

# SUJET

## Option A Informatique et Réseaux

Partie 1 - Domaine Professionnel

Durée 3 h - coefficient 3

### Partie A. Analyse du système

L'objectif de cette partie va être d'analyser le système présenté en précisant tout d'abord l'intérêt de l'utilisation d'un système GTB (Gestion Technique de Bâtiment). Les fonctionnalités du logiciel de supervision (Synco IC) et la structure matérielle du système seront ensuite étudiées pour compléter la documentation technique avec des diagrammes UML. Le choix du modèle du serveur WEB SIEMENS OZW772 terminera cette partie.

- Q1.** Préciser les avantages à utiliser un système de gestion technique de bâtiment.
- Q2.** En utilisant la partie de présentation de la plateforme de supervision Synco IC, compléter le diagramme UML des cas d'utilisation sur le **document réponses**. Vous devrez préciser les relations entre les cas d'utilisation ainsi que les relations entre acteurs humains.
- Q3.** En utilisant la partie de présentation du bâtiment support de l'étude, compléter le diagramme UML de déploiement sur le **document réponses**. Vous devrez préciser le type des relations entre les différents éléments ainsi que la cardinalité à chaque extrémité de ces relations.

Le serveur WEB SIEMENS OZW772 fait le lien entre la plateforme de supervision Synco IC et la partie CVC (chauffage, ventilation et climatisation) du système.

- Q4.** En utilisant la documentation PP1, choisir un modèle pour le serveur WEB OZW772. Justifier.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 1 sur 9
PCT-2024	Domaine professionnel - sujet	

## Partie B. Serveur WEB OZW772

L'objectif de cette partie va être l'étude du serveur WEB OZW772 du système GTB. Nous nous intéresserons à sa mise en service ainsi qu'aux connexions et communications avec les autres éléments du système.

La supervision du système GTB est réalisée par l'intermédiaire d'un serveur WEB installé sur l'appareil OZW772. Pour la suite, l'accès à ce serveur WEB sera fait directement depuis un ordinateur équipé d'un navigateur WEB (et non depuis Internet avec la plateforme de supervision Synco IC).

L'architecture simplifiée pour cette partie est représentée ci-dessous :



Figure 1: Architecture simplifiée de l'étude

Nous allons nous intéresser à la mise en service du serveur WEB OZW772, c'est à dire à la configuration permettant la communication entre l'ordinateur et ce serveur.

**Q5.** En utilisant la documentation PP1, compléter le **document réponses** en précisant les 2 interfaces disponibles coté serveur WEB OZW772 pour une connexion avec l'ordinateur. Préciser également la configuration IP (réglage usine) de ces interfaces ainsi que le pilote qu'il sera nécessaire d'installer sur le système d'exploitation de l'ordinateur pour que la communication soit opérationnelle.

On souhaite connecter un ordinateur au serveur WEB OZW772 en utilisant les deux interfaces précédentes en l'absence de serveur DHCP.

**Q6.** Proposer une configuration réseau (IP + masque CIDR) pour les 2 interfaces de cet ordinateur.

**Q7.** En utilisant les documentations PP1 et PP2, indiquer les protocoles applicatifs supportés par le serveur WEB OZW772. Quel est le protocole à privilégier pour accéder au serveur WEB ? Justifier.

Le thermostat RDG100 permet le contrôle de la température dans une pièce en fonction d'une valeur de consigne. Il est relié à une sonde de température QAA32 permettant de mesurer la température ambiante. Le thermostat communique avec le serveur WEB OZW772 par le bus de terrain KNX.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 2 sur 9
PCT-2024	Domaine professionnel - sujet	

Nous allons nous intéresser aux requêtes HTTP générées par le navigateur WEB de l'ordinateur en direction du serveur WEB OZW772. Les méthodes HTTP supportées sont GET, HEAD, POST et OPTIONS. Deux cas de requêtes HTTP seront étudiés :

- demande de la température ambiante mesurée par le thermostat RDG100 ;
- changement de la valeur de consigne de la température du thermostat RDG100.

**Q8.** En utilisant *la documentation PP2*, remplir le **document réponses** en précisant la méthode HTTP utilisée pour demander la température ambiante et celle utilisée pour changer la consigne ? Justifiez.

Nous allons maintenant nous intéresser aux informations circulant sur le bus de terrain KNX entre le serveur WEB OZW772 et le thermostat RDG100.

