h 15...300 l/h 10...300 l/h
Volume	0,46 cm^3 / impulsion		2,5 cm^3 / impulsion	
Tension	Alimentation 3...12 V DC			
Sortie	impulsions carrées /sortie tension			
R	Raccords filetés ¼" G		Raccords filetés ½" G	
Boîtier Rotor Joints Axe	Résine PPS NBR Inox 304	Résine PPS FPM SiC	Résine PPS NBR Inox 304	Résine PPS FPM SiC

Figure 20 – Notice de débitmètres

Q46. **Calculer**, en utilisant le résultat de la question Q45., le débit maximum que peut mesurer le débitmètre OF-10ZZT, noté D_{max}, exprimé en cm^3 par heure (figure 20).

Q47. **Calculer**, en utilisant la figure 20, le nombre d'impulsions, noté N_{I2}, nécessaires en sortie du débitmètre OF-10 ZZT afin de remplir un verre de 0,25 litre, soit 250 cm^3.

Cette fois, le technicien supérieur fait un relevé temporel (figure 21) dans les conditions les plus défavorables correspondant au débit minimal en sortie du débitmètre.

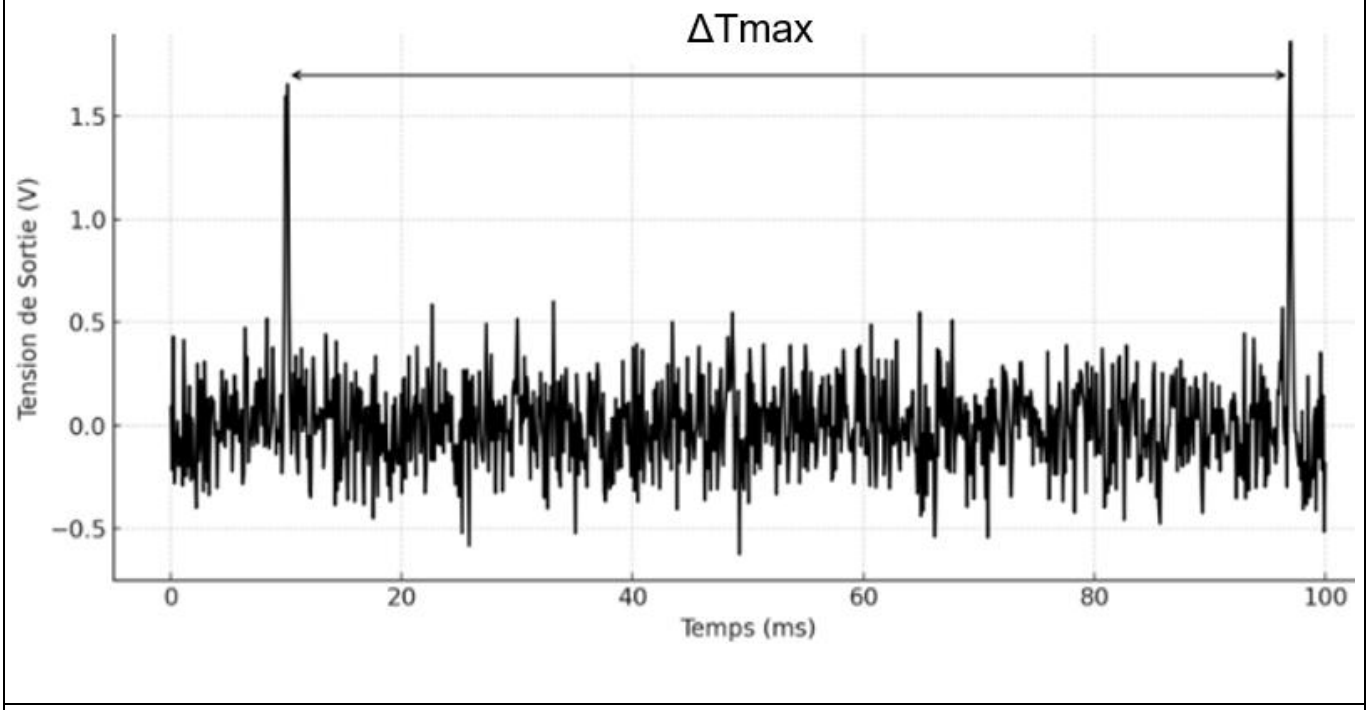


Figure 21 – Tension de sortie du débitmètre en fonction du temps pour le débit minimum

Q48. **Calculer** le temps maximal, noté T_{MAX}, nécessaire pour remplir un verre de 0,25 litre si le temps entre deux impulsions correspond à ΔT_{MAX}.

Q49. **Commenter** la validité du débitmètre OF-10 ZZT d'après les deux critères que doit vérifier le technicien supérieur.

Partie 4 – Détection des fûts de boisson vides

L'objectif de cette partie est de déterminer le nombre, noté N, en sortie du convertisseur analogique-numérique (CAN) qui doit permettre de déclencher l'alerte de fût bientôt vide.

Pour cela, des schémas électriques et les caractéristiques du CAN seront donnés au cours du questionnement.

Afin de maîtriser la manutention permettant de changer les fûts de boisson vides, le technicien supérieur doit vérifier le système permettant de mesurer la masse des fûts.

Le cahier des charges impose qu'une alerte prévienne l'opérateur lorsque la masse du fût est de 6,8 kg, ce qui correspond à une quantité restante de liquide de 2 litres dans le fût (code alerte « - 1 »).

Le capteur de force est constitué de 4 jauges de contraintes collées sur une pièce métallique, appelée corps d'épreuve, comme représenté figure 22.

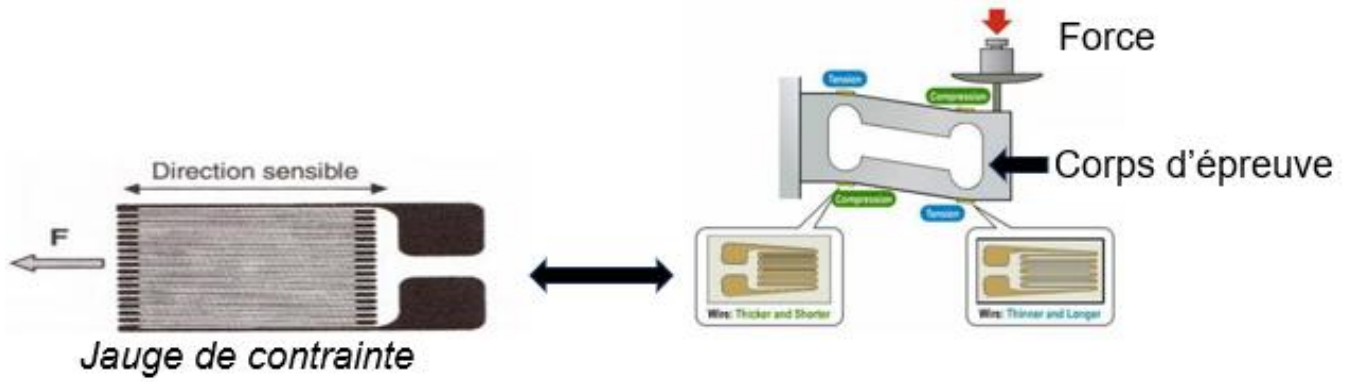


Figure 22 – Capteur de force

Les jauges de contraintes sont des composants purement résistifs dont la résistance varie en fonction de la déformation.

La variation de cette résistance, notée ΔR, est convertie en une tension ΔU par un circuit électronique de conditionnement, appelé pont de Wheatstone, représenté figure 23.

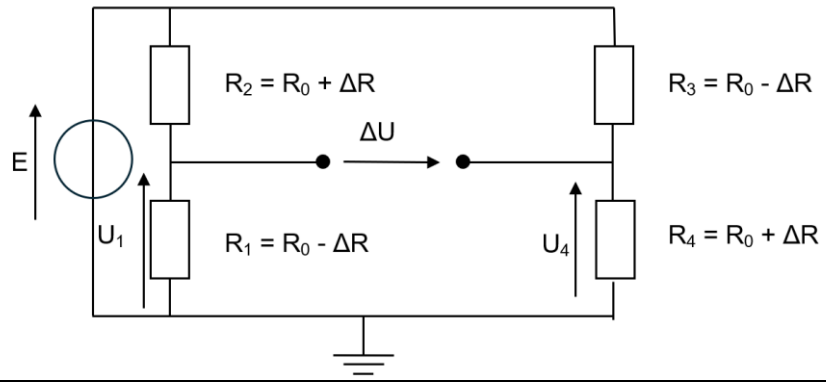


Figure 23 – Circuit électronique de conditionnement

Sur la figure 23 :

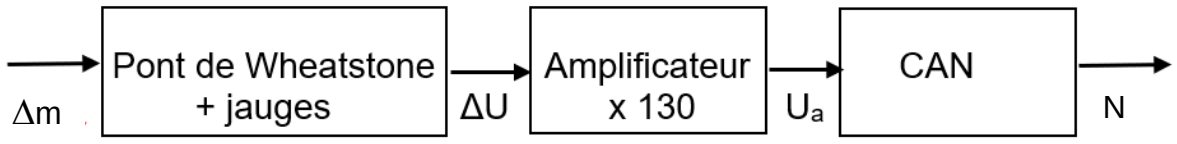
- E est le générateur qui fournit une tension de 5,0 V ;
- R_1, R_2, R_3 et R_4 sont les résistances des jauges de contraintes.

