# 在無線LAN控制器上配置NTP

## 目錄



## 簡介

本檔案介紹如何設定AireOS無線LAN控制器(WLC)以與網路時間協定(NTP)伺服器同步日期和時間。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- Cisco WLC組態的基本知識。
- NTP基礎知識。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本8.8.110的Cisco WLC 3504。

- 執行Cisco IOS®軟體版本15.2(6)E2的Cisco Catalyst 3560-CX系列L3交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

### 在無線LAN控制器上管理系統日期和時間

在WLC上，可以從WLC手動配置系統日期和時間，也可以配置為從NTP伺服器獲取日期和時間。

可以在CLI配置嚮導或WLC GUI/CLI中手動配置系統日期和時間。

本文提供通過NTP伺服器同步WLC系統日期和時間的配置示例。

NTP是一種網路協定，用於通過可變延遲資料網路在電腦系統之間實現時鐘同步，以將電腦的時鐘同步到某個時間基準。 RFC 1305 和RFC 5905 分別提供有關NTPv3和NTPv4實施的詳細資訊。

NTP網路通常從權威時間源（例如連線到時間伺服器的無線電時鐘或原子時鐘）接收其時間。然後，NTP將此時間分佈到整個網路。

NTP客戶端在輪詢間隔內與其伺服器進行事務，輪詢間隔隨時間動態變化並取決於NTP伺服器和客戶端之間的網路條件。

NTP使用層的概念來描述一台機器與權威時間源之間有多少NTP跳躍。例如，第1層時間伺服器直接連線了無線電時鐘或原子時鐘。然後通過NTP將其時間傳送到第2層時間伺服器，以此類推。

有關NTP部署的最佳實踐的詳細資訊，請參閱使用網路時間協定的最佳實踐。

本檔案中的範例使用Cisco Catalyst 3560-CX系列第3層交換器作為NTP伺服器。WLC配置為將其日期和時間與此NTP伺服器同步。

## 設定

### 網路圖表

採用----伺服器的WLC 3560-CX第3層----換器

### 組態

將L3交換機配置為授權NTP伺服器

如果希望系統成為授權NTP伺服器（即使系統未與外部時間源同步），請在全域性配置模式下使用此命令：

```
#ntp master  !--- Makes the system an authoritative NTP server
```

配置NTP身份驗證

如果出於安全目的，要對與其他系統的關聯進行身份驗證，請使用下一個命令。第一個命令啟用NTP身份驗證功能。

第二命令定義每個驗證金鑰。每個鍵都有一個鍵編號、型別和值。目前，唯一支援的金鑰型別是md5。

第三，定義可信驗證金鑰清單。如果金鑰受信任，則此系統已準備好與在其NTP資料包中使用此金鑰的系統同步。要配置NTP身份驗證，請在全域性配置模式下使用以下命令：

```
#ntp authenticate

!--- Enables the NTP authentication feature

#ntp authentication-key number md5 value

!--- Defines the authentication keys

#ntp trusted-key key-number

!--- Defines trusted authentication keys
```

以下是3560-CX L3交換機上的NTP伺服器配置示例。交換機是NTP master，這意味著路由器充當授權NTP伺服器，但路由器本身可以從另一個NTP伺服器xxxx.xxx獲取時間。

```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server xxxx.xxx
```

