Exemple de configuration du contrôleur CT5760 et du commutateur Catalyst 3850

Contenu

Introduction

Ce document décrit les étapes à suivre pour installer et préparer des services sans fil sur le contrôleur LAN sans fil (WLC) 5760 et le commutateur 3850. Ce document couvre la configuration initiale et le processus de jonction du point d'accès (AP) pour les deux plates-formes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Contrôleur sans fil Unified Access CT5760 - Version 3.02.02SE
- Commutateur Unified Access Catalyst 3850 - Version 3.02.02SE

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales pour le contrôleur sans fil Unified Access CT5760

Le WLC CT5760 est le premier contrôleur logiciel Cisco IOS-XE® conçu avec l'ASIC intelligent destiné à être déployé comme contrôleur centralisé dans l'architecture sans fil unifiée de nouvelle génération. La plate-forme prend également en charge la nouvelle fonctionnalité de mobilité avec les commutateurs de la gamme Converged Access 3850.

Les contrôleurs CT5760 sont généralement déployés près du coeur de réseau. Les ports de liaison ascendante connectés au commutateur principal peuvent être configurés en tant que ports de liaison EtherChannel pour garantir la redondance des ports. Ce nouveau contrôleur est un contrôleur sans fil extensible et hautes performances, qui peut évoluer jusqu'à 1 000 points d'accès et 12 000 clients. Le contrôleur dispose de six ports de données 10 Gbit/s pour une capacité totale de 60 Gbit/s.

La gamme 5760 fonctionne conjointement avec les points d'accès Cisco Aironet, l'infrastructure Cisco Prime et le moteur de services de mobilité Cisco afin de prendre en charge les applications stratégiques de services de données, voix, vidéo et localisation sans fil.

Informations générales sur les commutateurs Unified Access Catalyst 3850

La gamme Cisco Catalyst 3850 est la nouvelle génération de commutateurs de couche d'accès empilables d'entreprise qui assurent une convergence complète entre les réseaux filaires et sans fil sur une plate-forme unique. Optimisé par le logiciel IOS-XE, le service sans fil est pris en charge par le protocole CAPWAP (Control and Provisioning of Wireless Access Points). Le nouvel ASIC du plan de données d'accès unifié (UADP) de Cisco alimente le commutateur et permet l'application uniforme des politiques filaire-sans fil, la visibilité des applications, la flexibilité et l'optimisation des applications. Cette convergence repose sur la résilience du nouveau Cisco StackWise-480 amélioré. Les commutateurs de la gamme Cisco Catalyst 3850 prennent en charge la norme IEEE 802.3at Power over Ethernet Plus (PoE+) complète, des modules de réseau modulaires et remplaçables sur site, des ventilateurs redondants et des alimentations.

Configuration initiale du WLC 5760

Cette section décrit les étapes à suivre pour configurer correctement le WLC 5760 afin d'héberger des services sans fil.

Configuration

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 intial 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
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

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 de commande de configuration suivant 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 la participation des points d'accès

Note: Important : assurez-vous que la commande boot du commutateur est correcte dans la configuration globale. S'il a été extrait sur la mémoire Flash, la commande **w-5760-1(config)#boot system flash:packages.conf** boot est requise.