Comme expliqué dans la documentation PP3, le standard KNX est à la fois un bus de terrain et un protocole de communication. Chaque appareil (le serveur WEB OZW772 et le thermostat RDG100 dans notre cas) est appelé un **participant** et doit posséder une adresse physique unique pour pouvoir communiquer. Cette adresse est composée de 3 nombres séparés par des points. Le format de l'adresse est : **Zone.Ligne.Participant**

Dans un télégramme KNX (nom donné à la trame circulant sur le bus de terrain KNX), l'adresse est codée sur 2 octets :

- **numéro de zone** (4 bits) ;
- **numéro de ligne** (4 bits) ;
- **numéro de participant** (8 bits).

1 <sup>er</sup> octet								2 <sup>ème</sup> octet							
Z	Z	Z	Z	L	L	L	L	PT	PT	PT	PT	PT	PT	PT	PT

Par exemple, si dans un télégramme l'adresse vaut **0x2517**, le participant aura l'adresse physique **2.5.23** (qui correspond à la zone 2, la ligne 5 et le participant 23).

Nous allons nous intéresser au télégramme émis sur le bus de terrain lors de la réponse du thermostat RDG100 à une demande de valeur de température ambiante.

Le télégramme capturé est composé de 16 octets :

BC 02 01 02 96 68 03 D6 0C 33 10 01 04 01 00 **XX**

Avec **XX** représentant l'octet de sécurité permettant le contrôle de l'intégrité des données du télégramme.

**Q9.** En utilisant la partie **Composition du télégramme** de la documentation PP3, remplir le **document réponses** en précisant les différents champs de la trame reçue.

**Q10.** En utilisant la partie **Composition du télégramme** de la documentation PP3, compléter le **document réponses** permettant de calculer l'octet de sécurité.

Dans un télégramme, la valeur de la température ambiante mesurée est codée sur 2 octets. Pour la valeur 0x0FFF la température vaut 81,90 °C et pour la valeur 0x0000 la température vaut 0 °C.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 3 sur 9
PCT-2024	Domaine professionnel - sujet	

**Q11.** Dans le télégramme reçue le champ « valeur de température » vaut **0x0401**. En déduire la température ambiante mesurée en degré Celsius.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 4 sur 9
PCT-2024	Domaine professionnel - sujet	

## Partie C. Gestion des utilisateurs et des sessions

L'objectif de cette partie va être l'étude de la programmation permettant la gestion des utilisateurs et des sessions. L'ajout d'une fonctionnalité permettant le calcul de la durée de connexion d'un utilisateur (durée de la session) sera également traité.

Le système d'exploitation embarqué sur le serveur WEB OZW772 est une distribution Linux utilisant un noyau de version 4.4.2. Les données (utilisateurs et sessions) sont stockées sur un serveur de base de données MySQL interne au serveur WEB OZW772. La structure partielle de la base de données utilisée est décrite sur la figure 5 :

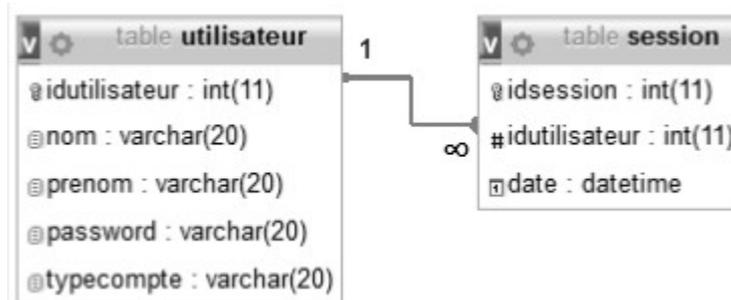


Figure 2: Structure partielle de la base de données

La modification des informations d'un compte dans la base de données se fait en fonction de l'identifiant utilisateur (**idutilisateur**). Il faut donc récupérer cette information.

**Q12.** En utilisant la documentation PP4, élaborer la requête SQL permettant d'obtenir le champ **idutilisateur** pour l'utilisateur de nom **durant**.

**Q13.** En utilisant la documentation PP4, élaborer la requête SQL permettant de modifier le mot de passe et le type de compte pour l'utilisateur ayant l'identifiant **idutilisateur=25**. Le nouveau mot de passe est **56bt7u**, et le type de compte doit être changé en **administrateur**.

Tout utilisateur utilisant le logiciel de supervision doit être authentifié. La table session de la base de données contient les informations de toutes les sessions. Cette table possède les champs suivants :

- **idsession** : identifiant de la session, clé primaire, auto-incrémentation ;
- **idutilisateur** : identifiant de l'utilisateur, clé étrangère ;
- **date** : date et heure du début de la session.

Il faut ajouter à cette table un champ permettant de stocker la durée de la session. Ce champ sera nommé  **duree**  et sera de type **double**.

