

# CT5760 controller en Catalyst 3850 switch

## Configuratievoorbeeld

### Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie voor de Unified Access CT5760 draadloze controller](#)

[Achtergrondinformatie voor Unified Access Catalyst 3850-switches](#)

[5760 WLC initiële configuratie](#)

[Configureren](#)

[Naschrift instellen](#)

[Vereiste configuratie voor access points voor gebruik](#)

[Verifiëren](#)

[Problemen oplossen](#)

[3850 switch - eerste configuratie](#)

[Configureren](#)

[Naschrift instellen](#)

[Vereiste configuratie voor access points voor gebruik](#)

[Verifiëren](#)

[Problemen oplossen](#)

### Inleiding

Dit document beschrijft de stappen om draadloze services te installeren en voorbereiden op de 5760 draadloze LAN-controller (WLC) en 3850-switch. Dit document bestrijkt de eerste configuratie en het access point (AP) wordt gebruikt in het proces voor beide platforms.

### Voorwaarden

#### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Unified Access CT5760 draadloze controller - versie 3.02.02SE
- Unified Access Catalyst 3850 switch - versie 3.2.02SE

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## **Achtergrondinformatie voor de Unified Access CT5760 draadloze controller**

De CT5760 WLC is de eerste Cisco IOS-XE<sup>®</sup> software-gebaseerde controller die met slimme ASIC is gebouwd en die is bedoeld om te worden ingezet als gecentraliseerde controller in de volgende generatie Unified draadloze architectuur. Het platform ondersteunt ook de nieuwe mobiliteitsfunctionaliteit met geconvergeerde Access 3850 Series switches.

CT5760 controllers worden doorgaans ingezet in de buurt van de kern. De uplink-poorten die op de kernschakelaar zijn aangesloten, kunnen als EtherChannel-boomstampoorten worden geconfigureerd om poortredundantie te waarborgen. Deze nieuwe controller is een uitbreidbare en hoogwaardige draadloze controller, die kan opschalen tot 1000 AP's en 12.000 klanten. De controller heeft zes 10 Gbps gegevenspoorten voor een totale capaciteit van 60 Gbps.

De 5760 Series werken in combinatie met Cisco Aironet APs, Cisco Prime-infrastructuur en de Cisco Mobility Services Engine om bedrijfskritische draadloze data-, spraak-, video- en locatieservices te ondersteunen.

## **Achtergrondinformatie voor Unified Access Catalyst 3850-switches**

Cisco Catalyst 3850 Series is de volgende generatie van stapelbare access-laagswitches van bedrijfsklasse die volledige convergentie tussen bekabeld en draadloos op één platform bieden. Draadloze service wordt ondersteund door het protocol Control en Provisioning of Wireless Access Point (CAPWAP). Cisco's nieuwe Unified Access Data Plane (UADP) ASIC stelt de switch in staat en maakt een uniforme bekabelde draadloze beleidshandhaving, zichtbaarheid van toepassingen, flexibiliteit en optimalisatie van toepassingen mogelijk. Deze convergentie is gebaseerd op de veerkracht van de nieuwe en verbeterde Cisco StackWise-480. De Cisco Catalyst 3850 Series-switches ondersteunen volledige IEEE 802.3at Power over Ethernet Plus (PoE+), modulaire en veldvervangbare netwerkmodules, redundante ventilatoren en voedingen.

## **5760 WLC initiële configuratie**

In dit gedeelte worden de stappen beschreven om de 5760 WLC met succes te configureren zodat er draadloze services kunnen worden gehost.

# Configureren

## Naschrift instellen

--- 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**

Het volgende configuratie commando script is gecreëerd:

```
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!

## Vereiste configuratie voor access points voor gebruik

Opmerking: Belangrijk - Zorg ervoor dat de schakelaar de juiste boogopdracht onder mondiale configuratie heeft. Als deze op de flitser is afgeleid, dan is de **w-5760-1 (configuratie)#bootsysteemflitser:Pkets.conf** laars opdracht vereist.

1. Netwerkconnectiviteit configureren. Configureer de TenGig interface die is aangesloten op het backbone netwerk waar CAPWAP-verkeer naar binnen/naar buiten stroomt. In dit voorbeeld is de interface die wordt gebruikt TenGigabit Ethernet1/0/1. VLAN 1 en VLAN 120 zijn toegestaan.

