

Контроллер СТ5760 и пример конфигурации коммутатора Catalyst 3850

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения для унифицированного доступа контроллер беспроводной локальной сети СТ5760](#)

[Общие сведения для унифицированных коммутаторов Catalyst 3850 доступа 5760 начальных конфигураций WLC](#)

[Настройка](#)

[Сценарий программы установки](#)

[Требуемая конфигурация для точек доступа для присоединения](#)

[Проверка](#)

[Устранение неполадок](#)

[3850 начальных конфигураций коммутатора](#)

[Настройка](#)

[Сценарий программы установки](#)

[Требуемая конфигурация для точек доступа для присоединения](#)

[Проверка](#)

[Устранение неполадок](#)

Введение

Этот документ описывает шаги, чтобы установить и подготовить беспроводные сервисы на 5760 Контроллерах беспроводной локальной сети (WLC) и 3850 коммутаторах. Этот документ покрывает начальную конфигурацию и процесс соединения Точки доступа (AP) для обеих из платформ.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Унифицированный доступ контроллер беспроводной локальной сети CT5760 - версия 3.02.02SE
- Унифицированный коммутатор Catalyst 3850 доступа - версия 3.02.02SE

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения для унифицированного доступа контроллер беспроводной локальной сети CT5760

CT5760 WLC является первым Cisco IOS-XE® программный контроллер, созданный с умным ASIC, предназначенным, чтобы быть развернутым как централизованный контроллер в Унифицированной беспроводной архитектуре следующего поколения. Платформа также поддерживает новую функциональность мобильности с Установившимся Доступом коммутаторы серии 3850.

Контроллеры CT5760, как правило, развертываются около ядра. Порты каскадного соединения, связанные с основным коммутатором, могут быть настроены как порты Транка Ethernet - канала для обеспечения резервирования порта. Этот новый контроллер является расширяемым и высокоэффективным контроллером беспроводной локальной сети, который может увеличиться к 1000 AP и 12,000 клиентов. Контроллер имеет шесть портов данных на 10 Гбит/с для общей емкости 60 Гбит/с.

Работы серии 5760 в сочетании с AP Cisco Aironet, Cisco Главная Инфраструктура и Cisco Mobility Services Engine Cisco для поддержки критически важных для бизнеса беспроводных данных, голоса, видео и приложений служб определения местоположения.

Общие сведения для унифицированных коммутаторов Catalyst 3850 доступа

Cisco Catalyst, серии 3850, является следующим поколением стекируемых коммутаторов уровня доступа промышленного класса, которые предоставляют полную конвергенцию между проводным и беспроводным на одной платформе. Приведенный в действие программным обеспечением IOS-XE, беспроводной сервис поддерживается через Контроль и Инициализацию Точек беспроводного доступа (CAPWAP) протокол. Новый ASIC Унифицированной плоскости данных доступа (UADP) Cisco приводит коммутатор в действие и включает универсальную проводную беспроводную принудительную политику, видимость приложения, гибкость и оптимизацию приложения. Эта конвергенция основана на упругости нового и улучшенного Cisco StackWise 480. Cisco Catalyst коммутаторы серии 3850 поддерживает полное Питание IEEE 802.3at над Ethernet Плюс (PoE +), модульные и заменяемые полем сетевые модули, избыточные вентиляторы и источники питания.

5760 начальных конфигураций WLC

Этот раздел выделяет шаги для успешной настройки 5760 WLC для хостинга беспроводных сервисов.

Настройка

Сценарий программы установки

```
--- 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
Tel1/0/1	unassigned	YES	unset	up	up
Tel1/0/2	unassigned	YES	unset	down	down
Tel1/0/3	unassigned	YES	unset	down	down
Tel1/0/4	unassigned	YES	unset	down	down
Tel1/0/5	unassigned	YES	unset	down	down
Tel1/0/6	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**

Следующий сценарий команды настройки был создан:

```
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!

Требуемая конфигурация для точек доступа для присоединения

Примечание: Важный - Гарантируют, что коммутатор имеет корректную команду загрузки под глобальной конфигурацией. Если это было извлечено на флэш-памяти, то **w-5760-1 (config) #boot система flash:packages.conf** команда загрузки требуется.

