

Exemple de configuration de commutateur du contrôleur CT5760 et du Catalyst 3850

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[L'information générale pour le contrôleur sans-fil unifié d'Access CT5760](#)

[L'information générale pour les Commutateurs unifiés du Catalyst 3850 d'Access](#)

[Configuration initiale 5760 WLC](#)

[Configurez](#)

[Script d'installation](#)

[Configuration requise pour que les Points d'accès joignent](#)

[Vérifiez](#)

[Dépannez](#)

[Configuration initiale de 3850 commutateurs](#)

[Configurez](#)

[Script d'installation](#)

[Configuration requise pour que les Points d'accès joignent](#)

[Vérifiez](#)

[Dépannez](#)

Introduction

Ce document décrit les étapes pour installer et préparer des Services sans fil sur le commutateur 5760 le contrôleur LAN Sans fil (WLC) et 3850. Ce document couvre la configuration initiale et le processus de jonction du Point d'accès (AP) pour chacun des deux Plateformes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur Sans fil unifié de l'accès CT5760 - Version 3.02.02SE
- Commutateur unifié du Catalyst 3850 d'accès - Version 3.02.02SE

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

L'information générale pour le contrôleur sans-fil unifié d'Access CT5760

Le CT5760 WLC est le contrôleur articulé autour d'un logiciel du premier [®] de Cisco IOS XE construit avec l'ASIC intelligent destiné pour être déployé comme contrôleur centralisé en architecture Sans fil unifiée de la deuxième génération. La plate-forme prend en charge également la nouvelle fonctionnalité de mobilité avec les Commutateurs convergés de gamme 3850 d'accès.

Les contrôleurs CT5760 sont typiquement déployés près du noyau. Les ports uplinks connectés au principal commutateur peuvent être configurés en tant que ports de joncteur réseau d'EtherChannel pour assurer la Redondance de port. Ce nouveau contrôleur est un contrôleur sans-fil extensible et de hautes performances, qui peut mesurer jusqu'à 1000 aps et 12,000 clients. Le contrôleur a six ports de données de 10 Gbits/s pour une capacité totale de 60 GBP.

La gamme 5760 fonctionne en même temps que Cisco Aironet aps, l'infrastructure principale de Cisco, et l'engine de services de mobilité Cisco afin de prendre en charge des données Sans fil entreprise-essentielles, la Voix, le vidéo, et des applications de services d'emplacement.

L'information générale pour les Commutateurs unifiés du Catalyst 3850 d'Access

La gamme Cisco Catalyst 3850 est la nouvelle génération de commutateurs de la couche d'accès empilables de classe entreprise qui fournissent la pleine convergence entre de câble et radio sur une plate-forme unique. Actionné par le logiciel IOS-XE, le service sans fil est pris en charge par le contrôle et le ravitaillement du protocole des points d'accès sans fil (CAPWAP). Le nouveau plan de données unifié d'Access de Cisco (UADP) ASIC actionne l'application de stratégie de commutateur et de câbler-radio d'enable, la visibilité d'application, la flexibilité, et l'optimisation uniformes d'application. Cette convergence est établie sur la résilience de Cisco nouveau et amélioré StackWise-480. Alimentation d'IEEE 802.3at de support de Commutateurs de gamme Cisco Catalyst 3850 la pleine au-dessus des Ethernets plus (PoE+), des modules réseau modulaires et remplaçables sur place, des thermostats redondants, et des alimentations d'énergie.

Configuration initiale 5760 WLC

Cette section trace les grandes lignes des étapes pour configurer avec succès les 5760 WLC afin

de héberger des Services sans fil.

Configurez

Script d'installation

--- System Configuration Dialog ---

Enable secret warning

In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the
enable secret
If you choose not to enter the initial configuration dialog, or if you exit setup
without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>

Would you like to enter the initial configuration dialog? [yes/no]: **yes**

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: **yes**

Configuring global parameters:

Enter host name [Controller]: **w-5760-1**

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.