**Q14.** En utilisant la documentation PP4, élaborer la requête SQL permettant d'ajouter le champ  **duree**  à la table session.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 5 sur 9
PCT-2024	Domaine professionnel - sujet	

## Partie D. Réseau WIFI

Cette partie traite de la conception du réseau WIFI permettant aux employés de se connecter au réseau local et à Internet. Elle permettra de vérifier et valider les choix technologiques effectués.

Dans la gestion des réseaux sans fil (WLAN - Wireless LAN), la tendance est à la centralisation de l'intelligence et du contrôle. Pour créer et appliquer des stratégies sur un grand nombre de points d'accès différents, l'architecture présentée ci-dessous fait appel à un contrôleur WLAN Cisco 2504 et à des points d'accès Cisco Aironet 1602.

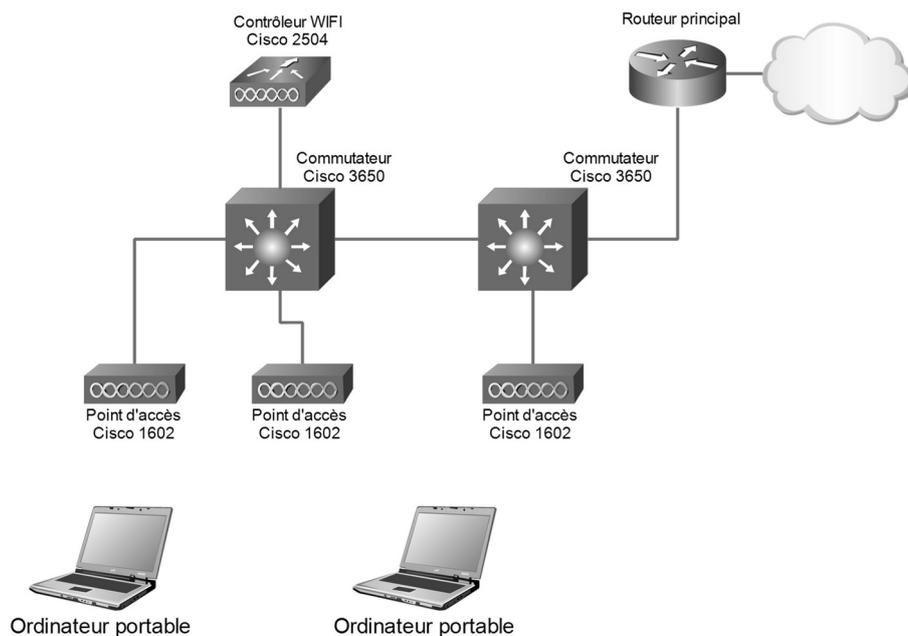


Figure 3: Schéma réseau WIFI

Pour simplifier le câblage électrique du bâtiment, il a été décidé d'alimenter les points d'accès Cisco 1602 en utilisant la technique PoE (PowerOverEthernet) offerte par les commutateurs.

**Q15.** En utilisant la documentation PP5 du point d'accès Cisco 1602, préciser la puissance maximale qu'un port du commutateur devra fournir pour alimenter un point d'accès.

Les commutateurs utilisés sont de type **Cisco 3650-24PS**.

**Q16.** En utilisant la documentation PP6, préciser la puissance maximale qu'un port du commutateur Cisco 3650-24PS peut fournir ainsi que la puissance maximale qu'il est capable de délivrer pour la technologie PoE.

**Q17.** En supposant que tous les points d'accès du bâtiment soient connectés sur le même commutateur, la puissance disponible pour la technologie PoE serait-elle suffisante ? Justifier.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 6 sur 9
PCT-2024	Domaine professionnel - sujet	

Deux réseaux WIFI de SSID **commercial** et **direction** sont gérés par le contrôleur Wireless Cisco 2504. Pour sécuriser l'architecture, Cisco préconise de séparer ces réseaux en utilisant des VLAN (Virtual Local Area Network).

Le réseau pour la gestion du contrôleur et des points d'accès devra également être sur un autre VLAN que ceux des réseaux WIFI (SSID) utilisés par les employés.

L'adresse du réseau de départ utilisée est **192.168.10.0/24**.

Ce réseau sera découpé en 4 sous-réseaux de taille identique. Seuls les 3 premiers sous-réseaux seront utilisés.

**Q18.** *Proposer un plan d'adressage complet pour les 3 sous-réseaux en complétant le document réponses.*

Le contrôleur Wireless Cisco 2504 possède un serveur DHCP permettant de créer 3 plages d'adresses IP pour les 3 sous-réseaux.

