

Ejemplo de Configuración del Controlador CT5760 y del Switch Catalyst 3850

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Información general del controlador inalámbrico Unified Access CT5760](#)

[Información general sobre los switches Catalyst 3850 de Unified Access](#)

[5760 Configuración Inicial del WLC](#)

[Configurar](#)

[Guión de configuración](#)

[Configuración necesaria para que los puntos de acceso se unan](#)

[Verificación](#)

[Troubleshoot](#)

[Configuración inicial del switch 3850](#)

[Configurar](#)

[Guión de configuración](#)

[Configuración necesaria para que los puntos de acceso se unan](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe los pasos para instalar y preparar servicios inalámbricos en el controlador de LAN inalámbrica 5760 (WLC) y el switch 3850. Este documento cubre la configuración inicial y el proceso de unión del punto de acceso (AP) para ambas plataformas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador inalámbrico Unified Access CT5760 - Versión 3.02.02SE
- Switch Catalyst 3850 de Unified Access - Versión 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.

Información general del controlador inalámbrico Unified Access CT5760

El CT5760 WLC es el primer controlador basado en software Cisco IOS-XE® construido con ASIC inteligente y diseñado para implementarse como un controlador centralizado en la arquitectura inalámbrica unificada de próxima generación. La plataforma también es compatible con la nueva funcionalidad de movilidad con los switches de acceso convergente serie 3850.

Los controladores CT5760 se suelen implementar cerca del núcleo. Los puertos de enlace ascendente conectados al switch principal se pueden configurar como puertos troncales EtherChannel para garantizar la redundancia de puerto. Este nuevo controlador es un controlador inalámbrico extensible y de alto rendimiento, que puede ampliarse hasta 1000 AP y 12 000 clientes. El controlador tiene seis puertos de datos de 10 Gbps para una capacidad total de 60 Gbps.

La serie 5760 funciona junto con los puntos de acceso Cisco Aironet, Cisco Prime Infrastructure y Cisco Mobility Services Engine para admitir aplicaciones de servicios de ubicación, vídeo, voz y datos inalámbricos fundamentales para la empresa.

Información general sobre los switches Catalyst 3850 de Unified Access

Cisco Catalyst serie 3850 es la última generación de switches apilables de nivel de acceso de clase empresarial que proporcionan una convergencia completa entre redes por cable e inalámbricas en una única plataforma. Con la tecnología del software IOS-XE, el servicio inalámbrico es compatible con el protocolo de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP). El nuevo ASIC de plano de datos de Unified Access (UADP) de Cisco alimenta el switch y permite la aplicación uniforme de políticas por cable e inalámbricas, la visibilidad de las aplicaciones, la flexibilidad y la optimización de las aplicaciones. Esta convergencia se basa en la resistencia de la nueva y mejorada Cisco StackWise-480. Los switches Catalyst de Cisco serie 3850 admiten alimentación a través de Ethernet Plus (PoE+) IEEE 802.3at completa, módulos de red modulares y reemplazables in situ, ventiladores redundantes y fuentes de alimentación.

5760 Configuración Inicial del WLC

Esta sección describe los pasos para configurar correctamente el WLC 5760 para alojar servicios

inalámbricos.

Configurar

Guión de configuración

--- 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**

Se creó el siguiente script de comando de configuración:

```
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!

Configuración necesaria para que los puntos de acceso se unan

Nota: Importante: asegúrese de que el switch tenga el comando de inicio correcto en la configuración global. Si se ha extraído en la memoria flash, se requiere el comando **w-5760-1(config)#boot system flash:packages.conf boot**.

1. Configure la conectividad de red. Configure la interfaz TenGig conectada a la red de estructura básica donde el tráfico CAPWAP fluye de entrada/salida. En este ejemplo, la interfaz utilizada es TenGigabitEthernet1/0/1. Se permiten VLAN 1 y VLAN 120.

```

interface TenGigabitEthernet1/0/1
switchport trunk allowed vlan 1,120
switchport mode trunk
ip dhcp relay information trusted
ip dhcp snooping trust

```

Configure la ruta de salida predeterminada:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

2. Configure el acceso web. Se puede acceder a la GUI a través de <https://<ipaddress>/wireless> Las credenciales de inicio de sesión ya están definidas en el diálogo de configuración inicial.