1. Настройте сетевое подключение. Настройте интерфейс TenGig, связанный до мозга костей сеть где входящие/исходящие трафики CAPWAP. В данном примере используемый интерфейс является TenGigabitEthernet1/0/1. VLAN 1 и VLAN 120 **ПОЗВОЛЕНЫ**.


```

interface TenGigabitEthernet1/0/1
switchport trunk allowed vlan 1,120
switchport mode trunk
ip dhcp relay information trusted
ip dhcp snooping trust
Настройте исходящий маршрут по умолчанию: ip route 0.0.0.0
0.0.0.0 192.168.1.1

```
2. Настройте веб - доступ. К GUI можно обратиться через `https://<ipaddress> /` радио. Учетные данные начала сеанса уже определены в диалоговом окне начальной конфигурации.


```

username admin privilege 15 password cisco

```
3. Гарантируйте, что правильно настроен интерфейс беспроводного управления.


```

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. Гарантируйте, что активная лицензия включена с надлежащим количеством AP. **Примечание:** 1) Эти 5760 не имеют активированных уровней лицензии, образ уже ipservices. 2) 5760, который действует как Контроллер мобильности (MC), могут поддержать до 1000 AP.
- ```
w-5760-1#license right-to-use activate apcount <count> slot 1 acceptEULA
```

5. Гарантируйте, что корректный код страны настроен на WLC в соответствии с управляющим домен страны, в которой развернут AP.
- ```
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 **Для изменения кода страны введите ЭТИ КОМАНДЫ:**

```
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. Гарантируйте, что AP в состоянии изучить IP-адрес WLC (192.168.120.94 в данном примере) через параметр DHCP 43, Сервисы доменных имен (DNS) или любой другой discovery механизм в CAPWAP.

Проверка

Чтобы гарантировать, что AP присоединились, введите команду **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

Устранение неполадок

Полезные отладки для решения AP присоединяются к проблемам:

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

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

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

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

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

3850 начальных конфигураций коммутатора

Этот раздел включает конфигурацию, требуемую размещать беспроводные сервисы на 3850.

Настройка

Сценарий программы установки

```
--- 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

Этот сценарий команды настройки был создан:

```
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!

Требуемая конфигурация для точек доступа для присоединения

Примечание: Важный - Гарантируют, что корректная команда загрузки настроена под глобальной конфигурацией. Если это было извлечено на флэш-памяти, то **коммутатор boot system вся flash:packages.conf** команда требуется.

1. Настройте беспроводные предварительные условия. Для включения беспроводных сервисов эти 3850 должны выполнить **ipservices** или **ipbase** лицензию.
2. Включите радио на коммутаторе. **Примечание:** AP должны быть связаны с режимом доступа switchports в той же VLAN! Включите беспроводное управление `sw-3850-1(config)#wireless management interface vlan <1-4095>` Определите MCS должен быть определен, чтобы позволить AP присоединяться. Если это 3850 будет MC, введите **беспроводную команду controller мобильности:** `sw-3850-1(config)#wireless mobility controller` **Примечание:** Это изменение конфигурации требует перезагрузки! Если это 3850 действует в качестве Агента мобильности (МА), то укажите его к IP-адресу MC с ЭТОЙ КОМАНДОЙ: `sw-3850-1(config)#wireless mobility controller ip a.b.c.d` И на MC, **введите ЭТИ КОМАНДЫ:** `3850MC(config)#wireless mobility controller peer-group <SPG1>`
`3850MC(config)#wireless mobility controller peer-group <SPG1> member ip w.x.y.z`
3. Гарантируйте доступность лицензии. Гарантируйте, что активные Лицензии AP доступны на MC (МА использует лицензии, которые активированы на MC): **Примечание:** 1) Эти 3850 должны выполнить **ipservices** или **ipbase** лицензию для включения беспроводных сервисов на 3850. 2) лицензии количества AP применены в MC, и

автоматически настроены и принуждены в МА. 3) 3850, который действует как МС, могут поддержать до 50 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
Для активации лицензии количества AP на этих 3850 войдите, эта команда с требуемым AP рассчитывают на МС:
sw-3850-1#license right-to-use activate apcount <count> slot <#> acceptEULA

4. Настройте процесс обнаружения AP. Для AP для присоединения к контроллеру конфигурация порта коммутатора **должна быть установлена как порт доступа в vlan беспроводного управления**. Если VLAN 100 используется для интерфейса беспроводного управления:
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. Настройте веб - доступ. К GUI можно обратиться через https://<ipaddress> / ради
Учетные данные начала сеанса уже определены в диалоговом окне начальной конфигурации.
username admin privilege 15 password 0 cisco (username for Web access)
6. Гарантируйте, что надлежащий код страны настроен на коммутаторе в соответствии с управляющим домен страны, в которой развернут AP.
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
Для изменения кода страны введите ЭТИ КОМАНДЫ:
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

Проверка

Чтобы гарантировать, что AP присоединился, введите команду **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

Устранение неполадок

Полезные отладки для решения AP присоединяются к проблемам:

```
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
```