Les seules adresses statiques du système seront affectées au contrôleur Wireless Cisco 2504 et aux interfaces du routeur pour l'accès Internet.

La trame suivante a été capturée sur le réseau par le logiciel Wireshark :

No.	Time	Source	Destination	Protocol	Length	Info
24	1.879911	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x82a947e6
25	1.882078	192.168.10.254	255.255.255.255	DHCP	316	DHCP Offer - Transaction ID 0x82a947e6
27	1.882509	0.0.0.0	255.255.255.255	DHCP	347	DHCP Request - Transaction ID 0x82a947e6
32	1.885337	192.168.10.254	255.255.255.255	DHCP	316	DHCP ACK - Transaction ID 0x82a947e6

```

> Frame 24: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{E0FA8AD4-6AEC-4974-A212-7642814D6330}, id 0
  > Ethernet II, Src: HewlettP_90:6c:37 (2c:41:38:90:6c:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: HewlettP_90:6c:37 (2c:41:38:90:6c:37)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 ... = Version: 4
    ... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x7195 (29077)
    > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 0.0.0.0
    Destination: 255.255.255.255
  > User Datagram Protocol, Src Port: 68, Dst Port: 67
  > Dynamic Host Configuration Protocol (Discover)
  
```

Figure 4: Capture trame réseau

**Q19.** *En utilisant la capture de la figure 4 pour la trame 24, compléter le document réponses.*

**Q20.** *Préciser le type d'équipement qui a pu envoyer une telle trame. Justifier.*

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 7 sur 9
PCT-2024	Domaine professionnel - sujet	

## Partie E. Évolution du mode de communication avec le serveur OZW

L'objectif de cette partie va être l'étude de l'évolution du système vers une architecture utilisant la notion d'IoT (internet of Things).

L'IoT (Internet of Things ou Internet des Objets en français) fait référence à l'écosystème des objets connectés utilisant Internet pour échanger des informations. Il recouvre un ensemble de technologies très vastes, qui vont de l'embarqué temps réel jusqu'au stockage dans le Cloud. Il s'agit de faire dialoguer et d'automatiser le comportement des objets du quotidien (capteurs, volets, frigos, vidéosurveillance) pour qu'ils fournissent des services ou envoient des informations sur leur état ou leur environnement afin d'en extraire de la valeur.

Pour améliorer le système, on se propose d'utiliser la notion d'IoT et les protocoles qui sont utilisés dans ce cas.

Le serveur WEB OZW772 pourrait ainsi utiliser ce modèle de connexion pour échanger des informations avec les capteurs et actionneurs de terrain ainsi qu'avec les applications tierces sur Internet.

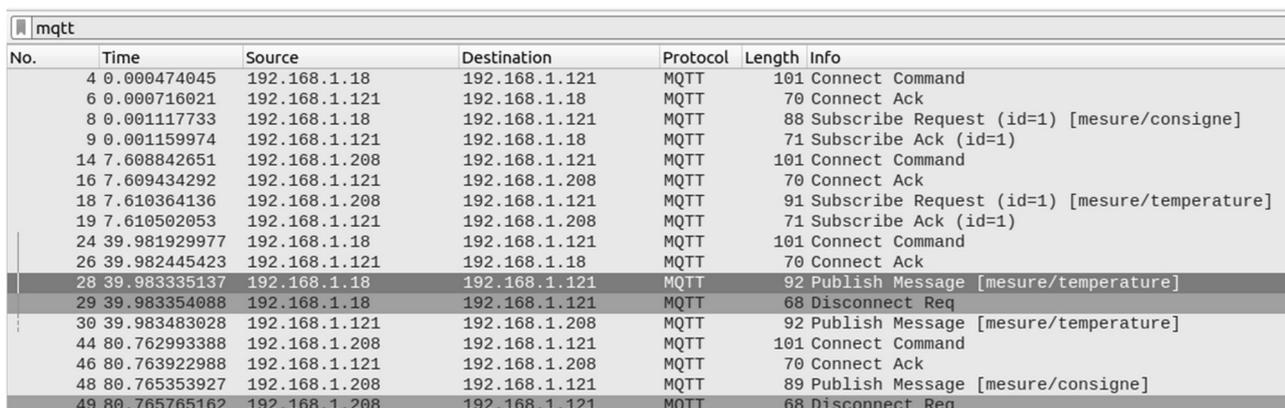
On présente, dans la documentation PP7, le protocole MQTT que l'on souhaite utiliser.

**Q21.** Comment se nomme le serveur utilisé dans le protocole MQTT ?

On propose maintenant d'étudier l'échange de données entre 3 hôtes : un objet connecté de type thermostat, un broker MQTT et un Smartphone d'un usager.