Les résistances des jauges de contraintes, R_1, R_2, R_3 et R_4, sont telles que $R_1 = R_3 = R_0 - \Delta R$ et $R_2 = R_4 = R_0 + \Delta R$ avec R_0 la résistance des jauges en l'absence de masse.

Q50. Exprimer la tension U_1 en fonction de R_1, R_2 et E.

Q51. Exprimer ΔU, grâce à la loi des mailles, en fonction de U_1 et U_4.

Sachant que la résistance de chaque jauge varie en fonction de la masse, on montre que la variation de tension ΔU, exprimée en volts, et la variation de masse Δm, exprimée en kilogrammes, sont liées par la relation : $\Delta U = 10^{-3} \times \Delta m$. Cette variation de tension est amplifiée puis numérisée tel qu'illustré sur la figure 24.



Δm : variation de masse en kg.
ΔU : variation de tension en V.
U_a : tension en entrée du convertisseur en V.

Figure 24 – Schéma fonctionnel de la chaîne de mesure de masse

Le convertisseur analogique-numérique possède une résolution de 24 bits et sa tension de pleine échelle, notée U_{PE}, est de 5,00 V.

Q52. Calculer le quantum q du convertisseur analogique-numérique.

La masse correspondante du fût devant déclencher l'alerte est de 6,8 kg, soit une tension ΔU_{alerte} de 6,8 mV.

Q53. Calculer la tension $U_{a,\ alerte}$ correspondant à ΔU_{alerte} à l'aide de la figure 24.

Q54. Déduire de la question précédente, la valeur numérique décimale, notée N_{alerte}, en sortie du CAN correspondant à cette alerte.

Le technicien supérieur cherche à savoir si la résolution numérique de 24 bits du CAN est suffisante sachant que la résolution analogique de la chaîne de mesure doit être de 2 kg.

Q55. Calculer la résolution analogique de cette chaîne de mesure, puis **en déduire** si la résolution numérique de 24 bits du CAN est suffisante, mais également si elle est judicieuse.

Partie 5 – Caractérisation du protocole de communication NFC

L'objectif de cette partie est de vérifier le protocole de communication entre un lecteur NFC et une étiquette (tag) NFC.

Pour cela, un chronogramme et un spectre de la communication du tag NFC seront donnés au cours du questionnement.

Le NFC est une technique de communication qui repose sur l'interaction magnétique entre le lecteur (composant actif, émetteur) et l'étiquette (purement passive). Le lecteur produit un champ magnétique qui joue un double rôle pour le tag :

- alimenter le tag (récepteur) ;
- envoyer au tag les informations selon le protocole NFC.

Dans un premier temps, le technicien supérieur observe la transmission du lecteur vers l'étiquette (liaison montante).

Le badge respecte le standard ISO/IEC 14443 type A relatif aux cartes d'identification à circuit(s) intégré(s), sans contact et de proximité.

Cette communication, à une fréquence porteuse f_p de 13,56 MHz, se fait par modulation d'amplitude avec un débit de 106 kbits·s^{-1}.

Le codage utilisé est le codage de Miller modifié. Celui-ci est illustré sur la figure 25. Il est construit de la façon suivante :

- le 1 est toujours codé de la même manière ;
- le codage du zéro dépend par contre du bit précédent.

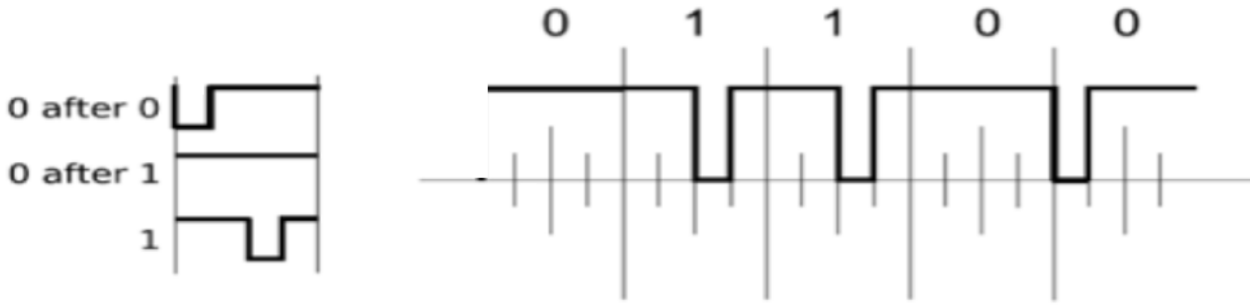


Figure 25 – Exemple de codage Miller modifié
Source : http://igm.univ-mlv.fr

Le signal en bande de base du tag, codé en Miller modifié, est ensuite modulé en amplitude.

Le technicien supérieur a fait une capture de trame de communication du tag et a obtenu l'oscillogramme de la figure 26.

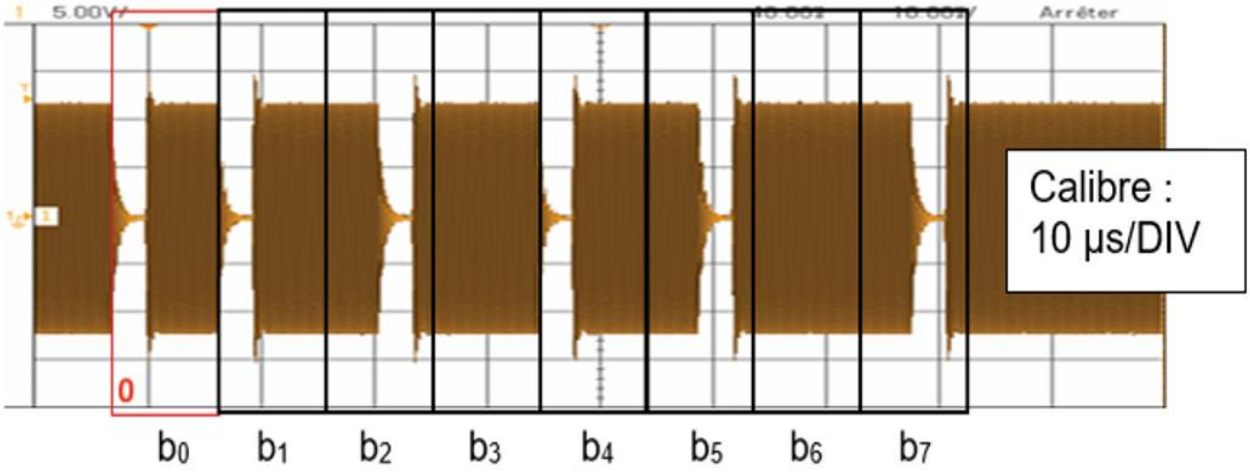


Figure 26 – Relevé d'une transmission vers un badge ou tag

Le premier bit b_0 est un '0'. Il correspond au bit de poids faible.

Q56. **Déterminer** en utilisant l'oscillogramme de la figure 26 la durée d'un bit, notée T_B.

Q57. **Calculer** le débit de cette transmission binaire, noté D, exprimé en kbits·s^{-1}.

Q58. **Écrire**, après l'avoir décodé, l'octet transmis du lecteur vers le tag sous la forme : {b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0}.

Le tableau figure 27 donne la correspondance entre les codes binaires et les commandes envoyées.

b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	0	0	1	1	0	'26' = REQA Commande d'initialisation
1	0	1	0	0	1	0	'52' = WUPA Commande envoyée pour réveiller un tag
0	1	1	0	1	0	1	'35' = Optional timeslot method
1	0	0	X	X	X	X	'40' to '4F' = Proprietary
1	1	1	1	X	X	X	'78' to '7F' = Proprietary
All other values							RFU Commande réservée pour usage futur

Figure 27 – Code binaire des commandes

Q59. **En déduire** en utilisant la figure 27 le nom de la commande transmise au tag.

