Ejemplo de configuración del regulador CT5760 y del Catalyst 3850 Switch

Contenido

Introducción

Este documento describe los pasos para instalar y para preparar los Servicios inalámbricos en el regulador del Wireless LAN 5760 (WLC) y el 3850 Switch. Esta configuración inicial de los documentos abarca y el punto de acceso se unen al proceso para ambas Plataformas.

Prerrequisitos

Requisitos

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.

- Regulador inalámbrico unificado del acceso CT5760 - Versión 3.02.02SE
- Catalyst 3850 Switch unificado del acceso - Versión 3.02.02SE

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Información previa para el regulador unificado de la Tecnología inalámbrica del acceso CT5760

El WLC CT5760 es el regulador basado en software del primer ® del Cisco IOS XE construido con ASIC elegante previsto para ser desplegado como regulador centralizado en la arquitectura inalámbrica unificada última generación. La plataforma también soporta las nuevas funciones de la movilidad con los 3850 Series Switch convergidos del acceso.

Los reguladores CT5760 se despliegan típicamente cerca de la base. Los puertos de link ascendente conectados con el switch del núcleo se pueden configurar como puertos de tronco EtherChannel para asegurar la redundancia del puerto. Este nuevo regulador es un regulador inalámbrico extensible y del rendimiento alto, que puede escalar hasta 1000 AP y a 12,000 clientes. El regulador tiene seis puertos de los datos del 10 Gbps por una capacidad total de 60 Gbps.

Las 5760 Series trabajan conjuntamente con el Cisco Aironet AP, la infraestructura primera de Cisco, y el motor de los Servicios de movilidad de Cisco para soportar los datos de red inalámbrica del negocio crítico, la Voz, el vídeo, y las aplicaciones de servicios de ubicación.

Información previa para los Catalyst 3850 Switch unificados del acceso

Las Cisco Catalyst 3850 Series son la última generación de switches de capa de acceso apilables de la empresa-clase que proporcionen la convergencia completa entre atado con alambre y Tecnología inalámbrica en una plataforma única. Accionado por el software IOS-XE, soportan al servicio de red inalámbrica con el control y el aprovisionamiento del protocolo de los untos de acceso de red inalámbrica (CAPWAP). El nuevo avión unificado de los datos del acceso de Cisco (UADP) ASIC acciona el Switch y los permisos uniforman la aplicación de políticas de la atar con alambre-Tecnología inalámbrica, la visibilidad de la aplicación, la flexibilidad, y la optimización de la aplicación. Esta convergencia se emplea la resistencia de Cisco nuevo y mejorado StackWise-480. El poder completo de IEEE 802.3at del soporte de los Cisco Catalyst 3850 Series Switch sobre los Ethernetes más (PoE+), módulos de red modulares y reemplazables en el terreno, fans redundantes, y fuentes de alimentación.

Configuración inicial del WLC 5760

Esta sección delinea los pasos para configurar con éxito los 5760 WLC para recibir los Servicios inalámbricos.

Configurar

Secuencia de comandos 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 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
```

El script siguiente del comando configuration fue creado:

```
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 Puntos de acceso se unan a

Nota: Importante - Asegúrese de que el Switch tenga el comando boot correcto bajo configuración global. Si se ha extraído en el flash, entonces el **FLASH de sistema w-5760-1(config)#boot:** requieren al **comando boot packages.conf**.

