Esempio di configurazione del controller CT5760 e dello switch Catalyst 3850

Sommario

Introduzione

In questo documento viene descritto come installare e preparare i servizi wireless sul controller WLC (Wireless LAN Controller) 5760 e sullo switch 3850. Questo documento descrive la configurazione iniziale e il processo di join del punto di accesso (AP) per entrambe le piattaforme.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni generali sul controller wireless Unified Access CT5760

CT5760 WLC è il primo controller basato su software Cisco IOS-XE® progettato con ASIC intelligente per essere implementato come controller centralizzato nell'architettura wireless unificata di nuova generazione. La piattaforma supporta inoltre la nuova funzionalità di mobilità con gli switch Converged Access 3850 Series.

I controller CT5760 sono generalmente installati vicino al core. Le porte uplink collegate allo switch principale possono essere configurate come porte trunk EtherChannel per garantire la ridondanza delle porte. Questo nuovo controller è un controller wireless estensibile e ad alte prestazioni, scalabile fino a 1000 punti di accesso e 12.000 client. Il controller dispone di sei porte dati a 10 Gb/s per una capacità totale di 60 Gb/s.

La serie 5760 funziona in combinazione con Cisco Aironet AP, Cisco Prime Infrastructure e Cisco Mobility Services Engine per supportare applicazioni business-critical di servizi wireless di dati, voce, video e posizione.

Informazioni generali sugli switch Unified Access Catalyst 3850

Cisco Catalyst serie 3850 è la nuova generazione di switch a livello di accesso impilabili di classe enterprise che forniscono la convergenza completa tra wireless e cablati su un'unica piattaforma. Basato sul software IOS-XE, il servizio wireless è supportato dal protocollo CAPWAP (Control and Provisioning of Wireless Access Point). Il nuovo UADP (Unified Access Data Plane) ASIC di Cisco alimenta lo switch e consente l'applicazione uniforme delle policy wireless, la visibilità, la flessibilità e l'ottimizzazione delle applicazioni. Questa convergenza è basata sulla resilienza del nuovo e migliorato Cisco StackWise-480. Gli switch Cisco Catalyst serie 3850 supportano lo standard completo IEEE 802.3at Power over Ethernet Plus (PoE+), moduli di rete modulari e sostituibili sul campo, ventole e alimentatori ridondanti.

Configurazione iniziale 5760 WLC

In questa sezione vengono illustrati i passaggi per configurare correttamente il WLC 5760 in modo da ospitare i servizi wireless.

Configurazione

Script di installazione

```
         --- 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
```

Èstato creato lo script di comando di configurazione seguente:

```
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!
```

Configurazione richiesta per l'aggiunta dei punti di accesso

Nota: Importante - verificare che lo switch abbia il comando di avvio corretto nella configurazione globale. Se è stato estratto dalla memoria flash, è necessario usare il comando **w-5760-1(config)#boot system flash:packages.conf** boot.

1. Configurare la connettività di rete.Configurare l'interfaccia TenGig connessa alla rete backbone in cui il traffico CAPWAP passa in entrata/in uscita. Nell'esempio, l'interfaccia utilizzata è TenGigabit Ethernet1/0/1. La VLAN 1 e la VLAN 120 sono consentite.
   ```
   interface TenGigabitEthernet1/0/1
   switchport trunk allowed vlan 1,120
   switchport mode trunk
   ip dhcp relay information trusted
   ip dhcp snooping trust
   ```
   Configurare la route predefinita in uscita:
   ```
   ip route 0.0.0.0 0.0.0.0 192.168.1.1
   ```
2. Configurare l'accesso Web.Èpossibile accedere alla GUI tramite https://<*indirizzoIP*>/wirelessLe credenziali di accesso sono già definite nella finestra di dialogo di configurazione iniziale.
   ```
   username admin privilege 15 password cisco
   ```
3. Verificare che l'interfaccia di gestione wireless sia configurata correttamente.
   ```
    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. Accertarsi che sia abilitata una licenza attiva con il numero di punti di accesso corretto.**Nota:** 1) Lo switch 5760 non dispone di livelli di licenza attivati, l'immagine è già ipservices. 2) Lo switch 5760 che opera come controller di mobilità (MC) può supportare fino a 1000 punti di accesso.
   w-5760-1#license right-to-use activate apcount <*count*> slot 1 acceptEULA
5. Verificare che sul WLC sia configurato il codice paese corretto in conformità al dominio normativo del paese in cui sono distribuiti gli access point.
   ```
   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
   ```
   Per modificare il codice del paese, immettere i seguenti comandi:
   ```
   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. Verificare che gli access point siano in grado di imparare l'indirizzo IP del WLC (192.168.120.94 nell'esempio) tramite l'opzione DHCP 43, il DNS (Domain Name Services) o qualsiasi altro meccanismo di rilevamento in CAPWAP.