Enter enable secret: **cisco**

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.

Enter enable password: **cisco**

The virtual terminal password is used to protect
access to the router over a network interface.

Enter virtual terminal password: **cisco**

Configure a NTP server now? [yes]:

Enter ntp server address : **192.168.1.200**

Enter a polling interval between 16 and 131072 secs which is power of 2:**16**

Do you want to configure wireless network? [no]: **no**

Setup account for accessing HTTP server? [yes]: **yes**

Username [admin]: **admin**

Password [cisco]: **cisco**

Password is UNENCRYPTED.

Configure SNMP Network Management? [no]: **no**

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	NO	unset	up	up
GigabitEthernet0/0	unassigned	YES	unset	up	up
Tel/0/1	unassigned	YES	unset	up	up
Tel/0/2	unassigned	YES	unset	down	down
Tel/0/3	unassigned	YES	unset	down	down
Tel/0/4	unassigned	YES	unset	down	down
Tel/0/5	unassigned	YES	unset	down	down
Tel/0/6	unassigned	YES	unset	down	down

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface Vlan1:

Configure IP on this interface? [yes]: **yes**

IP address for this interface: **192.168.1.20**

Subnet mask for this interface [255.255.255.0] : **255.255.255.0**

Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Wireless management interface needs to be configured at startup
It needs to be mapped to an SVI that's not Vlan 1 (default)

Enter VLAN No for wireless management interface: **120**

Enter IP address :**192.168.120.94**

Enter IP address mask: **255.255.255.0**

Le script suivant de commande de configuration a été créé :

```
w-5760-1
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY^Q
enable password cisco
line vty 0 15
password cisco
ntp server 192.168.1.200 maxpoll 4 minpoll 4
username admin privilege 15 password cisco
no snmp-server
!
no ip routing

!
interface Vlan1
no shutdown
ip address 192.168.1.20 255.255.255.0
!
interface GigabitEthernet0/0
shutdown
no ip address
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface TenGigabitEthernet1/0/3
!
interface TenGigabitEthernet1/0/4
```

```

!
interface TenGigabitEthernet1/0/5
!
interface TenGigabitEthernet1/0/6
vlan 120
interface vlan 120
ip addr 192.168.120.94 255.255.255.0
exit
wireless management interface Vlan120
!
end

```

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

Enter your selection [2]: 2

```

Building configuration...
Compressed configuration from 2729 bytes to 1613 bytes[OK]
Use the enabled mode 'configure' command to modify this configuration.

```

Press RETURN to get started!

Configuration requise pour que les Points d'accès joignent

Remarque: Important - Assurez-vous que le commutateur a la commande correcte de démarrage sous la configuration globale. S'il a été extrait sur l'éclair, puis la **mémoire Flash système w-5760-1(config)#boot** : la commande de **démarrage packages.conf** est exigée.

1. Connectivité de configure network. Configurez l'interface connectée de TenGig au réseau fédérateur où la circulation CAPWAP d'arrivée/sortante. Dans cet exemple, l'interface utilisée est TenGigabitEthernet1/0/1. On permet VLAN 1 et VLAN 120.

```

interface
TenGigabitEthernet1/0/1
switchport trunk allowed vlan 1,120
switchport mode trunk
ip dhcp relay information trusted
ip dhcp snooping trust
Configurez le default route sortant : ip route 0.0.0.0 0.0.0.0
192.168.1.1

```

2. Configurez l'accès de Web. Le GUI peut être accédé à par l'intermédiaire des <ipaddress >/wireless de https://Les qualifications de connexion sont déjà définies dans le dialogue de configuration initiale.

```

username admin privilege 15 password cisco

```

3. Assurez que l'interface de gestion Sans fil est correctement configurée. wireless

```

management interface Vlan120
w-5760-1#sh run int vlan 120
Building configuration...

Current configuration : 62 bytes
!
interface Vlan120
ip address 192.168.120.94 255.255.255.0
end