Cette fois-ci, le technicien supérieur veut vérifier la fréquence de la porteuse qui transporte l'information.

Pour cela, il utilise un analyseur de spectre et obtient le spectre en amplitude représenté sur la figure 28.

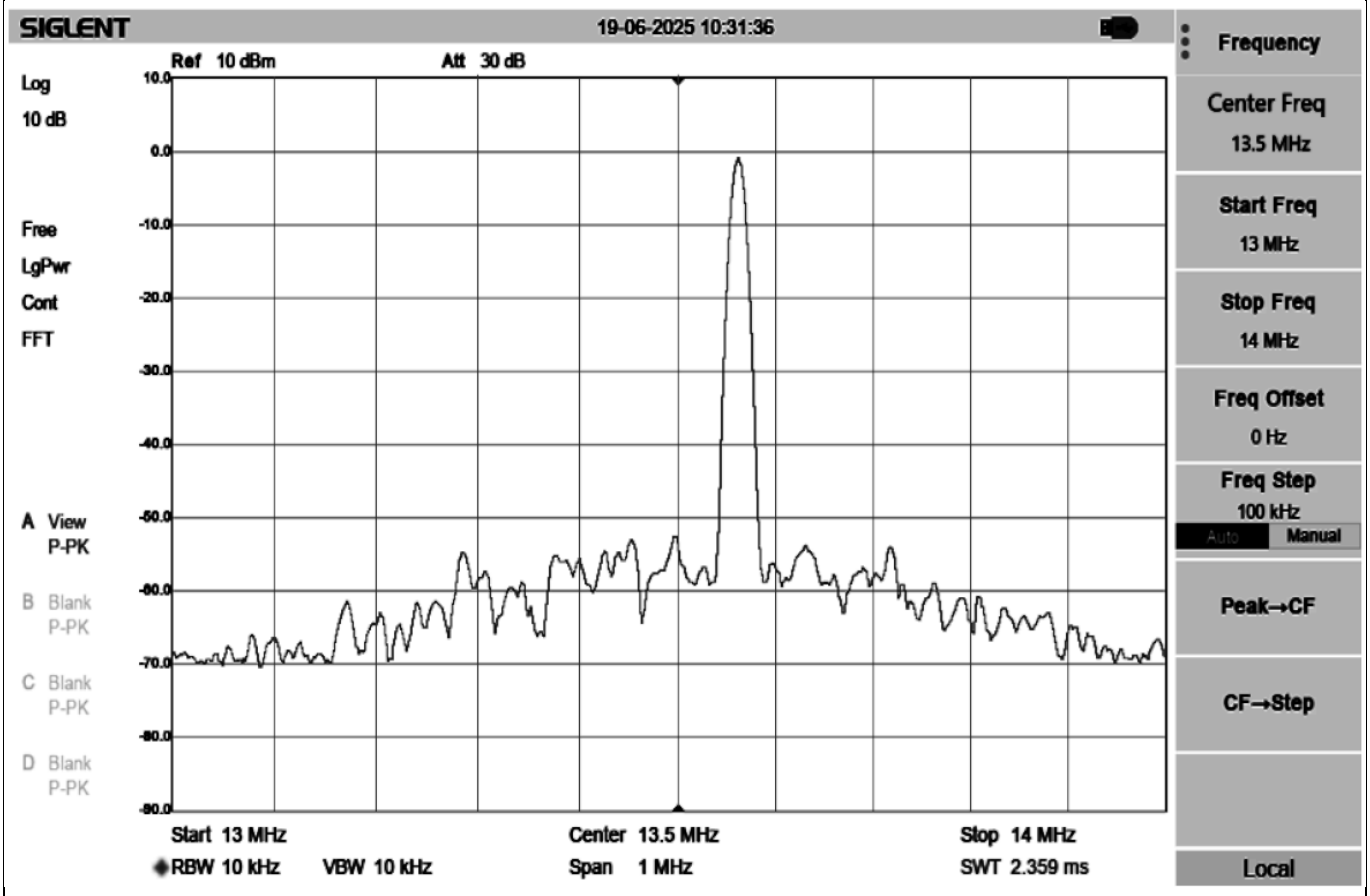


Figure 28 – Spectre en puissance de la porteuse

Q60. **Mesurer** la valeur de la fréquence de la porteuse, notée $f_{porteuse}$, grâce au spectre de la figure 28.

Q61. **Conclure** sur la validité des caractéristiques de fréquence et de débit binaire de la communication entre lecteur NFC et une étiquette (tag) NFC.

Partie 6 – Choix des antennes

L'objectif de cette partie est de faire le choix des antennes Wi-Fi à installer sur le site qui respectent les critères de gain, de fréquence et d'angle d'ouverture.

Pour cela, les caractéristiques des antennes, leur lieu d'implantation et des schémas de principe des bilans de liaisons seront donnés au cours du questionnement.

Le technicien supérieur fait l'étude de la transmission Wi-Fi 5 GHz en espace libre sans obstacle, entre chaque terminal (téléphones portables situés sur les différents stands) et les access points (AP) AP_1 et AP_2 (Cisco Aironet 3702e).

Il a mesuré les distances entre les stands et les AP et a trouvé une distance maximale de 65,0 m.

La communication Wi-Fi entre AP et terminal est bidirectionnelle.

Pour déterminer le gain minimum de l'antenne d'un AP, le technicien supérieur doit tout d'abord faire l'étude de la transmission de l'AP vers le terminal, puis du terminal vers l'AP.

La fréquence du Wi-Fi vaut :

- pour l'AP_1, $f_{Wi\text{-}Fi1}$ = 5,50 GHz (canal 100) ;
- pour l'AP_2, $f_{Wi\text{-}Fi2}$ = 5,54 GHz (canal 108).

On donne le bilan de puissance d'une transmission en espace libre :

$$P_r = P_e + G_e + G_r - FSL$$

avec :

- P_r : niveau de puissance reçue, exprimé en dBm ;
- P_e : niveau de la puissance transmise à l'antenne d'émission, exprimé en dBm ;
- FSL : pertes en espace libre, exprimé en dB ;
- G_e : gain de l'antenne d'émission, exprimé en dBi ;
- Gr : gain de l'antenne de réception, exprimé en en dBi.

Les pertes en espace libre FSL se calculent en utilisant la formule de Friis suivante :

$$FSL = - 147,5 + 20 \times \log(f) + 20 \times \log(d)$$

avec :

- f : fréquence du signal exprimée en Hz ;
- d : distance entre l'AP et le terminal exprimée en m.

Q62. **Montrer** que les pertes en espace libre FSL, pour une distance de 65 mètres et pour une fréquence $f_{Wi\text{-}Fi2}$ de 5,54 GHz, sont environ de 84 dB.

Le technicien supérieur étudie dans un premier temps la transmission du terminal vers l'AP, comme le montre la figure 29.

P_{TER} = 13 dBm	G_{TER} = 0 dBi	FSL = 84 dB	G_{APMIN2} = 6,0 dBi	P_{APMIN} = - 65 dBm

Figure 29 – Transmission entre le terminal et l'AP

Le technicien supérieur étudie dans un second temps la transmission de l'AP vers le terminal, comme le montre la figure 30.

P_{AP} = 23 dBm	G_{APMIN1}	FSL = 84 dB	G_{TER} = 0 dBi	P_{TERmin}

Figure 30 – Transmission entre l'AP et le terminal

La sensibilité du téléphone terminal, notée S_{TER}, vaut - 67 dBm. Elle correspond à la plus petite puissance reçue pour avoir une transmission correcte.

On souhaite une marge de 10 dB par rapport à la sensibilité du terminal.

Q63. **Calculer**, en utilisant la figure 30, la puissance minimale, notée P_{TERmin}, que peut recevoir le terminal pour que la communication soit établie.

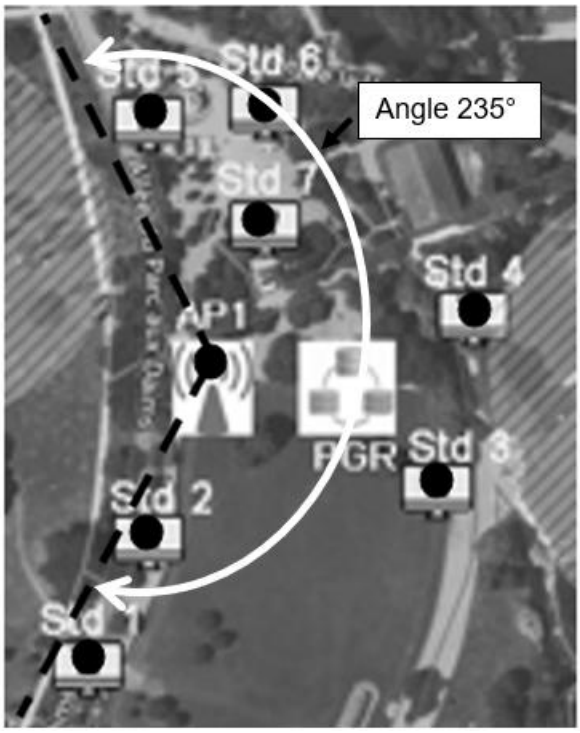
Q64. **Calculer**, en utilisant la figure 30, le gain minimum de l'antenne de l'AP, noté G_{APMIN1}, lorsque la communication se fait de l'AP vers le terminal.

