DOCUMENTATION

Table des matières

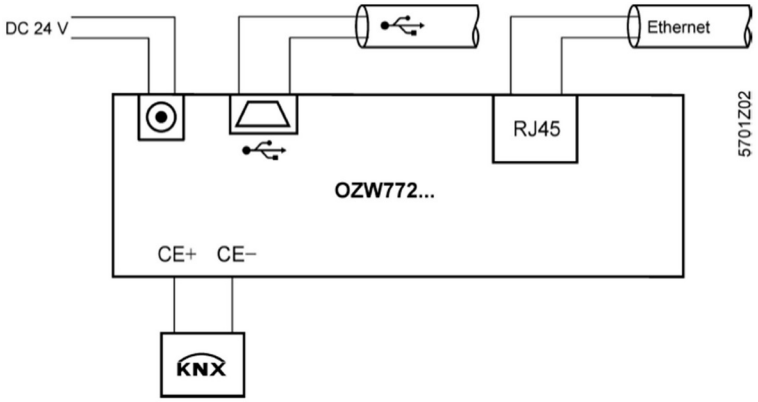
Documentation PP1 : Serveur WEB OZW772

Source : documentation constructeur Serveur WEB OZW772

Références des différents modèles :

Désignation	Nombre maximum d'appareils sur le bus KNX
OZW772.01	1 appareil
OZW772.04	4 appareils
OZW772.16	16 appareils
OZW772.250	250 appareils

Schéma de raccordement :



Caractéristiques techniques :

Alimentation	Tension/courant Consommation	24 V- TBTS, +/-5 %, 625 mA max 2W en général
Liste des appareils	OZW772.01 OZW772.04 OZW772.16 OZW772.250	1 appareil KNX jusqu'à 4 appareils KNX jusqu'à 16 appareils KNX jusqu'à 250 appareils KNX
Bus KNX	Type d'interface	TP1 (Twisted Pair, 1 paire de fils)

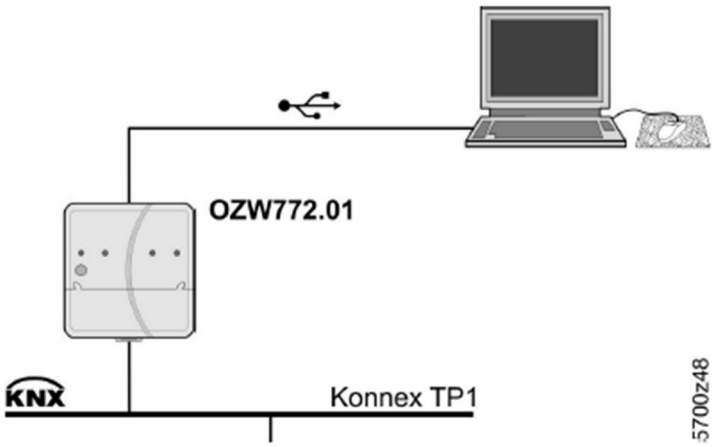
USB	Type d'interface	USB V2.0 Classe d'appareil
	Vitesse de transmission	12 Mb/s
	max. (full speed) Câble de raccordement	
	Longueur de câble	
	max. 3m Type de raccordement à l'ordinateur	
	USB Type A	
	Type de raccordement à l'OZW772	USB Type Mini-B

Ethernet	Type d'interface	100Base-
	TX, IEEE 802.3 Bitrate (vitesse de transmission)	
		max. 100
	Mo/s	
	Protocole	TCP/IP
	Identification	Auto MDI-X
	Raccordement prise	RJ45 (blindé)
	Type de câble	Cat-5 standard, UTP ou STP
	Longueur de câble	100 m max.

