

Exemplo de configuração do controlador CT5760 e do Catalyst 3850 Switch

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de fundo para o controlador unificado do Sem fio do acesso CT5760](#)

[Informações de fundo para os Catalyst 3850 Switch unificados do acesso](#)

[Configuração inicial de 5760 WLC](#)

[Configurar](#)

[Script de instalação](#)

[Configuração requerida para que os Access point juntem-se](#)

[Verificar](#)

[Troubleshooting](#)

[Configuração inicial do 3850 Switch](#)

[Configurar](#)

[Script de instalação](#)

[Configuração requerida para que os Access point juntem-se](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve as etapas para instalar e preparar Serviços sem fio no controlador do Wireless LAN 5760 (WLC) e no 3850 Switch. Esta configuração inicial das capas de documento e o Access Point (AP) juntam-se ao processo para ambas as Plataformas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Controlador wireless unificado do acesso CT5760 - Versão 3.02.02SE
- Catalyst 3850 Switch unificado do acesso - Versão 3.02.02SE

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de fundo para o controlador unificado do Sem fio do acesso CT5760

O CT5760 WLC é o controlador com base no software do primeiro [®] do Cisco IOS XE construído com o ASIC esperto pretendido ser distribuído como um controlador centralizado na arquitetura wireless unificada próxima geração. A plataforma igualmente apoia a funcionalidade nova da mobilidade com 3850 Series Switch convergidos do acesso.

Os controladores CT5760 são distribuídos tipicamente perto do núcleo. As portas de uplink conectadas ao switch central podem ser configuradas como portas de tronco de EtherChannel para assegurar a redundância de porta. Este controlador novo é um controlador wireless elástico e de alto desempenho, que possa escalar até 1000 AP e 12,000 clientes. O controlador tem seis portas dos dados do 10 Gbps para uma capacidade total de 60 Gbps.

O 5760 Series trabalha conjuntamente com o Cisco Aironet AP, a infraestrutura principal de Cisco, e o motor dos Serviços de mobilidade de Cisco a fim apoiar dados wireless críticos para negócio, Voz, vídeo, e aplicativos de serviços do lugar.

Informações de fundo para os Catalyst 3850 Switch unificados do acesso

O Cisco Catalyst 3850 Series é a próxima geração de switch de camada de acesso empilháveis da empresa-classe que fornecem a convergência completa entre prendido e Sem fio em uma plataforma única. Posto pelo software IOS-XE, o serviço Wireless é apoiado com o controle e o abastecimento do protocolo dos pontos de acesso Wireless (CAPWAP). O plano unificado novo dos dados do acesso de Cisco (UADP) ASIC põe o interruptor e permite o reforço de política do prender-Sem fio, a visibilidade do aplicativo, a flexibilidade, e a otimização uniformes do aplicativo. Esta convergência é construída na resiliência de Cisco novo e melhorado StackWise-480. Os Cisco Catalyst 3850 Series Switch apoiam a potência completa da IEEE 802.3at sobre Ethernet mais (PoE+), os módulos de rede modulares e campo-substituíveis, fãs redundantes, e fontes de alimentação.

Configuração inicial de 5760 WLC

Esta seção esboça as etapas para configurar com sucesso os 5760 WLC a fim hospedar Serviços sem fio.

Configurar

Script de instalação

--- 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**

O seguinte script do comando configuration 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 requerida para que os Access point juntem-se

Nota: Importante - Assegure-se de que o interruptor tenha o comando boot correto sob a configuração global. Se foi extraído no flash, então o **flash do sistema w-5760-1(config)#boot: o comando boot packages.conf** é exigido.

1. Configurar a conectividade de rede. Configurar a relação de TenGig conectada à rede de backbone onde os fluxos de tráfego CAPWAP de entrada/de partida. Neste exemplo, a relação usada é TenGigabitEthernet1/0/1. O VLAN1 e o VLAN 120 são permitidos.


```

interface TenGigabitEthernet1/0/1
switchport trunk allowed vlan 1,120
switchport mode trunk
ip dhcp relay information trusted
ip dhcp snooping trust
Configurar a rota padrão de partida:
ip route 0.0.0.0 0.0.0.0 192.168.1.1

```
2. Configurar o acesso à Web. O GUI pode ser alcançado através dos <ipaddress >/wireless de https://As credenciais de logon são definidas já no diálogo de configuração inicial.


```

username admin privilege 15 password cisco