Verifica

Per verificare che gli access point siano stati aggiunti, immettere il 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
```

Risoluzione dei problemi

Debug utili per la risoluzione dei problemi di aggiunta all'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
```

Configurazione iniziale dello switch 3850

In questa sezione viene illustrata la configurazione necessaria per ospitare i servizi wireless sullo switch 3850.

Configurazione

Script di installazione

```
         --- 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
```

Script di comando di configurazione creato:

```
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!
```

Configurazione richiesta per l'aggiunta dei punti di accesso

> **Nota:** Importante - Verificare che nella configurazione globale sia configurato il comando di avvio corretto. Se è stato estratto sul flash, allora il comando **boot system switch all flash:packages.conf** è richiesto.

1. Configurare i prerequisiti wireless.Per abilitare i servizi wireless, sullo switch 3850 è necessario eseguire una licenza **ipservices o ipbase**.
2. Attivare la modalità wireless sullo switch.**Nota:** I punti di accesso devono essere collegati alle porte di commutazione della modalità di accesso nella stessa VLAN.Abilita gestione wireless
   ```
   sw-3850-1(config)#wireless management interface vlan <1-4095>
   ```
   Definire l'MCPer consentire ai punti di accesso di unirsi, è necessario definire un MC.Se questo switch 3850 è il MC, immettere il comando **wireless mobility controller**:
   ```
   sw-3850-1(config)#wireless mobility controller
   ```
   Nota: La modifica della configurazione richiede il riavvio del sistema.Se lo switch 3850 funziona come agente di mobilità (MA), puntarlo all'indirizzo IP MC con questo comando:
   ```
   sw-3850-1(config)#wireless mobility controller ip a.b.c.d
   ```
   E sull'MC, immettere questi comandi:
   ```
   3850MC(config)#wireless mobility controller peer-group
   ```

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

3. Garanzia di disponibilità della licenza.Verificare che le licenze AP attive siano disponibili nel MC (il MA utilizza le licenze attivate nel MC):**Nota:** 1) Per abilitare i servizi wireless sullo switch 3850, sullo switch 3850 è necessario eseguire ipservices o una licenza ipbase. 2) Al MC vengono applicate licenze per il numero di access point, che vengono fornite e applicate automaticamente al MA. 3) Lo switch 3850, che agisce da MC, può supportare fino a 50 access point.

```
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
```

Per attivare la licenza AP count sullo switch 3850, immettere questo comando con il numero di access point richiesto sullo switch MC:

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

4. Configurare il processo di individuazione AP.Affinché gli access point si uniscano al controller, la configurazione dello switchport **deve essere impostata come porta di accesso** nella vlan di gestione wireless:Se si usa la vlan 100 per l'interfaccia di gestione wireless:

```
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. Configurare l'accesso Web.Èpossibile accedere alla GUI tramite https://<indirizzo_ip>/wirelessLe credenziali di accesso sono già definite nella finestra di dialogo di configurazione iniziale.

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

6. Verificare che sullo switch sia configurato il codice paese appropriato in conformità al dominio normativo del paese in cui sono distribuiti gli access point.

```
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
```

Per modificare il codice del paese, immettere i seguenti comandi:

```
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
```

Verifica

Per verificare che gli access point siano stati aggiunti, immettere il 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
```

Risoluzione dei problemi

Debug utili per la risoluzione dei problemi di aggiunta all'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
```