À 5,54 GHz (canal 108, dans la bande 5470 - 5725 MHz), la réglementation française autorise une puissance isotrope rayonnée équivalente (PIRE) maximale d'émission de 1 W, soit 30 dBm.

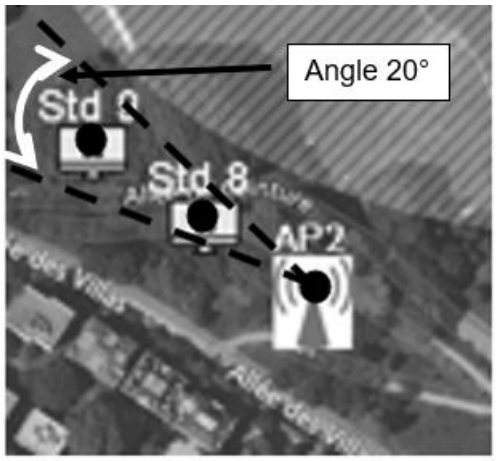
La puissance d'émission vers l'antenne de l'AP étant de 23 dBm, le gain maximum de l'antenne, noté G_{APMAX}, est limité lors de la transmission entre l'AP et le terminal.

Q65. **Calculer** le gain maximum de l'antenne de l'AP, noté G_{APMAX} en dBi, de façon à respecter la réglementation.

Le technicien supérieur mesure les angles d'ouverture des antennes pour l'AP_1 et l'AP_2, comme le montre la figure 31, grâce au plan d'implantation.



Antenne AP_1



Antenne AP_2

Figure 31 – Angles d'ouverture des antennes pour l'AP_1 et l'AP_2

Le technicien supérieur doit maintenant choisir l'antenne de l'AP parmi celles proposées par son fournisseur en figure 32.

Antennes	AIR-ANT 2547-VN	AIR-ANT 2466-PR	AIR-ANT 2568-VG	AIR-ANT 2588-P3M	AIR-ANT 5170-PR	AIR-ANT 5114-P2M
Gain (dBi)	7	6	8	8	7	14
Angle d'ouverture à – 3 dB (Horizontal)	360°	75°	360°	120°	70°	30°
Bande passante (MHz)	5150-5875	2400-2484	5150-5925	5150-5900	5150-5850	5150-5900
Impédance (Ω)	50	50	50	50	50	50

Figure 32 – Caractéristiques des antennes

Q66. **Déterminer**, en le(s) justifiant, le(s) choix d'antenne(s) que peut faire le technicien supérieur pour l'AP_1, puis pour l'AP_2, qui respecte(nt) les critères de gain, de fréquence et d'angle d'ouverture.