```
3. Assegure-se de que a interface de gerenciamento wireless esteja 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
Tel/0/1	unassigned	YES	unset	up	up
Tel/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. Assegure-se de que uma licença ativa esteja permitida com a contagem apropriada AP. Nota: 1) Os 5760 não ativaram níveis da licença, a imagem são já ipservices. 2) Os 5760 que atua como um controlador da mobilidade (o MC) podem apoiar até 1000 AP. w-5760-1#license right-to-use activate apcount <count> slot 1 acceptEULA

5. Assegure-se de que o código de país correto esteja configurado no WLC em conformidade com o domínio regulatório do país que os AP são distribuídos dentro. 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

A fim alterar o código de país, incorpore 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. Assegure-se de que os AP possam aprender o endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC (192.168.120.94 neste exemplo) através da opção de DHCP 43, dos serviços do Domain Name (DNS), ou do todo o outro mecanismo de descoberta em CAPWAP.

Verificar

A fim assegurar-se de que os AP se juntem, inscreva 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

Troubleshooting

Útil debuga para pesquisar defeitos o AP juntam-se a edições:

```
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 3850 Switch

Esta seção inclui a configuração exigida hospedar Serviços sem fio nos 3850.

Configurar

Script de instalação

```
--- 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

Este script do comando configuration 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 requerida para que os Access point juntem-se

Nota: Importante - Assegure-se de que o comando boot correto esteja configurado sob a configuração global. Se foi extraída no flash, então o interruptor do sistema da bota todo o flash: o comando **packages.conf** é exigido.

1. Configurar condições prévias wireless. A fim permitir Serviços sem fio, os 3850 devem executar **ipservices** ou licença do **ibase**.
2. Permita o Sem fio no interruptor. Nota: Os AP precisam de ser conectados aos switchports do modo de acesso no mesmo VLAN! Permita o Gerenciamento wireless `sw-3850-1(config)#wireless management interface vlan <1-4095>` Defina o MCUm MC deve ser definido a fim permitir que os AP juntem-se. Se estes 3850 serão o MC, inscreva o **comando controller wireless da mobilidade**: `sw-3850-1(config)#wireless mobility controller` Nota: Esta alteração de configuração exige uma repartição! Se estes 3850 se operam como um agente da mobilidade (MA), a seguir aponte-o ao endereço IP de Um ou Mais Servidores Cisco ICM NT MC com este comando: `sw-3850-1(config)#wireless mobility controller ip a.b.c.d` E NO MC, incorpore estes comandos: `3850MC(config)#wireless mobility controller peer-group <SPG1>`

`3850MC(config)#wireless mobility controller peer-group <SPG1> member ip w.x.y.z`
3. Assegure a Disponibilidade da licença. Assegure-se de que as licenças ativas AP estejam disponíveis no MC (o MA usa as licenças que são ativadas no MC): Nota: 1) Os 3850 devem executar **ipservices** ou uma licença do **ibase** a fim permitir Serviços sem fio nos 3850. 2) As licenças da contagem AP são aplicadas no MC, e são automaticamente fornecida e reforçadas no MA. 3) Os 3850 que atua como um MC podem apoiar até os 50 pés AP. `sw-3850-1#show license right-to-use summary`

License Name	Type	Count	Period left
ipservices	permanent	N/A	Lifetime
apcount	base	1	Lifetime

```
apcount      adder      49      Lifetime
-----
```

```
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 1
```

AP Count Licenses Remaining: 49

A fim ativar a licença da contagem AP nos 3850, incorpore este comando com a contagem exigida AP no MC:

```
sw-3850-1#license right-to-use activate apcount <count> slot <#> acceptEULA
```

4. Configurar o processo de descoberta AP. Para que os AP juntem-se ao controlador, a configuração de switchport deve ser ajustada como uma porta de acesso no Gerenciamento wireless vlan: Se o VLAN 100 é usado para a interface de gerenciamento 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. Configurar o acesso à Web. O GUI pode ser alcançado através de https://<ipaddress>/wireless. As credenciais de logon são definidas já no diálogo de configuração inicial.
- ```
username admin privilege 15 password 0 cisco (username for Web access)
```

6. Assegure-se de que o código de país apropriado esteja configurado no interruptor em conformidade com o domínio regulatório do país que os AP são distribuídos dentro.
- ```
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

A fim alterar o código de país, incorpore 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

A fim assegurar-se de que o AP se junte, inscreva 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

Troubleshooting

Útil debuga para pesquisar defeitos o AP juntam-se a edições:

```
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
```