Protocoles applicatifs	HTTP (Hypertext Transfer Protocol)	port 80
	HTTPS (HTTP Secure)	port 443
	FTP (File Transfer Protocol)	port 21

Mise en service :

La mise en service du serveur WEB OZW772 s'effectue avec un navigateur WEB via l'interface USB :

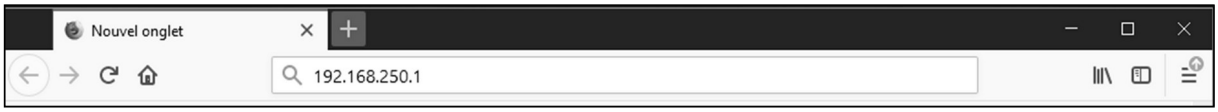


Conditions préalables :

- Le serveur Web est monté et câblé (cf. Instructions d'installation, G5701).
- Les appareils KNX communiquant sur le bus ont été mis en service.
- Les appareils KNX disposent d'une adresse KNX valide [1...253] et sont prêts à fonctionner.
- Remarque : Les serveurs Web sont livrés avec l'adresse KNX 150. Il convient donc d'attribuer à tous les autres appareils KNX une adresse KNX dans la plage [1…253], sauf 150.
- Le bus KNX est alimenté.
- Le serveur Web ou un autre appareil KNX est maître de l'horloge sur le bus KNX.
- Adresse IP USB : 192.168.250.1/24 (non modifiable)

- Adresse IP Ethernet : correspond à l'adresse fournie par le service DHCP s'il est présent. Sans DHCP : 192.168.2.10/24 (réglage usine).
- La mise en service s'effectue avec un PC/portable exploitant un navigateur WEB raccordé sur l'interface USB. La connexion au port USB nécessite l'installation du pilote RNDIS.
- Lorsque le PC/portable a établi une connexion avec Internet et qu'on le raccorde sur la prise USB, le pilote RNDIS s'installe automatiquement, à condition que le service de mise à jour en ligne de Microsoft ait été activé. En l'absence de connexion avec Internet, il est possible d'installer le pilote RNDIS manuellement.

Pour accéder au serveur WEB, entrer l'adresse http://192.168.250.1 dans le navigateur WEB :

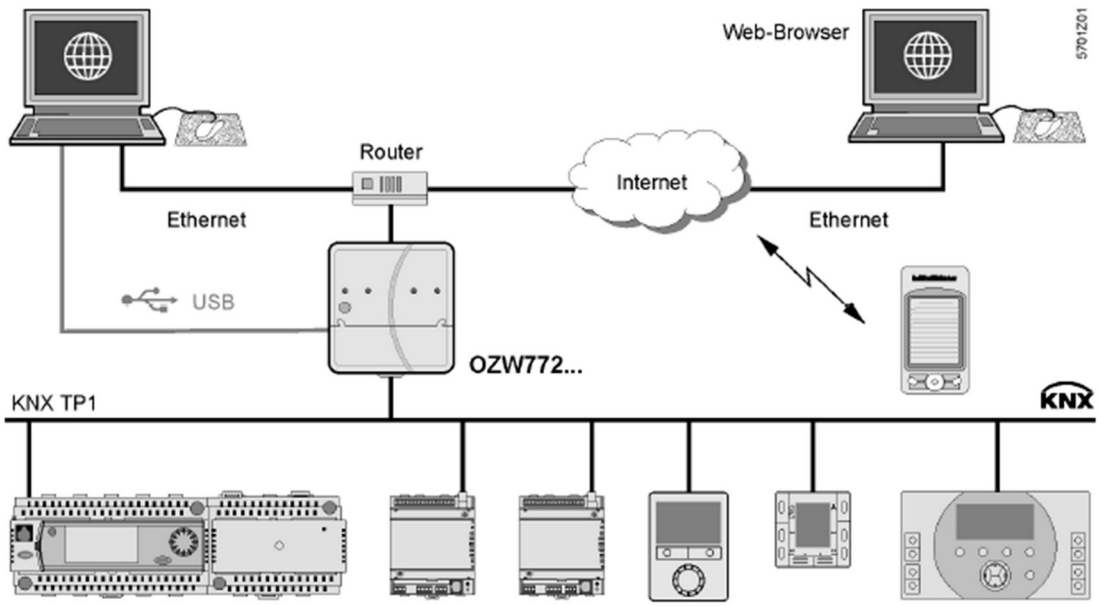


- Login par défaut :
  Username (Nom utilisateur) :
  Administrator Password (Mot de passe) : Password

Exploitation :

L'exploitation de l'installation s'effectue à l'aide d'un PC, d'un smartphone ou d'un téléphone portable disposant d'un navigateur Web compatible, par le biais d'une interface USB, d'une connexion LAN/Ethernet ou d'Internet.