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
```

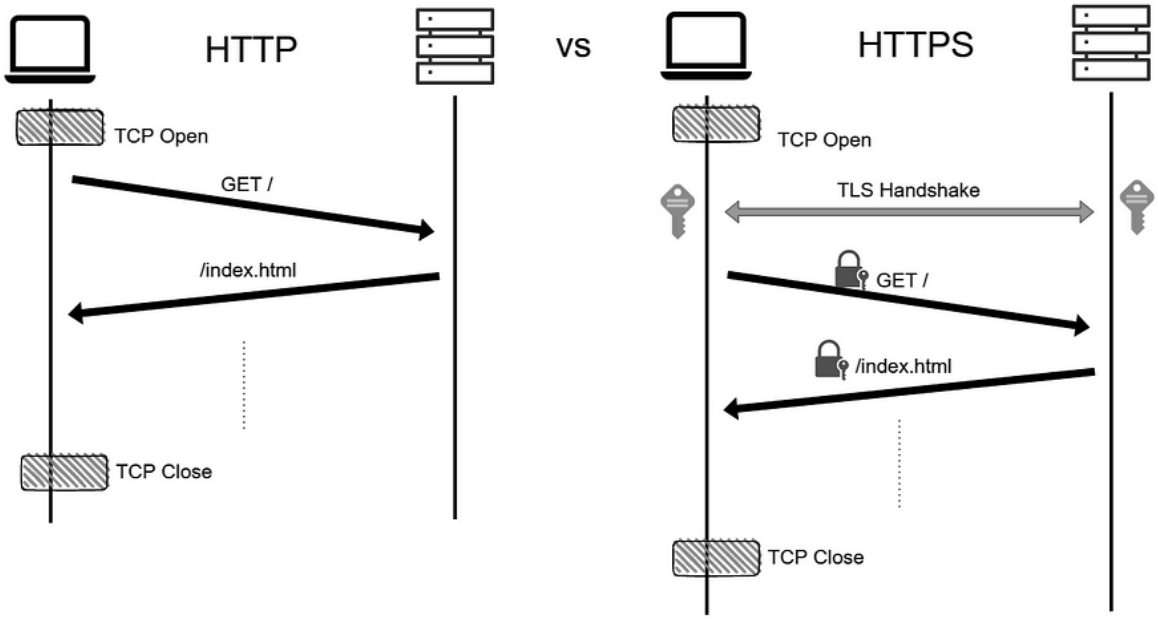
DT2 - Documentation WLC3504

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.

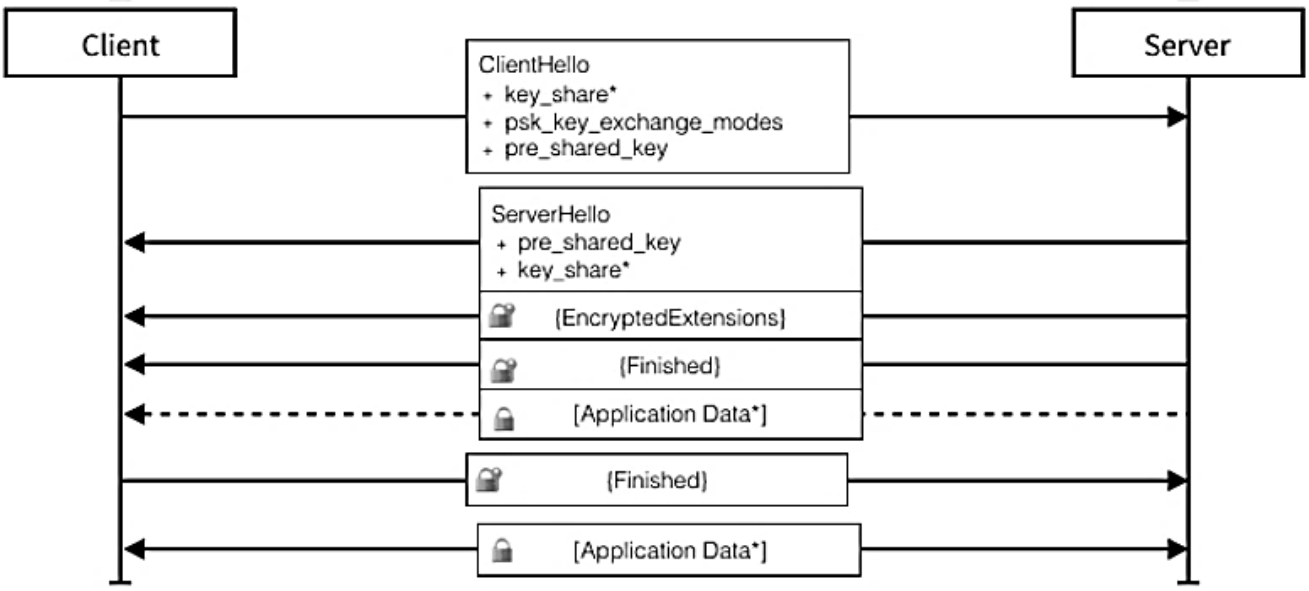
DT3 - Présentation http/https

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

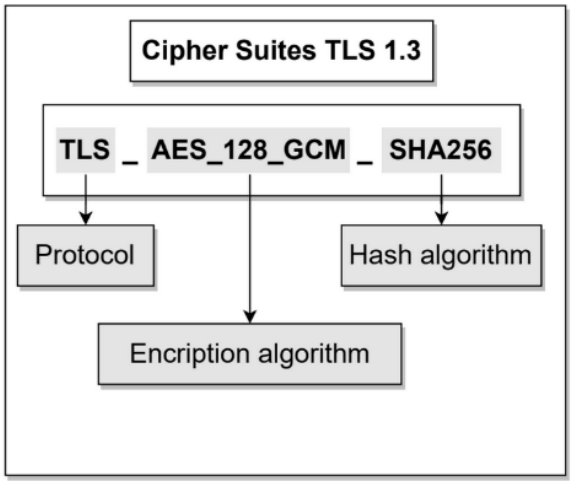


- <u>Diagramme de séquence TLS v1.3 « reprise de session » ou « reprise avec un PSK»</u>

  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

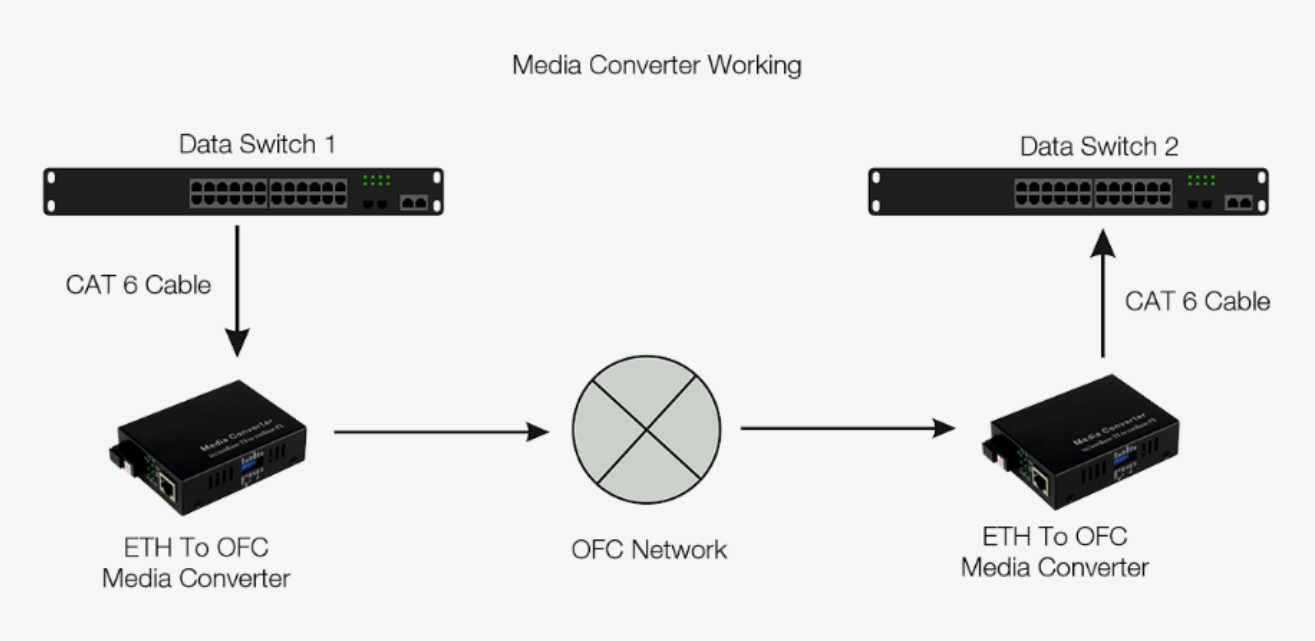
- sécurisation des bureaux distants : idéal pour les environnements de travail à distance, offrant des connexions VPN sécurisées ;
- protection des réseaux internes : renforcement de la sécurité des réseaux internes contre les menaces externes ;
- conformité réglementaire : aide à répondre aux exigences 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`

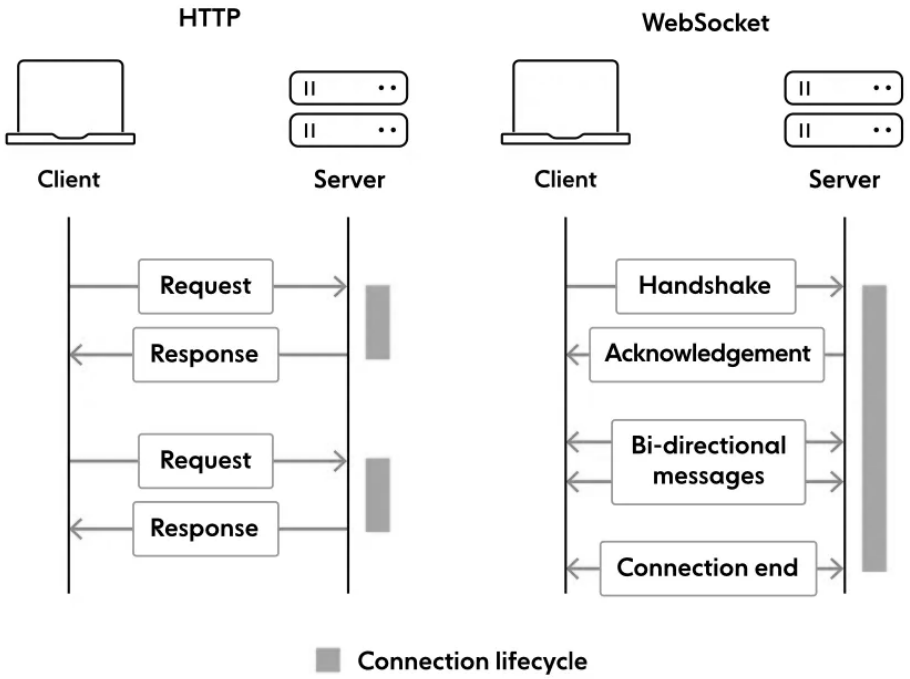
Payload	12	34	56	78	9a	bc	de	f0	12
Masking	ff	ab	89	cd	ff	ab	89	cd	ff
XOR	ed	9f	df	b5	65	17	57	3d	ed

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

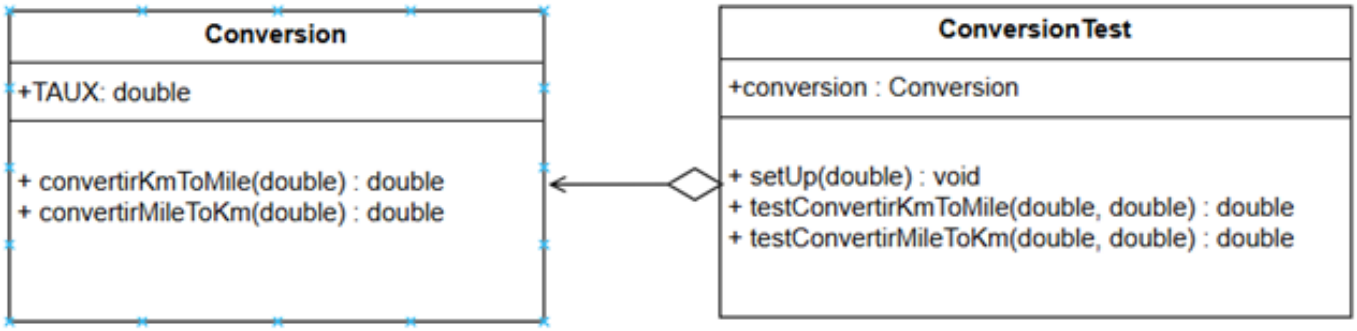


