Exemplo de configuração do controlador CT5760 e do switch Catalyst 3850

Contents

Introduction

Este documento descreve as etapas para instalar e preparar serviços sem fio no 5760 Wireless LAN Controller (WLC) e no switch 3850. Este documento aborda a configuração inicial e o processo de união do ponto de acesso (AP) para ambas as plataformas.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador sem fio Unified Access CT5760 - Versão 3.02.02SE
- Unified Access Switch Catalyst 3850 - Versão 3.02.02SE

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de fundo do Controlador sem fio Unified Access CT5760

O CT5760 WLC é o primeiro controlador baseado no software Cisco IOS-XE® construído com Smart ASIC destinado a ser implantado como um controlador centralizado na arquitetura sem fio unificada da próxima geração. A plataforma também oferece suporte à nova funcionalidade de mobilidade com switches Converged Access 3850 Series.

Os controladores CT5760 são normalmente implantados perto do núcleo. As portas de uplink conectadas ao switch central podem ser configuradas como portas de tronco EtherChannel para garantir a redundância da porta. Esse novo controlador é um controlador sem fio extensível e de alto desempenho, que pode ser dimensionado para até 1.000 APs e 12.000 clientes. O controlador tem seis portas de dados de 10 Gbps para uma capacidade total de 60 Gbps.

A série 5760 trabalha em conjunto com os APs Cisco Aironet, a Cisco Prime Infrastructure e o Cisco Mobility Services Engine para oferecer suporte a aplicativos de serviços de dados, voz, vídeo e localização essenciais para a empresa.

Informações de fundo para os Switches Unified Access Catalyst 3850

O Cisco Catalyst 3850 Series é a próxima geração de switches de camada de acesso empilhável de classe empresarial que fornecem convergência total entre com e sem fio em uma única plataforma. Equipado com o software IOS-XE, o serviço sem fio é suportado através do protocolo CAPWAP (Control and Provisioning of Wireless Access Points). O novo ASIC de plano de dados de acesso unificado (UADP) da Cisco alimenta o switch e permite aplicação uniforme de políticas com e sem fio, visibilidade de aplicativos, flexibilidade e otimização de aplicativos. Essa convergência é baseada na resiliência do novo e aprimorado Cisco StackWise-480. Os switches Cisco Catalyst 3850 Series suportam Power over Ethernet Plus (PoE+) IEEE 802.3at completo, módulos de rede modulares e substituíveis em campo, ventoinhas redundantes e fontes de alimentação.

Configuração inicial do 5760 WLC

Esta seção descreve as etapas para configurar com êxito a WLC 5760 para hospedar serviços sem fio.

Configurar

Script de configuração

```
         --- 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
```

O seguinte script de comando de configuração foi criado:

```
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!
```

Configuração necessária para que os pontos de acesso participem

Note: Importante - Assegure-se de que o switch tenha o comando boot correto na configuração global. Se ele tiver sido extraído na memória flash, o comando **w-5760-1(config)#boot system flash:packages.conf** boot será necessário.

1. Configure a conectividade de rede.Configure a interface TenGig conectada à rede de backbone onde o tráfego CAPWAP flui para entrada/saída. Neste exemplo, a interface usada é TenGigabitEthernet1/0/1. VLAN 1 e VLAN 120 são permitidas.
   ```
   interface TenGigabitEthernet1/0/1
   switchport trunk allowed vlan 1,120
   switchport mode trunk
   ip dhcp relay information trusted
   ip dhcp snooping trust
   ```
   Configure a rota de saída padrão:
   ```
   ip route 0.0.0.0 0.0.0.0 192.168.1.1
   ```
2. Configure o acesso à Web.A GUI pode ser acessada via https://<*ipaddress*>/wirelessAs credenciais de logon já estão definidas na caixa de diálogo de configuração inicial.
   ```
   username admin privilege 15 password cisco
   ```
3. Verifique se a interface de gerenciamento sem fio está configurada corretamente.
   ```
   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. Verifique se uma licença ativa está habilitada com a contagem de AP adequada.**Note**: 1) O 5760 não tem níveis de licença ativados, a imagem já é ipservices. 2) O 5760 que atua como um controlador de mobilidade (CP) pode suportar até 1000 APs.
   w-5760-1#license right-to-use activate apcount <*count*> slot 1 acceptEULA
5. Verifique se o código de país correto está configurado na WLC de acordo com o domínio regulatório do país no qual o(s) AP(s) está(ão) implantado(s).
   ```
   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 o código do país, insira estes 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. Certifique-se de que os APs possam aprender o endereço IP da WLC (192.168.120.94 neste exemplo) através da opção de DHCP 43, Serviços de Nome de Domínio (DNS) ou qualquer outro mecanismo de descoberta no CAPWAP.