```

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

```

Configureer de standaardroute naar buiten:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

2. Configuratie van web toegang. De GUI kan worden geraadpleegd via <https://<ipaddress>/Wireless> De aanmeldingsgegevens zijn al gedefinieerd in het dialoogvenster eerste configuratie.

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

3. Zorg ervoor dat de draadloze beheerinterface correct is geconfigureerd.

```

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. Zorg ervoor dat een actieve licentie is ingeschakeld met de juiste AP-telling. Opmerking: 1) De 5760 heeft geen actieve licentieniveaus, het beeld is al ipservices. 2) De 5760 die fungeert als een Mobility Controller (MC) kan maximaal 1000 AP's ondersteunen.

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

5. Zorg ervoor dat de juiste landcode op de WLC is ingesteld in overeenstemming met het wettelijk domein van het land waarin de AP(s) worden ingezet.

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
```

**U kunt de landcode als volgt wijzigen:**

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. Zorg ervoor dat APs het IP adres van de WLC (192.168.120.94 in dit voorbeeld) via DHCP optie 43, Domain Name Services (DNS) of een ander detectiemechanisme in CAPWAP kunnen leren.

## Verifiëren

Om ervoor te zorgen dat APs zich heeft aangesloten, voer de **samenvatting** van **show in**:

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

## Problemen oplossen

Handige oplossingen voor problemen:

```
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
```

## 3850 switch - eerste configuratie

Dit deel bevat de configuratie die vereist is om draadloze services te kunnen onderbrengen op de 3850.

## Configureren

### Naschrift instellen

```
--- 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

**Dit configuratiecommando script is gemaakt:**

```
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!

## Vereiste configuratie voor access points voor gebruik

Opmerking: Belangrijk - Zorg ervoor dat de juiste start-opdracht is geconfigureerd onder wereldwijde configuratie. Als deze op de flitser is afgeleid, moet het laarssysteem alle flitser:Packet.conf opdracht gebruiken.

1. Configureer de draadloze vereisten. Om draadloze services mogelijk te maken, moet de 3850 een **ipservices** of een basislicentie gebruiken.
2. Draadloze oplossingen aan de schakelaar inschakelen. Opmerking: APs moet worden aangesloten op toegangsmodus schakelpoorten in hetzelfde VLAN! Draadloos beheer inschakelen

```
sw-3850-1(config)#wireless management interface vlan <1-4095>
```

Bepaal de MCEr moet een MC worden gedefinieerd zodat AP's zich bij dit programma kunnen aansluiten. Als deze 3850 de MC is, voert u de opdracht **draadloze mobiliteitscontroller** in:

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

Opmerking: Deze configuratie moet opnieuw worden opgestart. Als deze 3850 werkt als een Mobility Agent (MA), dan richt u deze op het MC IP-adres met deze opdracht:

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

En op de MC, voer deze opdrachten in:

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

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

3. Zorg voor beschikbaarheid van licentie. Zorg ervoor dat actieve AP-licenties beschikbaar zijn op MC (de MA gebruikt de licenties die op MC zijn geactiveerd): Opmerking: 1) De 3850 moet ipservices of een ipbase-licentie uitvoeren om draadloze diensten op de 3850 mogelijk te maken. 2) AP-tellicenties worden toegepast op het MC, en worden automatisch voorzien en afgedwongen in het MA. 3) De 3850, dat als MC fungeert, kan maximaal 50 AP's ondersteunen.

```
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
```

Om de AP telling licentie op de 3850 te activeren, voert u deze opdracht in met de vereiste AP-telling op de MC:

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

4. Configuratie van het AP ontdekkingsproces. APs kunnen zich bij de controller aansluiten, **moet de switchpoortconfiguratie worden ingesteld als een toegangspoort** in het Wireless Management VLAN: Als VLAN 100 voor de draadloze beheerinterface wordt gebruikt:

```
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. Configuratie van web toegang. De GUI kan worden geraadpleegd via <https://<ipaddress>/Wireless> De aanmeldingsgegevens zijn al gedefinieerd in het dialoogvenster eerste configuratie.

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

6. Zorg ervoor dat de juiste landcode op de schakelaar is ingesteld in overeenstemming met het wettelijk domein van het land waarin de AP(s) zijn geïnstalleerd.

```
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
```

U kunt de landcode als volgt wijzigen:

```

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

```

## Verifiëren

Typ de opdracht **samenvatting** van de **show** om er zeker van te zijn dat er zich bij de AP(s) heeft aangesloten:

```

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

```

## Problemen oplossen

Handige oplossingen voor problemen:

```

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

```