```

w-5760-1#sh ip int br

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.20	YES	manual	up	up

Vlan120	192.168.120.94	YES	manual	up	up
GigabitEthernet0/0	unassigned	YES	unset	down	down
Te1/0/1	unassigned	YES	unset	up	up
Te1/0/2	unassigned	YES	unset	down	down
Te1/0/3	unassigned	YES	unset	down	down
Te1/0/4	unassigned	YES	unset	down	down
Te1/0/5	unassigned	YES	unset	down	down
Te1/0/6	unassigned	YES	unset	down	down
Capwap2	unassigned	YES	unset	up	up

w-5760-1#

4. Assurez qu'un permis actif est activé avec le compte approprié AP. Remarque: 1) les 5760 n'a pas lancé des niveaux de permis, l'image est déjà des ipservices. 2) les 5760 qui agit en tant que Mobility Controller (MC) peuvent prendre en charge jusqu'à 1000 aps. w-5760-1#license right-to-use activate apcount <count> slot 1 acceptEULA

5. Assurez que code de pays correct est configuré sur le WLC conformément au domaine réglementaire du pays qu'AP sont déployés dedans. w-5760-1#show wireless country configured

```
Configured Country.....: US - United States
Configured Country Codes
```

US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g Afin de modifier code de pays, sélectionnez ces commandes : w-5760-1(config)#ap dot11 24ghz shutdown

w-5760-1(config)#ap dot11 5ghz shutdown

w-5760-1(config)#ap country BE

Changing country code could reset channel and RRM grouping configuration.
If running in RRM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.

Are you sure you want to continue? (y/n)[y]: y

w-5760-1(config)#no ap dot11 24ghz shut

w-5760-1(config)#no ap dot11 5ghz shut

w-5760-1(config)#end

w-5760-1#wr

Building configuration...

Compressed configuration from 3564 bytes to 2064 bytes[OK]

w-5760-1#show wireless country configured

```
Configured Country.....: BE - Belgium
Configured Country Codes
```

BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g

6. Assurez-vous que les aps peuvent apprendre l'adresse IP du WLC (192.168.120.94 dans cet exemple) par l'intermédiaire de l'option 43 DHCP, des domaines name service (DN), ou de n'importe quel autre mécanisme de détection dans CAPWAP.

Vérifiez

Afin de s'assurer que les aps s'est joints, sélectionnez la commande de show ap summary :

w-5760-1#show ap summary

Number of APs: 1

Global AP User Name: Not configured

Global AP Dot1x User Name: Not configured

AP Name	AP Model	Ethernet MAC	Radio MAC	State
APa493.4cf3.232a	1042N	a493.4cf3.232a	10bd.186d.9a40	Registered

Dépannez

Utile met au point pour dépanner AP joignent des questions :

```
w-5760-1#debug capwap ap events
capwap/ap/events debugging is on
```

```
w-5760-1#debug capwap ap error
capwap/ap/error debugging is on
```

```
w-5760-1#debug dtls ap event
dtls/ap/event debugging is on
```

```
w-5760-1#debug capwap ios event
CAPWAP Event debugging is on
```

```
5760-1#debug capwap ios error
CAPWAP Error debugging is on
```

Configuration initiale de 3850 commutateurs

Cette section inclut la configuration exigée pour héberger des Services sans fil sur les 3850.