1. Configurez la connectivité réseau.Configurez l'interface TenGig connectée au réseau fédérateur où le trafic CAPWAP circule en entrée/sortie. Dans cet exemple, l'interface utilisée est TenGigabitEthernet1/0/1. Les VLAN 1 et 120 sont autorisés.
   ```
   interface TenGigabitEthernet1/0/1
   switchport trunk allowed vlan 1,120
   switchport mode trunk
   ip dhcp relay information trusted
   ip dhcp snooping trust
   ```
   Configurez la route sortante par défaut :
   ```
   ip route 0.0.0.0 0.0.0.0 192.168.1.1
   ```
2. Configurez l'accès Web.L'interface utilisateur graphique est accessible via https://<*ipaddress*>/wirelessLes informations d'identification de connexion sont déjà définies dans la boîte de dialogue de configuration initiale.
   ```
   username admin privilege 15 password cisco
   ```
3. Vérifiez 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-vous qu'une licence active est activée avec le nombre d'AP approprié.**Note**: 1) Le 5760 n'a pas de niveaux de licence activés, l'image est déjà ipservices. 2) Le 5760 qui agit en tant que contrôleur de mobilité (MC) peut prendre en charge jusqu'à 1 000 points d'accès.
   w-5760-1#license right-to-use activate apcount <*count*> slot 1 acceptEULA
5. Assurez-vous que le code de pays correct est configuré sur le WLC conformément au domaine réglementaire du pays dans lequel les points d'accès sont déployés.
   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 le code de pays, entrez les commandes suivantes :

```
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 AP sont capables d'apprendre l'adresse IP du WLC (192.168.120.94 dans cet exemple) via l'option DHCP 43, Domain Name Services (DNS), ou tout autre mécanisme de détection dans CAPWAP.

Vérification

Afin de s'assurer que les AP ont rejoint, entrez la commande **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
```

Dépannage

Débogages utiles pour dépanner les problèmes de jointure des points d'accès :

```
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 du commutateur 3850

Cette section inclut la configuration requise pour héberger des services sans fil sur le 3850.

Configuration

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 intial 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 la participation des points d'accès

> **Note**: Important : assurez-vous que la commande boot correcte est configurée dans la configuration globale. S'il a été extrait sur la mémoire Flash, la commande **boot system switch all flash:packages.conf** est requise.

1. Configurez les conditions requises pour le sans fil.Pour activer les services sans fil, le 3850 doit exécuter une licence **ipservices ou ipbase**.
2. Activez le sans fil sur le commutateur.**Note**: Les points d'accès doivent être connectés aux ports de commutation du mode d'accès dans le même VLAN !Activer la gestion sans fil
   `sw-3850-1(config)#wireless management interface vlan <1-4095>`
   Définir le MCUn MC doit être défini afin de permettre aux AP de se joindre.Si ce 3850 est MC, entrez la commande **wireless mobility controller** :
   `sw-3850-1(config)#wireless mobility controller`
   Note: Cette modification de configuration nécessite un redémarrage !Si ce 3850 fonctionne en tant qu'agent de mobilité (MA), pointez-le sur l'adresse IP de MC à l'aide de la commande suivante :
   `sw-3850-1(config)#wireless mobility controller ip a.b.c.d`
   Et sur MC, entrez ces commandes :
   `3850MC(config)#wireless mobility controller peer-group`

```
3850MC(config)#wireless mobility controller peer-group
```

3. Garantir la disponibilité des licences.Assurez-vous que les licences PA actives sont disponibles sur le MC (l'EM utilise les licences activées sur le MC) :**Note**: 1) Le 3850 doit exécuter ipservices ou une licence ipbase pour activer les services sans fil sur le 3850. 2) Les licences de nombre de points d'accès sont appliquées au MC et sont automatiquement provisionnées et appliquées au MA. 3) Le 3850 qui agit en tant que MC peut prendre en charge jusqu'à 50 points d'accès.

```
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 d'activer la licence de nombre d'AP sur le 3850, entrez cette commande avec le nombre d'AP requis sur le MC :

```
sw-3850-1#license right-to-use activate apcount
```

4. Configurez le processus de détection des points d'accès.Pour que les points d'accès rejoignent le contrôleur, la configuration du port de commutateur **doit être définie en tant que port d'accès** dans le VLAN de gestion sans fil :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 Web.L'interface utilisateur graphique est accessible via https://<adresse IP>/sans filLes informations d'identification de connexion sont déjà définies dans la boîte de dialogue de configuration initiale.

```
username admin privilege 15 password 0 cisco ( username for Web access)
```

6. Assurez-vous que le code de pays approprié est configuré sur le commutateur conformément au domaine réglementaire du pays dans lequel les points d'accès sont déployés.

```
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 le code de pays, entrez les commandes suivantes :

```
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
```

Vérification

Afin de s'assurer que le ou les AP ont rejoint, entrez la commande **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
```

Dépannage

Débogages utiles pour dépanner les problèmes de jointure des points d'accès :

```
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
```