1. Conectividad de red de la configuración.Configure la interfaz de TenGig conectada con la red de estructura básica en donde los flujos de tráfico CAPWAP entrantes/salientes. En este ejemplo, la interfaz usada es TenGigabitEthernet1/0/1. Se permiten el VLAN1 y el VLA N 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 predeterminado saliente:**ip route 0.0.0.0 0.0.0.0 192.168.1.1**
2. Configure el Acceso Web.El GUI se puede acceder vía los <ipaddress >/wireless de https://Los credenciales de inicio de sesión se definen ya en el diálogo de configuración inicial.**username admin privilege 15 password cisco**
3. Asegúrese que la interfaz de administración inalámbrica esté 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 que una licencia activa esté habilitada con la cuenta apropiada AP.Nota: 1) los 5760 no ha activado los niveles de la licencia, la imagen es ya ipservices. 2) los 5760 que actúa como regulador de la movilidad (MC) pueden soportar hasta 1000 AP.**w-5760-1#license right-to-use activate apcount <*count*> slot 1 acceptEULA**
5. Asegúrese que el código del país correcto esté configurado en el WLC de acuerdo con el dominio regulador del país que los AP se despliegan adentro. 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) vía la opción DHCP 43, los servicios de nombre del dominio (DNS), o cualquier otro mecanismo de detección en CAPWAP.

Verificación

Para asegurarse de que los AP se hayan unido a, 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
```

Troubleshooting

Los debugs útiles para resolver problemas el AP se unen a los problemas:

```
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 3850 Switch

Esta sección incluye la configuración requerida recibir los Servicios inalámbricos en los 3850.

Configurar

Secuencia de comandos 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 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
```

Este script del comando configuration fue creado:

```
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 Puntos de acceso se unan a

> Nota: Importante - Asegúrese de que configuren al comando boot correcto bajo configuración global. Si se ha extraído en el flash, después el **Switch del sistema del inicio todo el flash:** se requiere el **comando packages.conf**.

1. Requisitos previos de la Tecnología inalámbrica de la configuración.Para habilitar los Servicios inalámbricos, los 3850 deben ejecutar los **ipservices o la** licencia del **ipbase**.
2. Tecnología inalámbrica del permiso en el Switch.Nota: ¡Los AP necesitan ser conectados con los switchports del modo de acceso en el mismo VLA N!Administración de la Tecnología inalámbrica del permiso `sw-3850-1(config)#`**`wireless management interface vlan <1-4095>`**Defina el MCUn MC se debe definir para permitir que los AP se unan a.Si estos 3850 son el MC, ingrese el **comando controller sin hilos de la movilidad**:`sw-3850-1`**`(config)#wireless mobility controller`**Nota: ¡Este cambio de configuración requiere una reinicialización!Si estos 3850 actúa como agente de la movilidad (MA), después señálelo a la dirección IP 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 <SPG1>`**

   `3850MC(config)#`**`wireless mobility controller peer-group <SPG1> member ip w.x.y.z`**
3. Asegure la Disponibilidad de la licencia.Asegúrese de que las licencias activas AP estén disponibles en el MC (el MA utiliza las licencias que se activan en el MC):Nota: 1) los 3850 deben ejecutar los ipservices o una licencia del ipbase para habilitar los Servicios inalámbricos en los 3850. 2) las licencias de la cuenta AP son aplicadas en el MC, y son automáticamente aprovisionado y aplicado en el MA. 3) los 3850 que actúa como MC pueden 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 la cuenta AP en los 3850, ingrese este comando con la cuenta requerida AP en el MC:`sw-3850-1#`**`license right-to-use activate apcount <count> slot <#> acceptEULA`**

4. Configure el proceso de detección AP.Para que los AP se unan al regulador, la configuración de puerto de switch **se debe fijar como puerto de acceso** en la Administración inalámbrica vlan:Si el 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`**
5. Acceso Web de la configuración.El GUI se puede acceder vía https://<ipaddress>/wirelessLos credenciales de inicio de sesión se definen ya en el diálogo de configuración inicial.**`username admin privilege 15 password 0 cisco`** `( username for Web access)`
6. Asegúrese de que el código del país apropiado esté configurado en el Switch de acuerdo con el dominio regulador del país que los AP se despliegan adentro. `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 el AP se haya unido a, 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
```

Troubleshooting

Los debugs útiles para resolver problemas el AP se unen a los problemas:

```
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
```