Diagramme de classes

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.

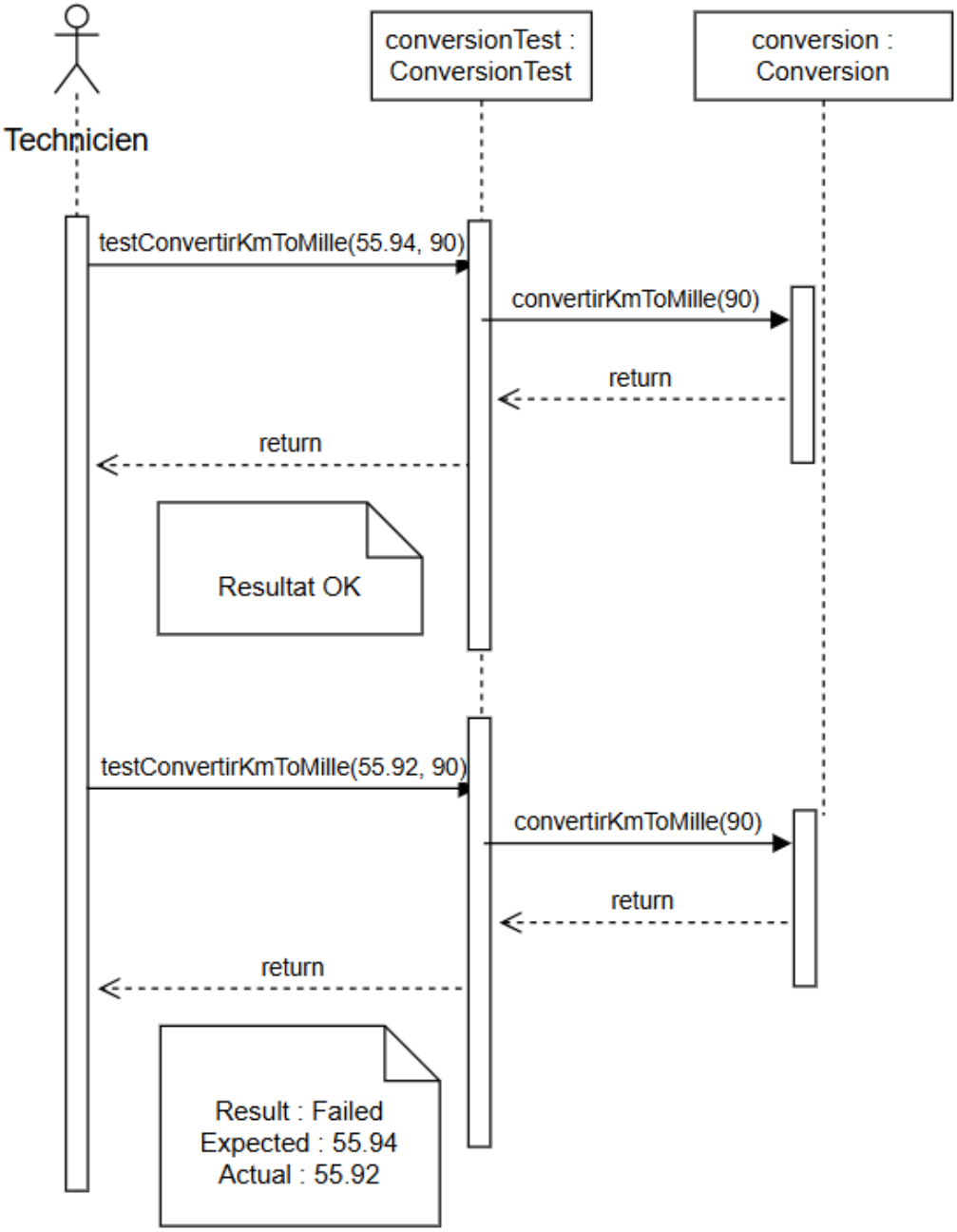
La méthode compare le premier paramètre et le résultat du deuxième paramètre.

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.

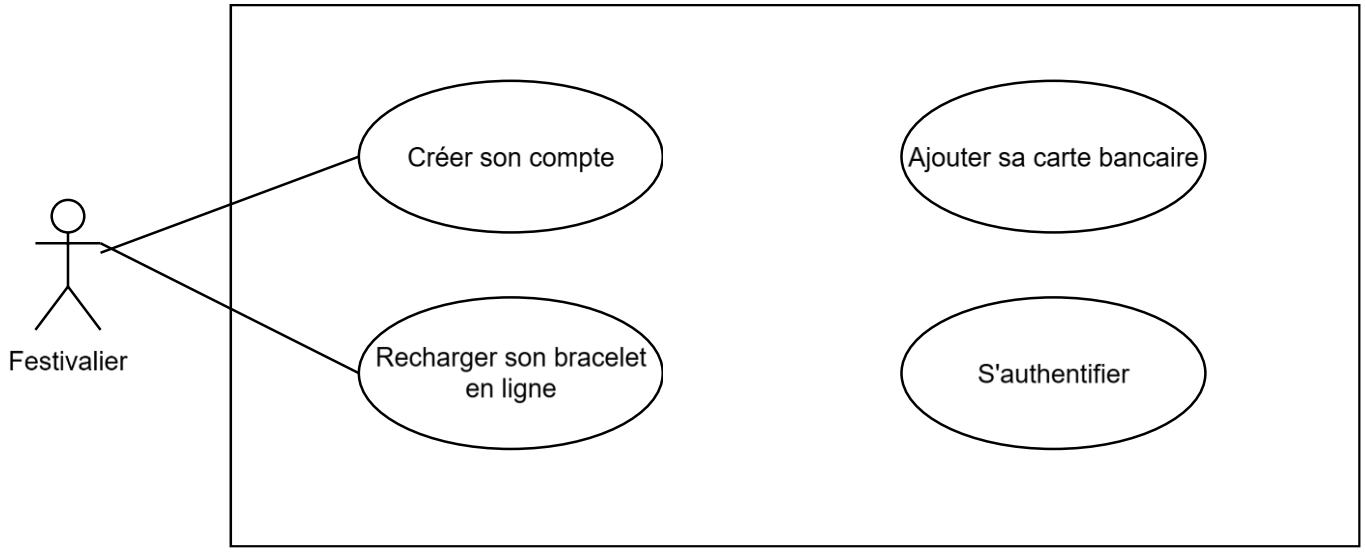
4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable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

DOCUMENT REPONSES – Domaine Professionnel

À RENDRE AVEC LA COPIE

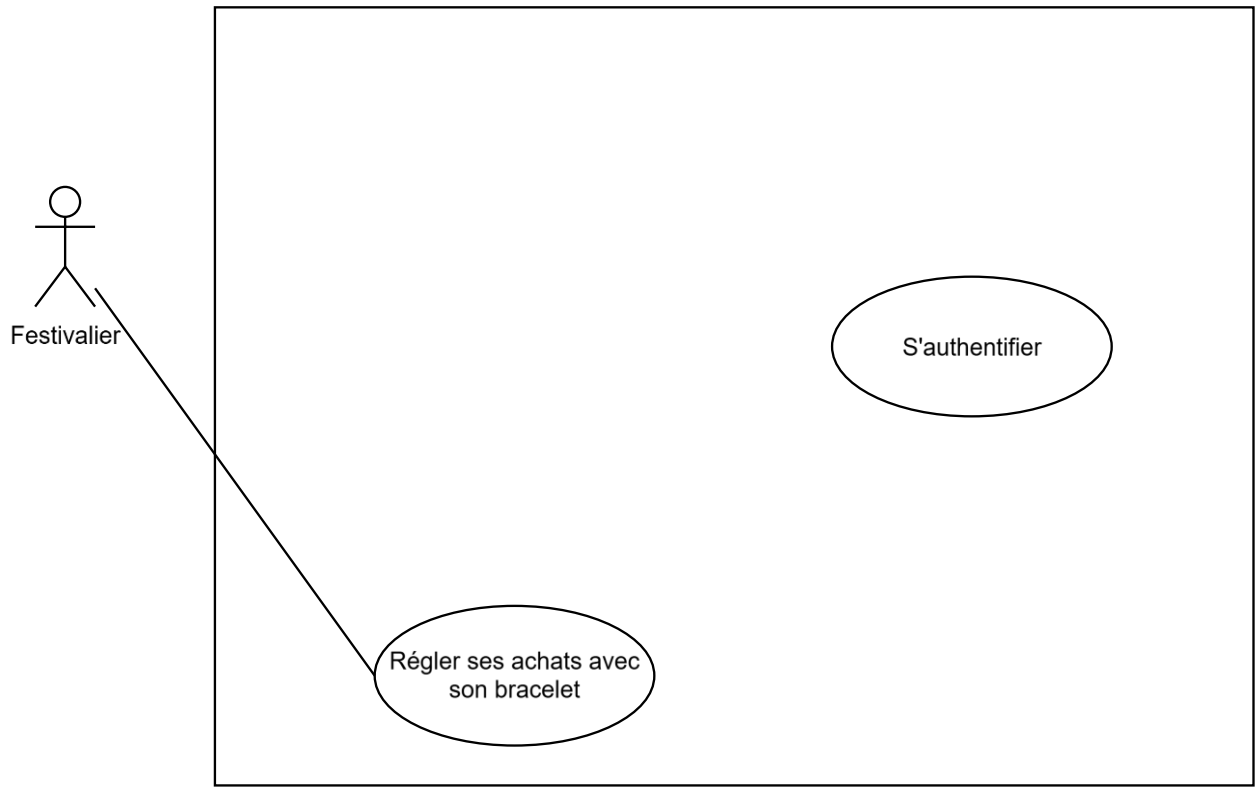
DR-Pro1

Question 1



DR-Pro2

Question 2



Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

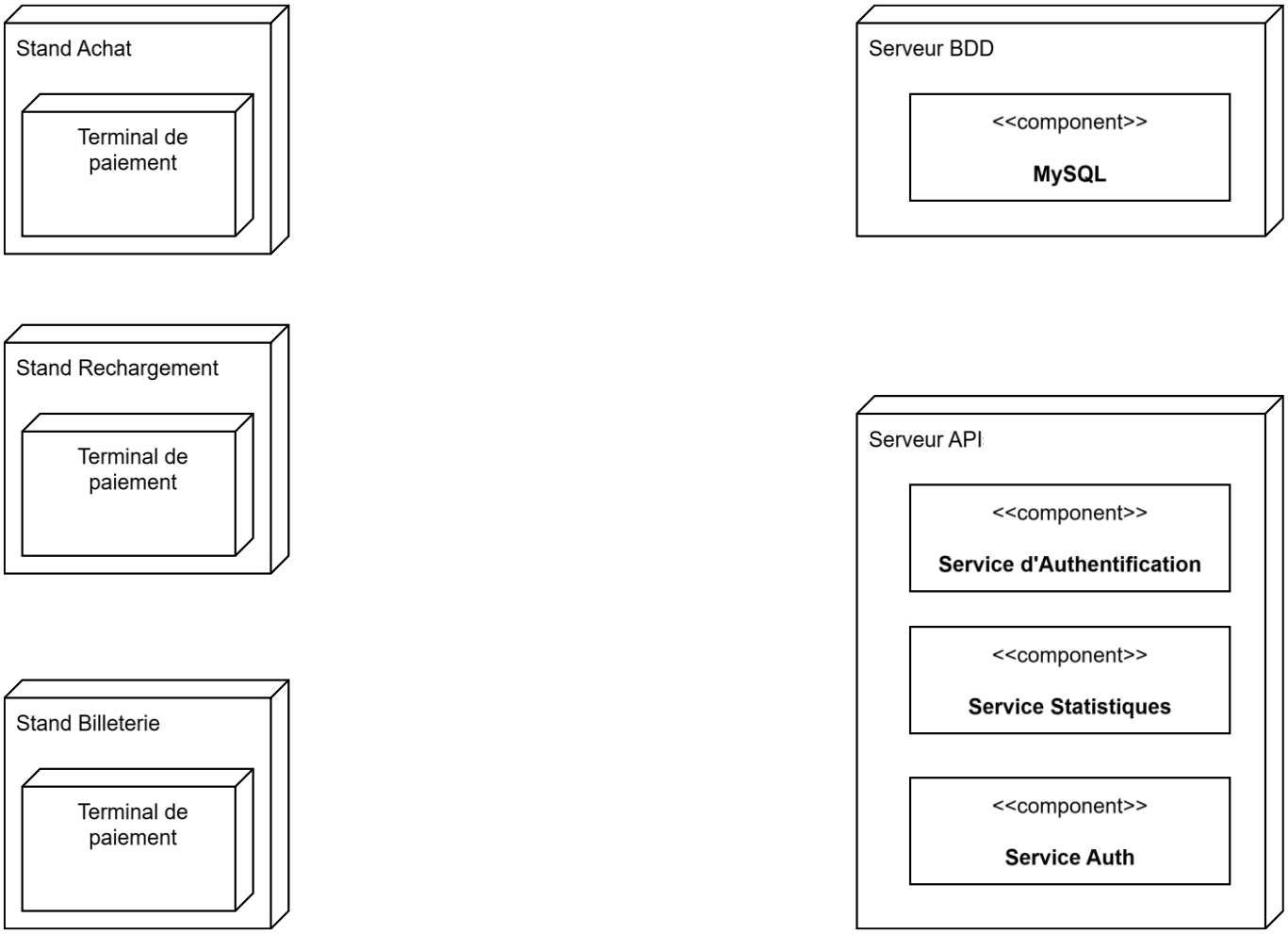
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2

DR-Pro3

Question 3



Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2

DR-Pro4
Question 4

Entourer les caractéristiques qui paraissent correctes pour chaque support.

Support informatique	**Téléphone portable** écran 4" (terminal Cashless)	**Tablette** écran 10", Wi-Fi	**Ordinateur portable** écran 17", Wi-Fi	**Ordinateur fixe** écran 24"
