Konfigurationsbeispiel für CT5760-Controller und Catalyst 3850-Switch

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen zum Unified Access CT5760 Wireless Controller](#)
[Hintergrundinformationen zu den Unified Access Catalyst Switches der Serie 3850](#)
[Erstkonfiguration des 5760 WLC](#)
[Konfigurieren](#)
[Setup-Skript](#)
[Erforderliche Konfiguration für die Teilnahme von Access Points](#)
[Überprüfen](#)
[Fehlerbehebung](#)
[Erstkonfiguration des 3850 Switches](#)
[Konfigurieren](#)
[Setup-Skript](#)
[Erforderliche Konfiguration für die Teilnahme von Access Points](#)
[Überprüfen](#)
[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Schritte zur Installation und Vorbereitung von Wireless-Services auf dem 5760 Wireless LAN Controller (WLC) und dem 3850 Switch. Dieses Dokument behandelt die Erstkonfiguration und den Prozess zum Verbinden von Access Points (AP) für beide Plattformen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Unified Access CT5760 Wireless Controller - Version 3.02.02SE
- Unified Access Catalyst 3850-Switch - Version 3.02.02SE

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen zum Unified Access CT5760 Wireless Controller

Der CT5760 WLC ist der erste softwarebasierte Cisco IOS-XE®-Controller mit intelligenten ASIC-Modulen, der als zentraler Controller in der Unified Wireless-Architektur der nächsten Generation eingesetzt werden soll. Die Plattform unterstützt außerdem die neue Mobilitätsfunktion mit den konvergenten Access Switches der Serie 3850.

CT5760-Controller werden in der Regel in der Nähe des Kerns bereitgestellt. Die mit dem Core-Switch verbundenen Uplink-Ports können als EtherChannel-Trunk-Ports konfiguriert werden, um die Port-Redundanz sicherzustellen. Dieser neue Controller ist ein erweiterbarer und hochleistungsfähiger Wireless-Controller, der bis zu 1.000 APs und 12.000 Clients skalieren kann. Der Controller verfügt über sechs 10-Gbit/s-Datenports für eine Gesamtkapazität von 60 Gbit/s.

Die Serie 5760 unterstützt in Verbindung mit Cisco Aironet APs, der Cisco Prime-Infrastruktur und der Cisco Mobility Services Engine geschäftskritische Wireless-Daten-, Sprach-, Video- und Standortdienste-Anwendungen.

Hintergrundinformationen zu den Unified Access Catalyst Switches der Serie 3850

Die Cisco Catalyst Switches der Serie 3850 sind die nächste Generation von Stackable Access-Layer-Switches der Enterprise-Klasse, die eine vollständige Konvergenz zwischen kabelgebundenen und Wireless-Netzwerken auf einer einzigen Plattform bieten. Der Wireless-Service wird durch die IOS-XE-Software unterstützt und wird durch das CAPWAP-Protokoll (Control and Provisioning of Wireless Access Points) unterstützt. Der neue Unified Access Data Plane (UADP)-ASIC von Cisco unterstützt den Switch und ermöglicht die einheitliche Durchsetzung von Richtlinien für kabelgebundene und Wireless-Netzwerke, Anwendungstransparenz, Flexibilität und Anwendungsoptimierung. Diese Konvergenz basiert auf der Ausfallsicherheit des neuen und verbesserten Cisco StackWise-480. Die Cisco Catalyst Switches der Serie 3850 unterstützen vollständige Power over Ethernet Plus (PoE+) nach IEEE 802.3at, modulare und vor Ort austauschbare Netzwerkmodule, redundante Lüfter und Netzteile.

Erstkonfiguration des 5760 WLC

In diesem Abschnitt werden die Schritte zur erfolgreichen Konfiguration des 5760 WLC zum

Hosten von Wireless-Services beschrieben.

Konfigurieren

Setup-Skript

```
         --- 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
```

Das folgende Konfigurationsbefehlskript wurde erstellt:

```
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!
```

Erforderliche Konfiguration für die Teilnahme von Access Points

Hinweis: Wichtig: Stellen Sie sicher, dass der Switch unter der globalen Konfiguration über den richtigen Boot-Befehl verfügt. Wenn sie im Flash-Speicher extrahiert wurde, ist der Befehl **w-5760-1(config)#boot system flash:packages.conf** boot erforderlich.