Configurez

Script d'installation

```
--- System Configuration Dialog ---
```

```
Enable secret warning
```

```
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted
for the enable secret
If you choose not to enter the initial configuration dialog, or if you
exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
```

```
-----
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].
```

```
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

```
Would you like to enter basic management setup? [yes/no]: yes
```

Configuring global parameters:

Enter host name [Switch]: **sw-3850-1**

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: **Cisco123**

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **Cisco123**

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: **Cisco123**

Do you want to configure country code? [no]: **yes**

Enter the country code[US]:**US**

Note : Enter the country code in which you are installing this 3850 Switch and the AP(s). If your country code is not recognized, enter one that is compliant with the regulatory domain of your own country

Setup account for accessing HTTP server? [yes]: **yes**

Username [admin]: **admin**

Password [cisco]: **cisco**

Password is UNENCRYPTED.

Configure SNMP Network Management? [no]: **no**

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	NO	unset	up	down
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet2/0/1	unassigned	YES	unset	down	down
GigabitEthernet2/0/2	unassigned	YES	unset	down	down
GigabitEthernet2/0/3	unassigned	YES	unset	down	down
...					
...					
...					
GigabitEthernet2/0/46	unassigned	YES	unset	down	down
GigabitEthernet2/0/47	unassigned	YES	unset	down	down
GigabitEthernet2/0/48	unassigned	YES	unset	up	up
GigabitEthernet2/1/1	unassigned	YES	unset	down	down
GigabitEthernet2/1/2	unassigned	YES	unset	down	down
GigabitEthernet2/1/3	unassigned	YES	unset	down	down
GigabitEthernet2/1/4	unassigned	YES	unset	down	down
Te2/1/1	unassigned	YES	unset	down	down
Te2/1/2	unassigned	YES	unset	down	down
Te2/1/3	unassigned	YES	unset	down	down
Te2/1/4	unassigned	YES	unset	down	down

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface Vlan1:

Configure IP on this interface? [yes]: **yes**

IP address for this interface: **192.168.1.2**

Subnet mask for this interface [255.255.255.0] : **255.255.255.0**

Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Ce script de commande de configuration a été créé :

```
hostname sw-3850-1
enable secret 4 vwcGVdcUZcRMCyxaH2U9Y/PTujsnQWPSbt.LFG8lhTw
enable password Cisco123
line vty 0 15
password Cisco123
  ap dot11 24ghz shutdown
  ap dot11 5ghz shutdown
  ap country US
  no ap dot11 24ghz shutdown
  no ap dot11 5ghz shutdown

username admin privilege 15 password 0 cisco
no snmp-server
!
no ip routing

!
interface Vlan1
no shutdown
ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/0
shutdown
no ip address
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
...
...
...
interface GigabitEthernet2/0/46
!
interface GigabitEthernet2/0/47
!
interface GigabitEthernet2/0/48
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface TenGigabitEthernet2/1/3
!
interface TenGigabitEthernet2/1/4
!
end
```

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

```
Enter your selection [2]: 2
The enable password you have chosen is the same as your enable secret.
This is not recommended. Re-enter the enable password.
Changing country code could reset channel and RRM grouping configuration.
If running in RRM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n)[y]: y
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
```

```
Building configuration...
Compressed configuration from 4414 bytes to 2038 bytes[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Press RETURN to get started!

Configuration requise pour que les Points d'accès joignent

Remarque: Important - Assurez-vous que la commande correcte de démarrage est configurée sous la configuration globale. S'il a été extrait sur l'éclair, puis le **commutateur de boot system tout l'éclair : la commande packages.conf** est exigée.

1. Configurez les conditions préalables Sans fil. Afin d'activer des Services sans fil, les 3850 doivent exécuter les **ipservices** ou le permis d'**ibase**.
2. Radio d'enable sur le commutateur. Remarque: Les aps doivent être connectés aux switchports de mode d'accès dans le même VLAN ! Gestion de radio d'enable `sw-3850-1(config)#wireless management interface vlan <1-4095>` Définissez MCMC doit être défini afin de permettre à des aps pour se joindre. Si ces 3850 seront MC, sélectionnez la commande de **contrôleur de mobilité sans fil** : `sw-3850-1(config)#wireless mobility controller` Remarque: Cette modification de configuration exige une réinitialisation ! Si ces 3850 fonctionne comme agent de mobilité (mA), alors indiquez-le l'adresse IP de MC avec cette commande : `sw-3850-1(config)#wireless mobility controller ip a.b.c.d` Et sur MC, sélectionnez ces commandes : `3850MC(config)#wireless mobility controller peer-group <SPG1>`