Avantages	Mobilité Taille de l'écran Connexion 4G/5G	Mobilité Taille de l'écran Connexion 4G/5G	Mobilité Taille de l'écran Connexion 4G/5G	Mobilité Taille de l'écran Connexion 4G/5G
Inconvénients	Recharge de la batterie Difficile à déplacer Taille de l'écran	Recharge de la batterie Difficile à déplacer Taille de l'écran	Recharge de la batterie Difficile à déplacer Taille de l'écran	Recharge de la batterie Difficile à déplacer Taille de l'écran

Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2

DR-Pro5
Question 5

Couche physique	Répondre par OUI ou NON
Wifi	
Ethernet	
I2C	
4G / 5G	

DR-Pro6
Question 6

Types de protocole	Répondre par OUI ou NON	Nom de la couche (OSI)
HTTPS		
IP		
SSH		
UDP		

Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

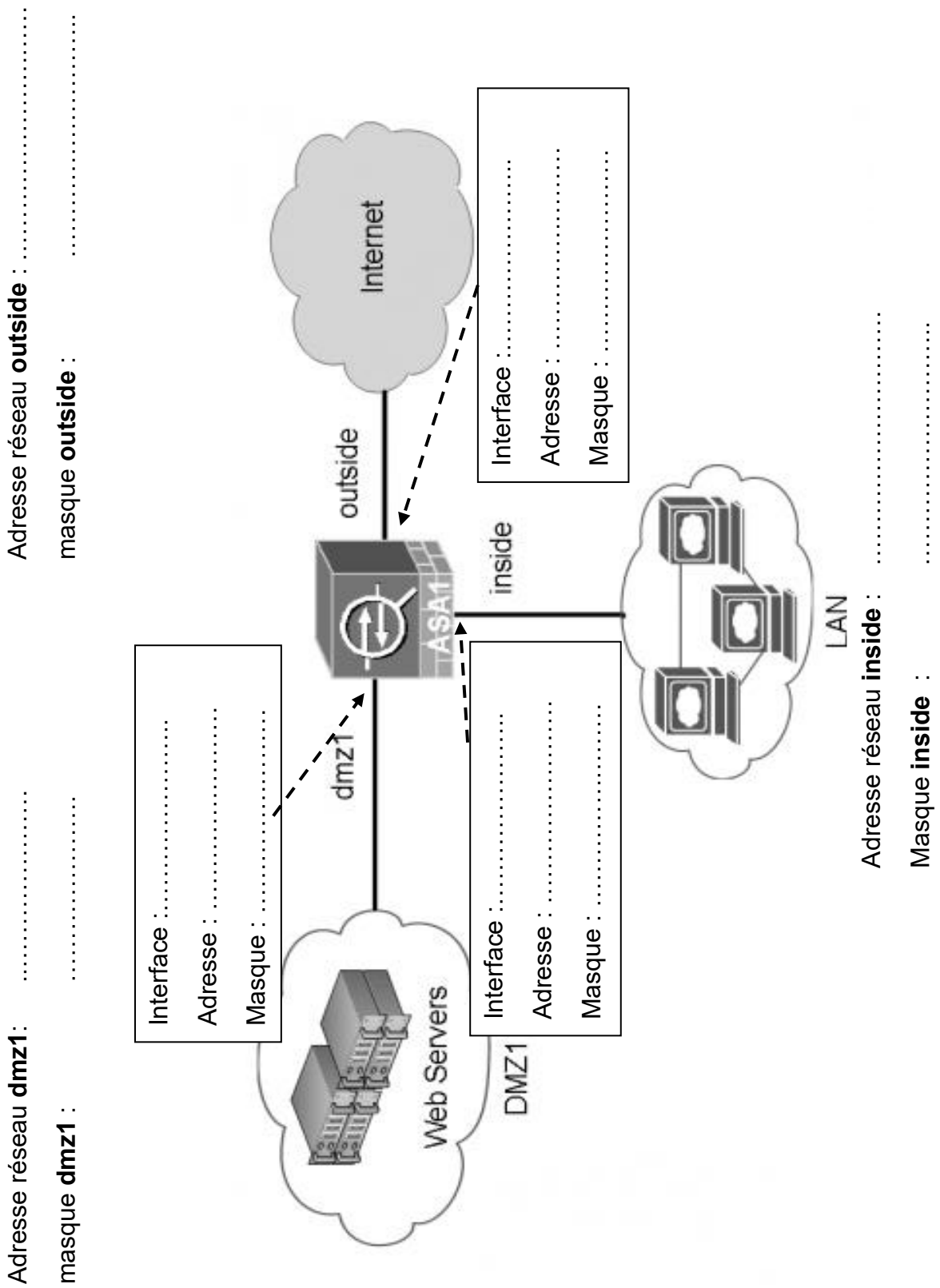
(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2

DR-Pro7
Question 28



Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

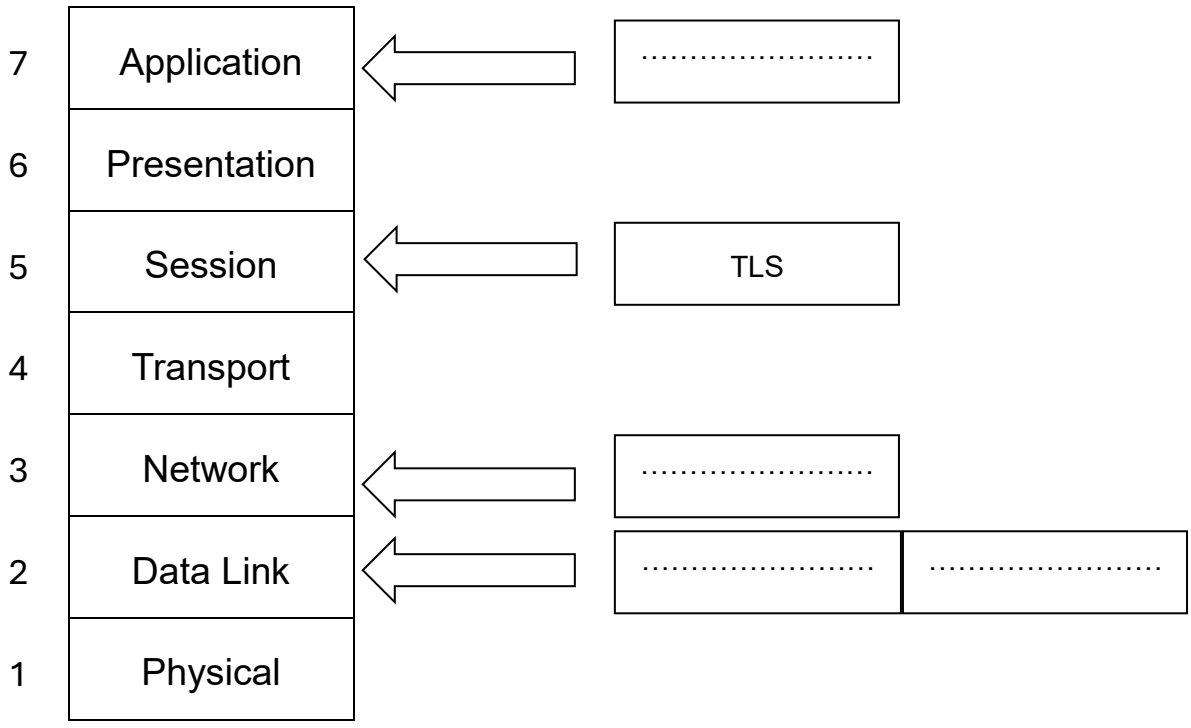
Né(e) le : / /

1.2

DR-Pro8
Question 29

	Adresse du sous réseau	Masque CIDR	Plage des terminaux de paiement	Adresse de la passerelle par défaut	Adresse broadcast
VLAN 10	…….	…..	…… …. …… ….	…….	…….