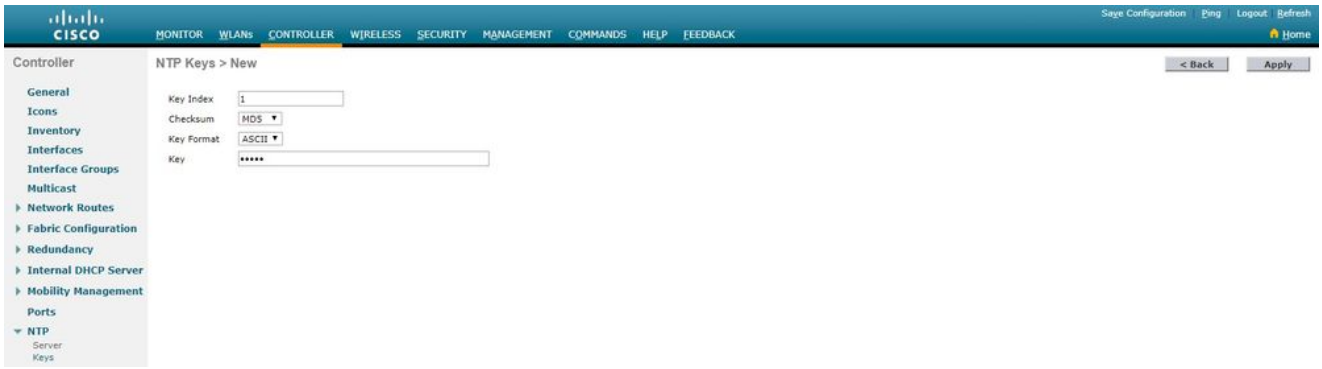
為NTP伺服器配置WLC

從版本8.6起，您可以啟用NTPv4。您也可以在控制器和NTP伺服器之間配置身份驗證通道。

要在控制器GUI中配置NTP身份驗證，請執行以下步驟：

1. 選擇Controller > NTP > Keys。
2. 按一下New以建立金鑰。
3. 在「鍵索引」文本框中輸入鍵索引。
4. 選擇Key Checksum（MD5或SHA1）和Key Format下拉選單。

5. 在「金鑰」文本框中輸入金鑰：

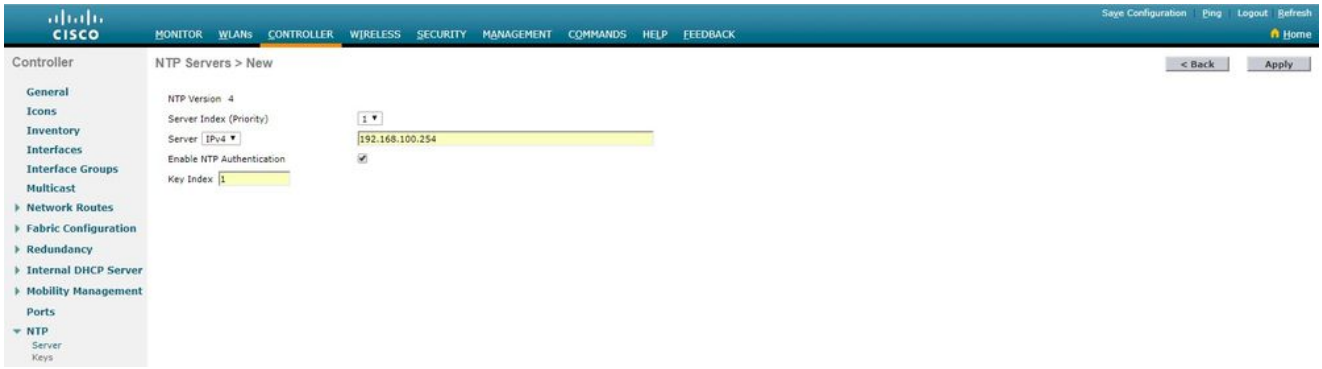



6. 選擇Controller > NTP > Servers以開啟NTP Servers頁。選擇版本3或4，然後按一下New以新增NTP伺服器。出現NTP Servers > New頁面。