`3850MC(config)#wireless mobility controller peer-group <SPG1> member ip w.x.y.z`
3. Assurez la Disponibilité de permis. Assurez-vous que les permis actifs AP sont disponibles sur MC (le mA utilise les permis qui sont lancés sur MC) : Remarque: 1) les 3850 doivent exécuter des **ipservices** ou un permis d'**ibase** afin d'activer des Services sans fil sur les 3850. 2) les permis de compte AP sont appliqués chez MC, et automatiquement provisioned et sont imposés au mA. 3) les 3850 qui agit en tant que MC peuvent prendre en charge jusqu'à 50 aps. `sw-3850-1#show license right-to-use summary`

License Name	Type	Count	Period left
-----	-----	-----	-----
ipservices	permanent	N/A	Lifetime

```

apcount          base          1          Lifetime
apcount          adder         49         Lifetime
-----

```

```

License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 1

```

AP Count Licenses Remaining: 49 Afin de lancer le permis de compte AP sur les 3850, sélectionnez cette commande avec le compte requis AP sur MC :`sw-3850-1#license right-to-use activate apcount <count> slot <#> acceptEULA`

4. Configurez le processus de découverte AP. Pour que des aps joignent le contrôleur, la configuration switchport doit être placée comme port d'accès dans le VLAN Sans fil de Gestion : Si le VLAN 100 est utilisé pour l'interface de gestion Sans fil :

```

sw-3850-1(config)#interface gigabit1/0/10
sw-3850-1(config-if)#switchport mode access
sw-3850-1(config-if)#switchport access vlan 100

```

5. Configurez l'accès de Web. Le GUI peut être accédé à par l'intermédiaire de `https://<ipaddress>/wireless` Les qualifications de connexion sont déjà définies dans le dialogue de configuration initiale. `username admin privilege 15 password 0 cisco (username for Web access)`
6. Assurez-vous que code de pays approprié est configuré sur le commutateur conformément au domaine réglementaire du pays qu'AP sont déployés dedans. `sw-3850-1#show wireless country configured`

```

Configured Country.....: US - United States
Configured Country Codes

```

US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g Afin de modifier code de pays, sélectionnez ces commandes :

```

sw-3850-1(config)#ap dot11 24ghz shutdown
sw-3850-1(config)#ap dot11 5ghz shutdown

```

```

sw-3850-1(config)#ap country BE
Changing country code could reset channel and RRM grouping configuration.
If running in RRM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n)[y]: y

```

```

sw-3850-1(config)#no ap dot11 24ghz shut
sw-3850-1(config)#no ap dot11 5ghz shut
sw-3850-1(config)#end
sw-3850-1#wr

```

```

Building configuration...
Compressed configuration from 3564 bytes to 2064 bytes[OK]

```

```

sw-3850-1#show wireless country configured

```

```

Configured Country.....: BE - Belgium
Configured Country Codes
BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g

```

Vérifiez

Afin de s'assurer qu'AP s'est joint, sélectionnez la commande de `show ap summary` :

```

sw-3850-1#show ap summary

```

```

Number of APs: 1

```

Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured

AP Name	AP Model	Ethernet MAC	Radio MAC	State
APa493.4cf3.232a	1042N	a493.4cf3.231a	10bd.186e.9a40	Registered

Dépannez

Utile met au point pour dépanner AP joignent des questions :

```
sw-3850-1#debug capwap ap events  
capwap/ap/events debugging is on
```

```
sw-3850-1#debug capwap ap error  
capwap/ap/error debugging is on
```

```
sw-3850-1#debug dtls ap event  
dtls/ap/event debugging is on
```

```
sw-3850-1#debug capwap ios event  
CAPWAP Event debugging is on
```

```
sw-3850-1#debug capwap ios error  
CAPWAP Error debugging is on
```