La figure ci-dessous illustre une application d'exploitation type via internet et un réseau local.



Documentation PP2 : Protocoles HTTP et HTTPS

HTTP (Hypertext Transfer Protocol) est un protocole de communication client-serveur développé pour le World Wide Web.

HTTPS (avec S pour Secure) est la variante du protocole HTTP sécurisée par l'usage des protocoles SSL (Secure Sockets Layer) ou TLS (Transport Layer Security). Il garantit la confidentialité des données échangées.

HTTP est un protocole de la couche application du modèle OSI. Il utilise le protocole TCP (mode connecté) au niveau de la couche transport. Un serveur HTTP utilise par défaut le port 80 (443 pour HTTPS).

Les clients HTTP les plus connus sont les navigateurs Web permettant à un utilisateur d'accéder à un serveur Web contenant les données.

Dans le protocole HTTP, une méthode est une commande spécifiant un type de requête, c'est- à-dire qu'elle demande au serveur d'effectuer une action. En général l'action concerne une ressource identifiée par l'URL qui suit le nom de la méthode.

La version HTTP/1.1 du protocole HTTP (RFC 7230 à 7237) définit les méthodes suivantes :

Méthode	Description
GET	Permet de demander une ressource à un serveur. Une requête GET est sans effet sur la ressource.
HEAD	Permet de demander des informations sur une ressource à un serveur, sans demander la ressource elle-même.
POST	Permet de transmettre des données à un serveur dans le but de manipuler une ressource
PUT	Permet d'envoyer des données à un serveur pour créer/mettre à jour une ressource.
DELETE	Permet de supprimer une ressource stockée sur un serveur
CONNECT	Permet d'utiliser un proxy comme tunnel de communication.
OPTIONS	Permet d'obtenir les options de communication d'une ressource ou du serveur en général.
TRACE	Permet de tester et d'effectuer un diagnostic de la connexion en demandant au serveur de retourner la requête reçue.

Documentation PP3 : Le standard KNX

Le standard KNX (abréviation de KoNneX) est à la fois un bus de terrain et un protocole de communication. Il est issu du regroupement de 3 standards européens BatisBus, EIB et EHS en 2002. KNX est utilisé dans des applications de gestion d'énergie, d'éclairage, de chauffage, de ventilation, de climatisation, etc.

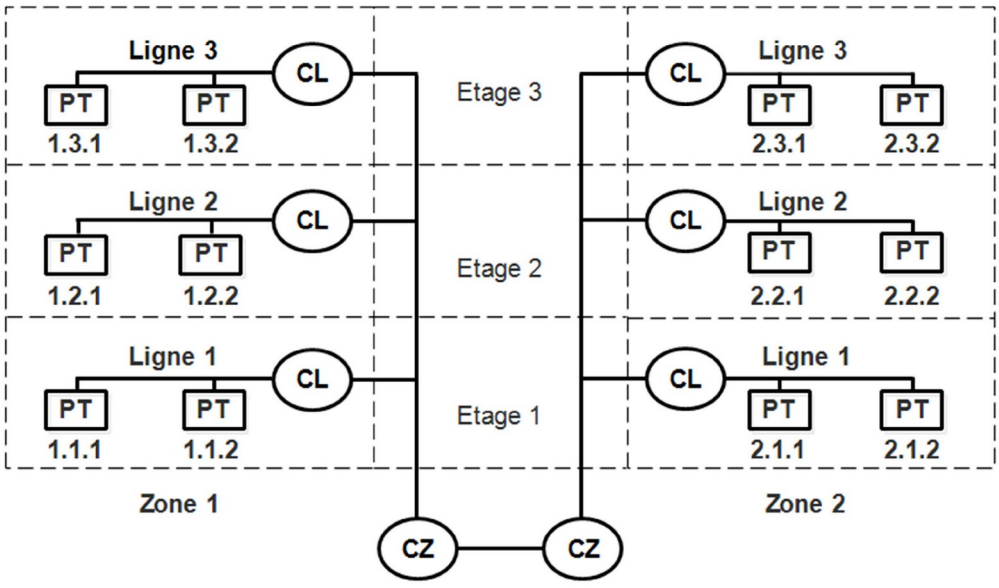
Architecture d'une installation KNX :