Verificar

Para garantir que os APs se juntaram, insira o comando **show ap summary**:

```
w-5760-1#show ap summary

Number of APs: 1
```

```
Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured

AP Name              AP Model  Ethernet MAC    Radio MAC       State
-----------------------------------------------------------------------
APa493.4cf3.232a     1042N     a493.4cf3.232a  10bd.186d.9a40  Registered
```

Troubleshoot

Depurações úteis para solucionar problemas de união de AP:

```
w-5760-1#debug capwap ap events
capwap/ap/events debugging is on

w-5760-1#debug capwap ap error
capwap/ap/error debugging is on

w-5760-1#debug dtls ap event
dtls/ap/event debugging is on

w-5760-1#debug capwap ios event
CAPWAP Event debugging is on

5760-1#debug capwap ios error
CAPWAP Error debugging is on
```

Configuração inicial do switch 3850

Esta seção inclui a configuração necessária para hospedar serviços sem fio no 3850.

Configurar

Script de configuração

```
         --- 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 de comando de configuração foi criado:

```
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!
```

Configuração necessária para que os pontos de acesso participem

> **Note**: Importante - Assegure-se de que o comando boot correto esteja configurado na configuração global. Se ele tiver sido extraído na flash, o comando **boot system switch all flash:packages.conf** será necessário.

1. Configurar pré-requisitos sem fio.Para habilitar serviços sem fio, o 3850 deve executar uma licença **ipservices ou ipbase**.
2. Ative a conexão sem fio no switch.**Note**: Os APs precisam ser conectados às portas de switch do modo de acesso na mesma VLAN!Habilitar gerenciamento sem fio
   `sw-3850-1(config)#wireless management interface vlan <1-4095>`
   Definir a CPUm MC deve ser definido para permitir a adesão de APs.Se esse 3850 for o MC, insira o comando **wireless mobility controller**:
   `sw-3850-1(config)#wireless mobility controller`
   Note: Esta alteração de configuração requer uma reinicialização!Se este 3850 operar como um Agente de Mobilidade (MA), aponte-o para o endereço IP MC com este comando:
   `sw-3850-1(config)#wireless mobility controller ip a.b.c.d`
   E no MC, insira estes comandos:
   `3850MC(config)#wireless mobility controller peer-group`

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

3. Verifique a disponibilidade da licença.Certifique-se de que as licenças de AP ativas estejam disponíveis no MC (o MA usa as licenças ativadas no MC):**Note**: 1) O 3850 deve executar ipservices ou uma licença ipbase para habilitar os serviços sem fio no 3850. 2) As licenças de contagem de AP são aplicadas no MC e provisionadas e aplicadas automaticamente no MA. 3) O 3850, que atua como um MC, pode suportar até 50 APs.

```
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 ativar a licença de contagem de AP no 3850, insira este comando com a contagem de AP necessária no MC:

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

4. Configure o processo de descoberta de AP.Para que os APs se juntem ao controlador, a configuração da porta do switch **deve ser definida como uma porta de acesso** na vlan de gerenciamento sem fio:Se a vlan 100 for usada para a interface de gerenciamento sem fio:

```
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. Configure o acesso à Web.A GUI pode ser acessada via https://<ipaddress>/wirelessAs credenciais de logon já estão definidas na caixa de diálogo de configuração inicial.

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

6. Certifique-se de que o código de país apropriado esteja configurado no switch em conformidade com o domínio regulatório do país no qual os APs estão implantados.

```
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 o código do país, insira estes 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
```

Verificar

Para garantir que o(s) AP(s) se juntou(m), insira o comando **show ap summary**:

```
sw-3850-1#show ap summary

Number of APs: 1

Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured

AP Name              AP Model Ethernet MAC    Radio MAC          State
-------------------------------------------------------------------------------

APa493.4cf3.232a     1042N     a493.4cf3.231a  10bd.186e.9a40      Registered
```

Troubleshoot

Depurações úteis para solucionar problemas de união de AP:

```
sw-3850-1#debug capwap ap events
capwap/ap/events debugging is on

sw-3850-1#debug capwap ap error
capwap/ap/error debugging is on

sw-3850-1#debug dtls ap event
dtls/ap/event debugging is on

sw-3850-1#debug capwap ios event
CAPWAP Event debugging is on

sw-3850-1#debug capwap ios error
CAPWAP Error debugging is on
```