Le thermostat s'abonne à la consigne de température puis publie périodiquement la température mesurée.

Le Smartphone de l'utilisateur s'abonne à la mesure de température et publie la consigne de température fixée par l'utilisateur. La capture de trames suivante a été effectuée par le logiciel Wireshark :



No.	Time	Source	Destination	Protocol	Length	Info
4	0.000474045	192.168.1.18	192.168.1.121	MQTT	101	Connect Command
6	0.000716021	192.168.1.121	192.168.1.18	MQTT	70	Connect Ack
8	0.001117733	192.168.1.18	192.168.1.121	MQTT	88	Subscribe Request (id=1) [mesure/consigne]
9	0.001159974	192.168.1.121	192.168.1.18	MQTT	71	Subscribe Ack (id=1)
14	7.608842651	192.168.1.208	192.168.1.121	MQTT	101	Connect Command
16	7.609434292	192.168.1.121	192.168.1.208	MQTT	70	Connect Ack
18	7.610364136	192.168.1.208	192.168.1.121	MQTT	91	Subscribe Request (id=1) [mesure/temperature]
19	7.610502053	192.168.1.121	192.168.1.208	MQTT	71	Subscribe Ack (id=1)
24	39.981929977	192.168.1.18	192.168.1.121	MQTT	101	Connect Command
26	39.982445423	192.168.1.121	192.168.1.18	MQTT	70	Connect Ack
28	39.983335137	192.168.1.18	192.168.1.121	MQTT	92	Publish Message [mesure/temperature]
29	39.983354088	192.168.1.18	192.168.1.121	MQTT	68	Disconnect Req
30	39.983483028	192.168.1.121	192.168.1.208	MQTT	92	Publish Message [mesure/temperature]
44	80.762993388	192.168.1.208	192.168.1.121	MQTT	101	Connect Command
46	80.763922988	192.168.1.121	192.168.1.208	MQTT	70	Connect Ack
48	80.765353927	192.168.1.208	192.168.1.121	MQTT	89	Publish Message [mesure/consigne]
49	80.765765162	192.168.1.208	192.168.1.121	MQTT	68	Disconnect Req

Figure 5: Capture trames réseau

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 8 sur 9
PCT-2024	Domaine professionnel - sujet	

- Q22.** En analysant la capture de la figure 5, préciser les différents topics utilisés dans cet échange.
- Q23.** En analysant la capture de la figure 5, compléter le tableau du **document réponses** en précisant les adresses IP des hôtes.
- Q24.** En analysant la capture de la figure 5, préciser le numéro de la trame qui permet d'envoyer la température mesurée au Smartphone de l'utilisateur.

On détaille la trame 28 :

```

Frame 28: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_75:3d:14 (08:00:27:75:3d:14), Dst: PcsCompu_ad:b0:a6 (08:00:27:ad:b0:a6)
Internet Protocol Version 4, Src: 192.168.1.18, Dst: 192.168.1.121
Transmission Control Protocol, Src Port: 46058, Dst Port: 1883, Seq: 36, Ack: 5, Len: 26
MQ Telemetry Transport Protocol, Publish Message
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 24
  Topic Length: 18
  Topic: mesure/temperature
  Message: 31322e35
0000  08 00 27 ad b0 a6 08 00 27 75 3d 14 08 00 45 00  ..'.....'u=...E.
0010  00 4e d6 c8 40 00 40 06 e0 05 c0 a8 01 12 c0 a8  .N.@.@.....
0020  01 79 b3 ea 07 5b 5c 62 b1 42 e3 f9 38 50 80 18  .y...[\b -B-8P..
0030  00 e5 70 f0 00 00 01 01 08 0a 00 00 9c 46 00 00  .p.....F..
0040  be 19 30 18 00 12 6d 65 73 75 72 65 2f 74 65 6d  ..0...me sure/tem
0050  70 65 72 61 74 75 72 65 31 32 2e 35             perature 12.5

```

Figure 6: Détail de la trame 28

On s'intéresse à la modélisation en couches selon le modèle TCP/IP.

- Q25.** En vous aidant de la capture de la figure 6, compléter le tableau du **document réponses** en indiquant les noms des protocoles.
- Q26.** En analysant la capture de la figure 6, préciser la valeur de la température mesurée.

Épreuve 0.2	BTS Cybersécurité Informatique et Électronique Option A Informatique et Réseaux Épreuve E4	Page S-Pro 9 sur 9
PCT-2024	Domaine professionnel - sujet	