L'installation KNX dans un bâtiment est divisée en **zones** (15 max.). Chaque zone peut contenir plusieurs **lignes** (15 max.). Les appareils KNX appelés **participants** seront connectés à une ligne (maximum de 64 participants par ligne).
Les lignes peuvent être reliées ensemble par des coupleurs de lignes. Les zones peuvent être reliées entre elles par des coupleurs de secteurs.

Tous les participants KNX possèdent une adresse physique. Cette adresse doit être unique dans toute l'installation. Elle est composée de 3 nombres séparés par des points. Le format de l'adresse est : **Zone.Ligne.Participant**

Par exemple un participant peut avoir l'adresse physique 2.5.23 qui correspond à la zone 2, la ligne 5 et le participant 23.

Exemple d'architecture d'un bâtiment contenant 2 zones de 3 lignes chacune.



Des coupleurs de zones (CZ) et des coupleurs de lignes (CL) permettent à tous les participants (PT) de communiquer même si ceux-ci ne se trouvent pas sur la même ligne.

Bus de terrain KNX :

Le bus de terrain préconisé est une paire torsadée d'où le nom de KNX TP (Twisted Pair). Les informations sont transmises de façon symétrique sur le bus. Le participant exploite la différence de tension entre les deux fils du bus pour décoder les données. Les parasites sont supprimés et le signal amplifié. La paire différentielle est très utilisée en Gestion technique du Bâtiment, cette liaison est une liaison série asynchrone, multipoints et symétrique (ou différentielle). La liaison est du type RS485. La transmission se fait en mode série asynchrone à la vitesse de 9600 bits/seconde.

Les messages envoyés par les participants KNX sont appelés des **télégrammes**.

Composition du télégramme dans le cas où le champ destinataire est une adresse physique :

Le télégramme se décompose en plusieurs champs :

Contrôle	**Adresse source**	**Adresse destinataire**	**Type de destinataire**	**Compteur routage**	**Longueur données**	**Données**	**Sécurité**
8 bits	16 bits	16 bits	1 bit	3 bits	4 bits	Jusqu'à 16*8 bits	8 bits
Octet 1	Octets 2/3	Octets 4/5	Octet 6			Octets 7 à n	Octet n+1

La longueur du télégramme peut varier de 9 à 23 octets (2 octets de données au minimum).

Champ de contrôle (octet 1)

Codé sur 1 octet, il sert à définir la priorité de transmission de la façon suivante :

champ de contrôle								
1	0	R	1	P	P	0	0	
				0	0			priorité système
				1	0			priorité alarme
				0	1			priorité haute
				1	1			priorité basse
		0						répétition
		1						émission normale

Champ adresse source (octet 2 et 3)

Il s'agit de l'adresse physique du participant émetteur codée sur 2 octets.
Chaque participant est identifié par une **adresse physique unique** sur tout le réseau. Cette adresse comprend :

- Un n° de zone (4 bits)
- Un n° de ligne (4 bits)
- Un n° de participant (8 bits)

1er octet								2ème octet							
Z	Z	Z	Z	L	L	L	L	PT	PT	PT	PT	PT	PT	PT	PT

Exemple :

L'adressage physique d'un participant raccordé à la ligne 3 de la zone 2 sera 2.3.X où X est le numéro de participant qui doit être compris entre 1 et 255 inclus. Si le numéro du participant est 1, cette adresse s'écrira **2.3.1** soit en binaire : **00100011 00000001**.

Champ adresse destinataire (octet 4 et 5)

Ce champ est composé de la même manière que le **champ adresse source**.

Champ type de destinataire (bit de poids fort b7 de l'octet 6)

Ce bit à la valeur **0** (l'adresse du destinataire est une adresse physique).