1. Konfigurieren Sie die Netzwerkverbindung.Konfigurieren Sie die mit dem Backbone-Netzwerk verbundene TenGig-Schnittstelle, über die der CAPWAP-Datenverkehr ein- und ausgeht. In diesem Beispiel wird die Schnittstelle TenGigabitEthernet1/0/1 verwendet. VLAN 1 und VLAN 120 sind zulässig.
   ```
   interface TenGigabitEthernet1/0/1
   switchport trunk allowed vlan 1,120
   switchport mode trunk
   ip dhcp relay information trusted
   ip dhcp snooping trust
   ```
   Konfigurieren Sie die Standardroute Outbound:
   ```
   ip route 0.0.0.0 0.0.0.0 192.168.1.1
   ```
2. Konfigurieren Sie den Webzugriff.Der Zugriff auf die Benutzeroberfläche erfolgt über https://<*IP-Adresse*>/wirelessDie Anmeldedaten werden bereits im Dialogfeld für die Erstkonfiguration definiert.
   ```
   username admin privilege 15 password cisco
   ```
3. Stellen Sie sicher, dass die Wireless-Verwaltungsschnittstelle korrekt konfiguriert ist.
   ```
    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. Stellen Sie sicher, dass eine aktive Lizenz mit der richtigen AP-Anzahl aktiviert ist.**Hinweis**: 1) Die 5760 hat nicht aktiviert Lizenzstufen, das Bild ist bereits ipservices. 2) Der 5760, der als Mobility Controller (MC) fungiert, kann bis zu 1.000 APs unterstützen.
   w-5760-1#license right-to-use activate apcount <*count*> slot 1 acceptEULA
5. Stellen Sie sicher, dass der richtige Ländercode auf dem WLC in Übereinstimmung mit der Zulassung des Landes konfiguriert ist, in dem die Access Points bereitgestellt werden.
   ```
   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
   ```
   Geben Sie die folgenden Befehle ein, um den Ländercode zu ändern:
   ```
   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. Stellen Sie sicher, dass die APs die IP-Adresse des WLC (in diesem Beispiel 192.168.120.94) über die DHCP-Option 43, Domain Name Services (DNS) oder einen anderen Erkennungsmechanismus in CAPWAP erfassen können.

Überprüfen

Geben Sie den Befehl **show ap summary** ein, um sicherzustellen, dass die APs beigetreten sind:

```
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
```

Fehlerbehebung

Hilfreiches Debuggen zur Fehlerbehebung bei Verbindungsproblemen mit dem Access Point:

```
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
```

Erstkonfiguration des 3850 Switches

Dieser Abschnitt enthält die erforderliche Konfiguration zum Hosten von Wireless-Services auf dem 3850.

Konfigurieren

Setup-Skript

```
         --- 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
```

Dieses Konfigurationsbefehlsskript wurde erstellt:

```
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!
```

Erforderliche Konfiguration für die Teilnahme von Access Points

> **Hinweis**: Wichtig: Stellen Sie sicher, dass der richtige Boot-Befehl unter der globalen Konfiguration konfiguriert ist. Wenn die Datei im Flash-Speicher extrahiert wurde, wird der Befehl **flash:packages.conf** benötigt.

1. Konfigurieren der Wireless-VoraussetzungenUm Wireless-Services zu aktivieren, muss der 3850 eine **ipservices- oder ipbase-**Lizenz ausführen.
2. Aktivieren Sie Wireless auf dem Switch.**Hinweis**: Die APs müssen mit Access-Mode-Switch-Ports im gleichen VLAN verbunden werden!Wireless-Management aktivieren
   `sw-3850-1(config)#wireless management interface vlan <1-4095>`
   Definieren des MCEin MC muss definiert werden, damit APs beitreten können.Wenn der 3850 das MC ist, geben Sie den Befehl **Wireless Mobility Controller** ein:
   `sw-3850-1(config)#wireless mobility controller`
   Hinweis: Diese Konfigurationsänderung erfordert einen Neustart!Wenn der 3850 als Mobility Agent (MA) fungiert, weisen Sie ihn mit dem folgenden Befehl auf die MC-IP-Adresse:
   `sw-3850-1(config)#wireless mobility controller ip a.b.c.d`
   Geben Sie auf dem MC die folgenden Befehle ein:
   `3850MC(config)#wireless mobility controller peer-group`

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

3. Sicherstellen der LizenzverfügbarkeitStellen Sie sicher, dass aktive AP-Lizenzen auf dem MC verfügbar sind (der MA verwendet die auf dem MC aktivierten Lizenzen):**Hinweis**: 1) Der 3850 muss ipservices oder eine iBase-Lizenz ausführen, um Wireless-Services auf dem 3850 zu aktivieren. 2) Lizenzen für die AP-Zählung werden auf dem MC angewendet und automatisch bereitgestellt und bei der MA durchgesetzt. 3) Der 3850, der als MC fungiert, kann bis zu 50 APs unterstützen.

```
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
```

Um die AP-Zähllizenz für den 3850 zu aktivieren, geben Sie diesen Befehl mit der erforderlichen AP-Anzahl für das MC ein:

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

4. Konfigurieren Sie den AP-Erkennungsvorgang.Damit APs dem Controller beitreten können, **muss** die Switch-Port-Konfiguration **als Zugriffsport** im Wireless-Management-VLAN **festgelegt werden**:Wenn VLAN 100 für die Wireless-Verwaltungsschnittstelle verwendet wird:

```
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. Konfigurieren Sie den Webzugriff.Der Zugriff auf die Benutzeroberfläche erfolgt über https://<ipaddress>/wireless.Die Anmeldedaten werden bereits im Dialogfeld für die Erstkonfiguration definiert.

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

6. Stellen Sie sicher, dass der korrekte Ländercode auf dem Switch entsprechend der gesetzlichen Bestimmungen des Landes konfiguriert ist, in dem die Access Points bereitgestellt werden.

```
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
```

Geben Sie die folgenden Befehle ein, um den Ländercode zu ändern:

```
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
```

Überprüfen

Geben Sie den Befehl **show ap summary** ein, um sicherzustellen, dass die Access Points beigetreten sind:

```
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
```

Fehlerbehebung

Hilfreiches Debuggen zur Fehlerbehebung bei Verbindungsproblemen mit dem Access Point:

```
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
```