VLAN 20	…….	…..	…… …. …… ….	…….	…….
VLAN 99	…….	…..	…… …. …… ….	…….	…….

DR-Pro9
Question 30



Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2

DR-Pro10
Question 32

Le taux de TVA est de 20%

Nom	Réf	Nombre	Prix unitaire (HT)	Prix total (HT)
Convertisseur	**5618**	……	……	……
Switch	……	**1**	……	……
Module SFP	……	……	……	……
			Total (HT)	……

Total (TTC) …… €

DR-Pro11
Question 34

	Adresse IPV4	Port
Terminal de paiement	……	……
RPI	……	……
Serveur d'applications		

DR-Pro12
Question 35

	N° ligne (début phase)	N° ligne (fin phase)	N° ligne
Phase de connexion de TCP	……	……	
Séquence où commence WS			……
Acquittement TCP du RPI			……
Acquittement TCP du terminal			……

Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

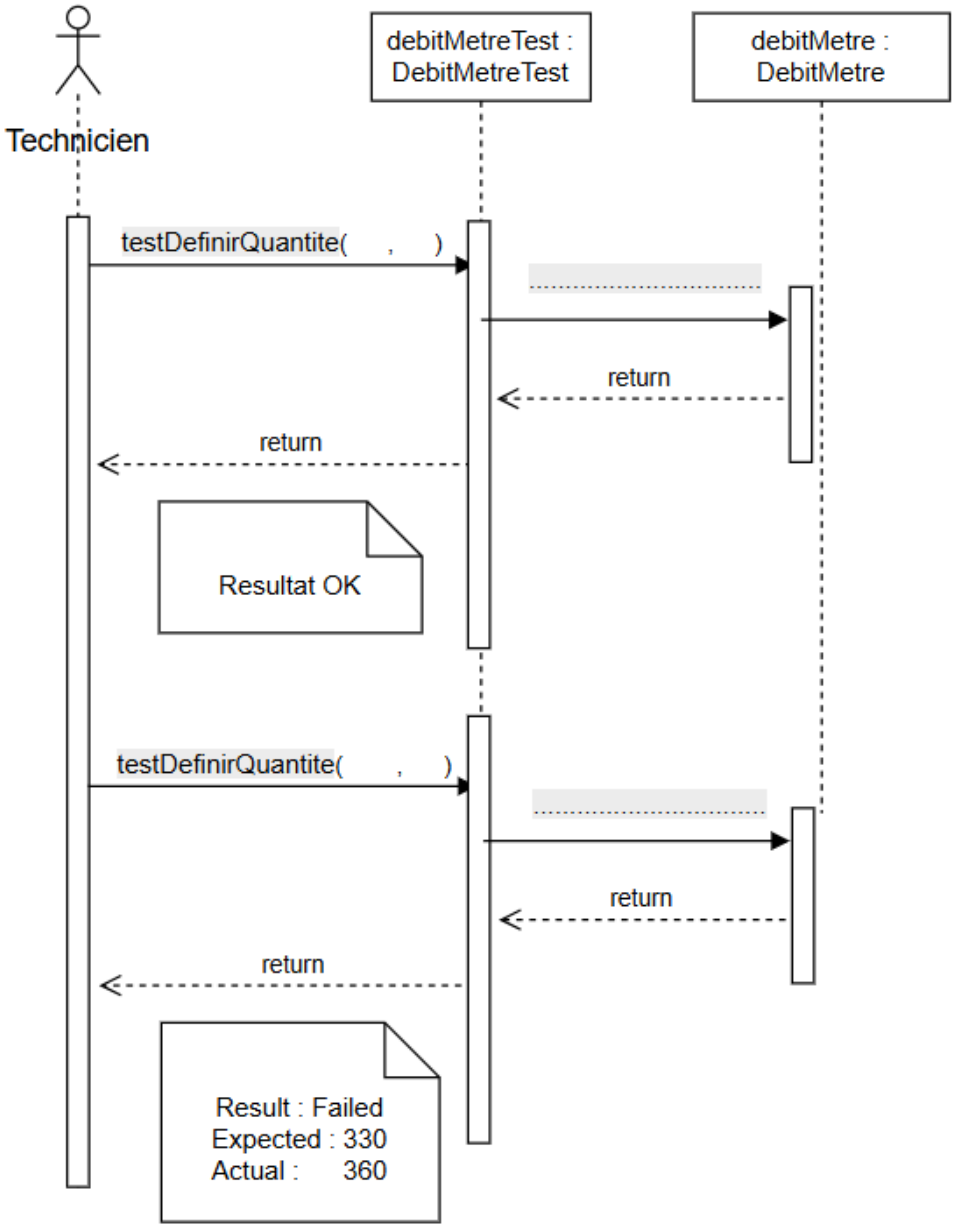
(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2

DR-Pro13
Question 42



Modèle CCYC : ©DNE

NOM DE FAMILLE (naissance) : *(en majuscules)*

PRENOM : *(en majuscules)*

N° candidat :

N° d'inscription :

(Les numéros figurent sur la convocation, si besoin demander à un surveillant.)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Né(e) le : / /

1.2