Champ compteur de routage (bits b6-b5-b4 de l'octet 6)

Le participant émetteur délivre le télégramme avec le compteur de routage (CR) initialisé à 6. Chaque coupleur (zone ou ligne) décrémente le CR de 1 et transmet le télégramme plus loin tant que le CR est positif (on tient compte de la table de filtrage).

Si le CR = 7 alors il ne sera pas décrémenté et il pourra sillonner toute l'installation sans tenir compte des tables de filtrage.

Il contient la valeur du compteur de routage codée sur 3 bits (valeur 6 la plupart du temps, valeur 7 diagnostics).

Champ longueur des données (bits b3-b2-b1-b0 de l'octet 6)

Il indique la longueur du champ de données en octets : codage sur 4 bits (la longueur du champ de données est comprise entre 2 et 16 octets).

Champ de longueur				
0	0	0	1	2 octets
0	0	1	0	3 octets
0	0	1	1	4 octets
0	1	0	0	5 octets
0	1	0	1	6 octets
0	1	1	0	7 octets
0	1	1	1	8 octets
1	0	0	0	9 octets
1	0	0	1	10 octets
1	0	1	0	11 octets
1	0	1	1	12 octets
1	1	0	0	13 octets
1	1	0	1	14 octets
1	1	1	0	15 octets
1	1	1	1	16 octets

Champ de données (octets 7 à n)

Champ contenant les données transmises.
Le champ de données peut contenir jusqu'à 16 octets avec un minimum de 2 octets.

Champ de sécurité (octet n+1)

Le champ de sécurité est constitué d'un octet qui permet le contrôle de la bonne transmission du télégramme.

Cet octet de vérification (bits S0 à S7) est généré en parité impaire.

Il faut faire la somme des bits de même poids qui sont à 1 dans tous les octets du télégramme. Si cette somme est paire, la valeur du bit correspondant dans l'octet de sécurité sera mise à 1. Si cette somme est impaire la valeur du bit correspondant dans l'octet de sécurité sera mise à 0.

Exemple numérique :

Si le télégramme reçu (sans l'octet de sécurité) est : BC 12 0A 33 03 E1 00 81

D7	D6	D5	D4	D3	D2	D1	D0	
1	0	1	1	1	1	0	0	BC : 1er octet du télégramme
0	0	0	1	0	0	1	0	12 : 2ème octet du télégramme
0	0	0	0	1	0	1	0	0A : 3ème octet du télégramme
0	0	1	1	0	0	1	1	33 : 4ème octet du télégramme
0	0	0	0	0	0	1	1	03 : 5ème octet du télégramme
1	1	1	0	0	0	0	1	E1 : 6ème octet du télégramme
0	0	0	0	0	0	0	0	00 : 7ème octet du télégramme
1	0	0	0	0	0	0	1	81 : 8ème octet du télégramme

3	1	3	3	2	1	4	4	Calcul du nombre de bits à 1

0	0	0	0	1	0	1	1	Octet de vérification S
0				B				Valeur de S en hexadécimale

Le télégramme complet est alors : BC 12 0A 33 03 E1 00 81 0B

Documentation PP4 : Principales requêtes SQL d'un serveur MySQL

Utiliser (rendre active) une base de données existante	USE nom_de_la_base;
Créer une base de données	CREATE DATABASE nom_de_la_base;
Supprimer une base de données	DROP DATABASE nom_de_la_base;
Créer une table dans la base de données active	CREATE TABLE nomTable (id INT NOT NULL AUTO_INCREMENT, champ1 DOUBLE, champ2 VARCHAR, champ3 TIMESTAMP NOT NULL, …, PRIMARY KEY(id)) ;
Ajouter des nouveaux champs (colonnes) dans une table	ALTER TABLE nomTable ADD nomChamp1 double, ADD nomChamp2 varchar(20) ;
Sélectionner toutes les informations de la table	SELECT * FROM nomTable ;
Sélectionner seulement les informations d'un champ	SELECT nomChamp FROM nomTable ;
Sélectionner tous les champs d'une table correspondant à un critère	SELECT * FROM nomTable WHERE nomChamp1 = 10;
Sélectionner tous les champs d'une table correspondant à deux critères	SELECT * FROM nomTable WHERE nomChamp1 = 'poste' AND nomChamp3 < 12 ;
Sélectionner sur plusieurs tables nomTable1.nomChamp1 est une clé primaire nomTable2.nomChamp4 est une clé étrangère	SELECT * FROM nomTable1, nomTable2 WHERE nom_table1.nomChamp1 = nom_table2.nomChamp4 ;
Écrire une nouvelle entrée dans une table de BDD	INSERT INTO nomTable(nomChamp1, nomChamp2) VALUES(valeur, 'chaine') ;
Modifier les informations de l'entrée dont le champ id = 51	UPDATE nomTable SET nomChamp1=10, nomChamp2='chaine' WHERE id=51 ;