```
username admin privilege 15 password cisco
```

3. Asegúrese de que la interfaz de administración inalámbrica está configurada correctamente.

```

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. Asegúrese de que una licencia activa esté habilitada con el conteo de AP adecuado. **Nota:** 1) El 5760 no tiene niveles de licencia activados, la imagen ya es ipservices. 2) El 5760 que actúa como controlador de movilidad (MC) puede admitir hasta 1000 AP.

```
w-5760-1#license right-to-use activate apcount <count> slot 1 acceptEULA
```

5. Asegúrese de que el código de país correcto esté configurado en el WLC de conformidad con el dominio regulador del país en el que se implementan los AP.

```
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
```

Para modificar el código del país, ingrese estos comandos:

```
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. Asegúrese de que los AP puedan aprender la dirección IP del WLC (192.168.120.94 en este ejemplo) a través de la opción DHCP 43, Servicios de nombres de dominio (DNS) o cualquier otro mecanismo de detección en CAPWAP.

Verificación

Para asegurarse de que los AP se han unido, ingrese el comando **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

Troubleshoot

Depuraciones útiles para resolver problemas de unión de AP:

```
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
```

Configuración inicial del switch 3850

Esta sección incluye la configuración necesaria para alojar servicios inalámbricos en el 3850.

Configurar

Guión de configuración

```
--- 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

Se creó este script de comando de configuración:

```
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!

Configuración necesaria para que los puntos de acceso se unan

Nota: Importante: asegúrese de que el comando de arranque correcto esté configurado en la configuración global. Si se ha extraído en la memoria flash, se requiere el comando **boot system switch all flash:packages.conf**.

1. Configure los requisitos previos inalámbricos. Para habilitar los servicios inalámbricos, el 3850 debe ejecutar una licencia **ipservices** o **ipbase**.
2. Active la función inalámbrica en el switch. **Nota:** Los AP deben estar conectados a los puertos de switch del modo de acceso en la misma VLAN. Habilitar la gestión inalámbrica
`sw-3850-1(config)#wireless management interface vlan <1-4095>`

Definir el MC Se debe definir un MC para permitir que los AP se unan. Si este 3850 será el MC, ingrese el comando **wireless mobility controller**:

```
sw-3850-1(config)#wireless mobility controller
```

Nota: Este cambio de configuración requiere un reinicio. Si este 3850 funciona como agente de movilidad (MA), señale la dirección IP de MC con este comando:

```
sw-3850-1(config)#wireless mobility controller ip a.b.c.d
```

Y en el MC, ingrese estos comandos:

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

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

- Garantizar la disponibilidad de la licencia. Asegúrese de que las licencias AP activas estén disponibles en el MC (el MA utiliza las licencias activadas en el MC): **Nota:** 1) El 3850 debe ejecutar ipservices o una licencia ipbase para habilitar los servicios inalámbricos en el 3850. 2) Las licencias de conteo de AP se aplican en el MC y se aprovisionan y aplican automáticamente en el MA. 3) El 3850 que actúa como MC puede soportar hasta 50 AP.

```
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
```

Para activar la licencia de conteo AP en el 3850, ingrese este comando con el conteo AP requerido en el MC:

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

- Configure el proceso de detección de AP. Para que los AP se unan al controlador, la configuración del switchport **debe configurarse como un puerto de acceso** en la vlan de administración inalámbrica. Si vlan 100 se utiliza para la interfaz de administración inalámbrica:

```
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
```

- Configure el acceso web. Se puede acceder a la GUI a través de <https://<ipaddress>/wireless> Las credenciales de inicio de sesión ya están definidas en el diálogo de configuración inicial.
`username admin privilege 15 password 0 cisco (username for Web access)`
- Asegúrese de que el código de país adecuado esté configurado en el switch de conformidad con el dominio regulador del país en el que se implementan los AP.

```
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
```

Para modificar el código del país, ingrese estos comandos:

```
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

```

Verificación

Para asegurarse de que los AP se han unido, ingrese el comando **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

```

Troubleshoot

Depuraciones útiles para resolver problemas de unión de AP:

```

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

```