Documentation PP5: Cisco Aironet 1600

Source : extrait de la documentation constructeur Cisco Aironet 1600

Item	Specification
Environmental	**Cisco Aironet 1600i** ・Nonoperating (storage) temperature: -22 to 158 °F (-30 to 70 °C) ・Nonoperating (storage) Altitude Test -25 °C, 15,000 ft. ・Operating temperature: 32 to 104°F (0 to 40°C) ・Operating humidity: 10 to 90 % percent (noncondensing) ・Operating Altitude Test - 40 °C, 9843 ft. **Cisco Aironet 1600e** ・Nonoperating (storage) temperature: -22 to 158 °F (-30 to 70 °C) ・Nonoperating (storage) Altitude Test - 25°C, 15,000 ft. ・Operating temperature: -4 to 122 °F (-20 to 50 °C) ・Operating humidity: 10 to 90 percent (noncondensing) ・Operating Altitude Test -40 °C, 9843 ft
System Memory	・256 MB DRAM ・32 MB flash
Input Power Requirements	・AP1600: 44 to 57 VDC ・Power Supply and Power Injector: 100 to 240 VAC; 50 to 60 Hz
Powering Options	・802.3af Ethernet Switch ・Cisco AP1600 Power Injectors (AIR-PWRINJ4=, AIR-PWRINJ5=) ・Cisco AP1600 Local Power Supply (AIR-PWR-B=)
Power Draw	・AP1600: 12.95 W **Note:** When deployed using PoE, the power drawn from the power sourcing equipment will be higher by some amount dependent on the length of the interconnecting cable. This additional power may be as high as 2.45 W, bringing the total system power draw (access point + cabling) to 15.4 W.
Warranty	Limited Lifetime Hardware Warranty

Compliance	**Standards** • **Safety:** ◦ UL 60950-1 ◦ CAN/CSA-C22.2 No. 60950-1 ◦ UL 2043 ◦ IEC 60950-1 ◦ EN 60950-1 • **Radio approvals:** ◦ FCC Part 15.247, 15.407 ◦ RSS-210 (Canada) ◦ EN 300.328, EN 301.893 (Europe) ◦ ARIB-STD 33 (Japan) ◦ ARIB-STD 66 (Japan) ◦ ARIB-STD T71 (Japan) ◦ AS/NZS 4268.2003 (Australia and New Zealand) ◦ EMI and susceptibility (Class B) ◦ FCC Part 15.107 and 15.109 ◦ ICES-003 (Canada) ◦ VCCI (Japan) ◦ EN 301.489-1 and -17 (Europe) ◦ EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC • **IEEE Standard:** ◦ IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11h, IEEE 802.11d • **Security:** ◦ 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA ◦ 802.1X ◦ Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP) • **EAP Type(s):** ◦ Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) ◦ EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) ◦ Protected EAP (PEAP) v0 or EAP-MSCHAPv2

Documentation PP6 : Cisco Catalyst 3650 Series Switches

Source : documentation constructeur Cisco Catalyst 3650 Series Switches

Product Overview

- Integrated wireless controller capability with:
  - Up to 40G of wireless capacity per switch (48-port models)
  - Support for up to 50 access points and 1000 wireless clients on each switching entity (switch or stack)
- 24 and 48 10/100/1000 data and PoE+ models with energy-efficient Ethernet (EEE) supported ports
- 24 and 48 100-Mbps and 1-, 2.5-, 5-, and 10-Gbps (multigigabit) Cisco UPOE and PoE+ models with EEE[1]
- Five fixed-uplink models with four Gigabit Ethernet, two 10 Gigabit Ethernet, four 10 Gigabit Ethernet, eight 10 Gigabit Ethernet, or two 40 Gigabit Ethernet Quad Small Form-Factor Pluggable Plus (QSFP+) ports
- 24-port and 48-port 10/100/1000 PoE+ models with lower noise and reduced depth of 11.62 inches for shallow depth cabinets in enterprise, retail, and branch-office environments
- Optional Cisco StackWise-160 technology that provides scalability and resiliency with 160 Gbps of stack throughput
- Dual redundant, modular power supplies and three modular fans providing redundancy[2]
- Support for external power system RPS 2300 on the 3650 mini SKUs for power redundancy
- Full IEEE 802.3at (PoE+) with 30W power on all ports in 1 rack unit (RU) form factor
- IEEE 802.3BZ (2.5GBASE-T and 5GBASE-T) to go beyond 1 Gbps with existing Category 5e and Category 6
- IEEE 802.1ba Audio Video Bridging (AVB) built in to provide a better AV experience, including improved time synchronization and quality of service (QoS)
- Software support for IPv4 and IPv6 routing, multicast routing, modular QoS, Flexible NetFlow (FNF) Version 9, and enhanced security features
- Single universal Cisco IOS® Software image across all license levels, providing an easy upgrade path for software features
- Enhanced limited lifetime warranty (E-LLW) with next business day (NBD) advance hardware replacement and 90-day access to Cisco Technical Assistance Center (TAC) support

Switch Models and Configurations

All Cisco Catalyst 3650 Series Switches have fixed, built-in uplink ports and ship with one power supply. Tables 1 through 5 provide further details. Figure 1 is an image of the Cisco Catalyst 3650 Series Switches.

Table 1 shows the Cisco Catalyst 3650 Series configurations.

Table 1. Cisco Catalyst 3650 Series Configurations

Models	Fixed Uplinks	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
WS-C3650-24TS	4 x Gigabit Ethernet with Small Form-Factor Pluggable (SFP)	24	250 WAC	-
WS-C3650-48TS		48		
WS-C3650-24PS		24 PoE+	640 WAC	390 W
WS-C3650-48PS		48 PoE+		
WS-C3650-48FS		48 PoE+	1025 WAC	775 W
WS-C3650-24TD	2 x 10 Gigabit Ethernet with SFP+ and 2 x 1 Gigabit Ethernet with SFP	24	250 WAC	
WS-C3650-48TD		48		
WS-C3650-24PD		24 PoE+	640 WAC	390 W
WS-C3650-24PDM		24 PoE+	Fixed 640 WAC	390 W
WS-C3650-48PD		48 PoE+	640 WAC	390 W
WS-C3650-48FD		48 PoE+	1025 WAC	775 W

Documentation PP7 : Le protocole MQTT

Pour répondre à la problématique du nombre grandissant d'objets connectés, l'IoT, s'est doté d'un nouveau standard : le protocole MQTT (Message Queuing Telemetry Transport).

MQTT est ouvert, simple, léger et facile à mettre en œuvre. Il est idéal pour répondre aux besoins suivants :

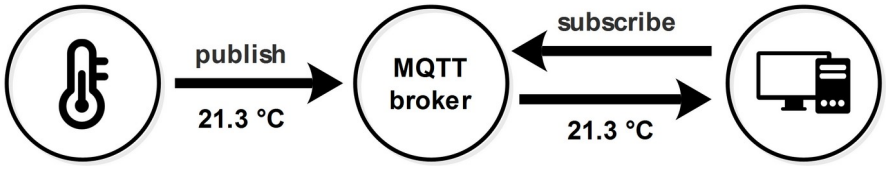
- faible consommateur en énergie ;
- très rapide, il permet un temps de réponse supérieur aux autres standards du web actuel ;
- permet une forte fiabilité si nécessaire ;
- nécessite peu de ressources processeurs et de mémoires ;
- légèreté : beaucoup moins verbeux que HTTP, avec un côté asynchrone natif.

MQTT est basé sur la suite de protocoles TCP/IP, utilisée par les protocoles internet dont HTTP. On peut donc le trouver sur n'importe quelle plateforme matérielle, que ce soit un microcontrôleur, un PC ou même un Cloud Microsoft Azure ou Amazon AWS.

Principe de fonctionnement :

MQTT est un **service de publication/abonnement** TCP/IP simple et extrêmement léger. Il fonctionne sur le principe **client/serveur**.

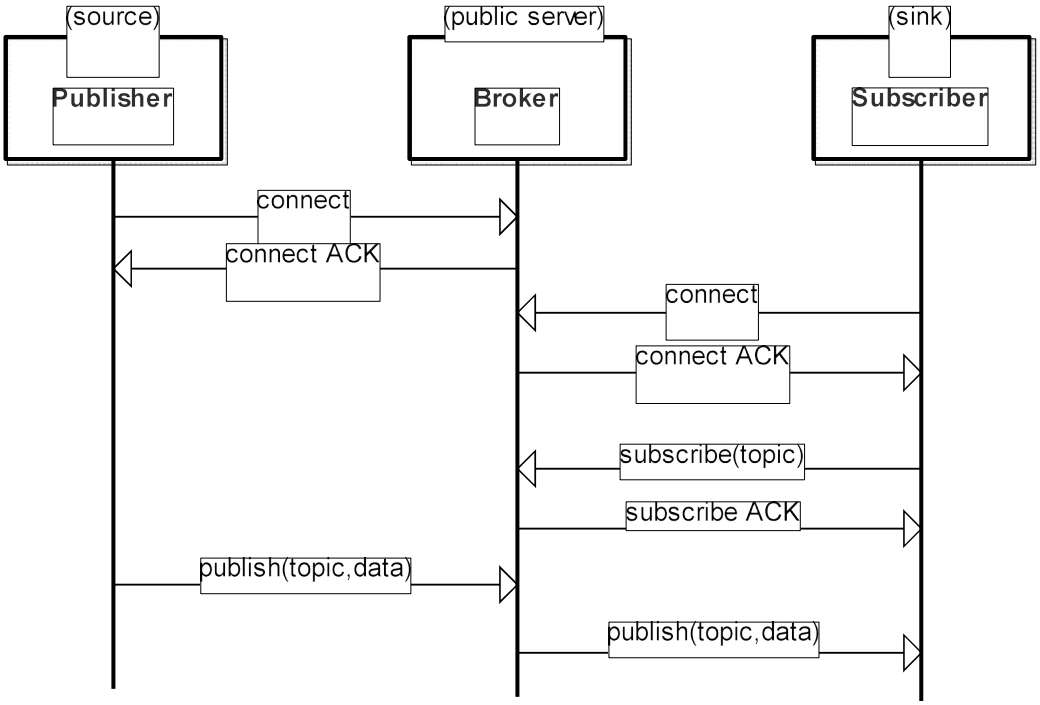
L'application réseau serveur, nommé **broker**, va collecter des informations que les éditeurs (**publishers**) vont lui transmettre. Certaines informations collectées par le broker seront renvoyées à certains abonnés (**subscribers**) en ayant préalablement fait la demande au broker. Un client peut être à la fois éditeur et abonné.



Les messages sont envoyés par les éditeurs sur un canal d'information appelé **topic**. Ces messages peuvent être lus par les abonnés. Les topics peuvent avoir une hiérarchie qui permet de sélectionner finement les informations que l'on désire.

Un topic est une chaîne de caractère. Il peut y avoir plusieurs niveaux de sujets séparés par un
« / ».

Exemples de topics : sensors/COMPUTER_NAME/temperature/HARDDRIVE_NAME
sensor/temperature/salon
sensor/temperature/#



Les messages sont constitués de 2 éléments :

- un « topic » ou identifiant du message **;**
- un « body » ou corps du message : les données du message qui peuvent se présenter sous différentes formes (binaire, chaine de caractères ou chaine avec encodage JSON par exemple). Les **messages** envoyés ne peuvent excéder une taille de **256 Mo**.

MQTT fonctionne sur **TCP/IP**. Le principal travail du broker est de servir de relais.