7. 選擇服務器索引（優先順序）。

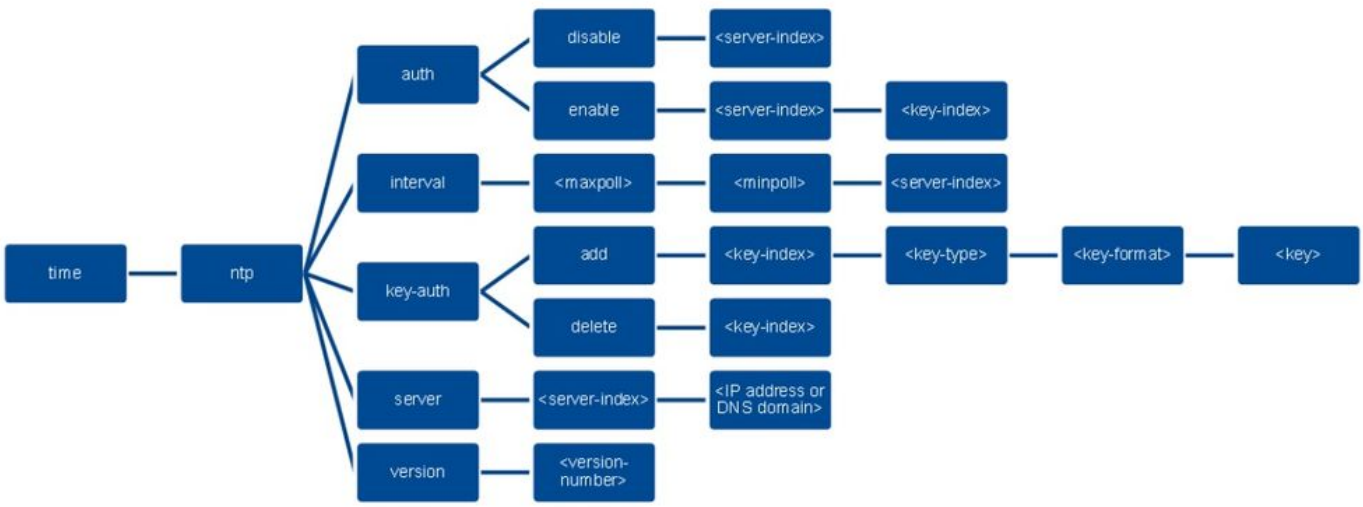
8. 在「伺服器IP地址」文本框中輸入NTP服務器IP地址。

9. 啟用NTP伺服器身份驗證，選中NTP Server Authentication覈取方塊，並選擇之前配置的金鑰索引。




10. 按一下「Apply」。

若要透過控制器CLI設定NTP驗證，請追蹤以下命令樹：



```
>config time ntp version 4
>config time ntp key-auth add 1 md5 ascii cisco
>config time ntp server 1 192.168.100.254
>config time ntp auth enable 1 1
```

# 驗證

## 在NTP伺服器上

```
#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406 msec, root delay is 59.97 msec
root dispersion is 25.98 msec, peer dispersion is 1.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000042509 s/s
system poll interval is 128, last update was 7 sec ago.

#show ntp associations

 address ref clock st when poll reach delay offset disp
*~x.x.x.x y.y.y.y 2 20 1024 17 13.634 0.024 1.626
 ~127.127.1.1 .LOCL. 7 9 16 377 0.000 0.000 0.232
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

#show ntp information
Ntp Software Name : Cisco-ntpv4
Ntp Software Version : Cisco-ntpv4-1.0
Ntp Software Vendor : CISCO
Ntp System Type : Cisco IOS / APM86XXX
```

## 在WLC上

### 在GUI中

### WLC建立通訊時：

建立連線後：


在WLC CLI中

```
(Cisco Controller) >show time

Time..................................... Fri Feb 8 10:14:47 2019

Timezone delta..................................... 0:0
Timezone location.................................

NTP Servers
 NTP Version..................................... 4

Index NTP Key NTP Server NTP Key Polling Intervals
 Index Type Max Min
 ------------------------------------------------------------
 1 1 192.168.100.254 MD5 10 6

NTPQ status list of NTP associations

assoc
 ind assid status conf reach auth condition last_event cnt src_addr
 ===============================================================================
 1 1385 f63a yes yes ok sys.peer sys_peer 3 192.168.100.254


(Cisco Controller) >
```

# 疑難排解

在執行Cisco IOS的NTP伺服器端，可以使用 debug ntp all enable 指令:

```
#debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
```

```
#
(communication between SW and NTP server xxxx.xxx)
Feb 8 09:52:30.563: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:53:10.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:53:10.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).

(communication between SW and NTP server xxxx.xxx)
Feb 8 09:53:37.566: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:54:17.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:54:17.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).
```

在WLC端：

```
 >debug ntp ?

detail Configures debug of detailed NTP messages.
low Configures debug of NTP messages.
packet Configures debug of NTP packets.

(at the time of writte this doc there was Cisco bug ID CSCvo29660
on which the debugs of ntpv4 are not printed in the CLI. The below debugs are using NTPv3.)
(Cisco Controller) >debug ntp detail enable
(Cisco Controller) >debug ntp packet enable
(Cisco Controller) >*emWeb: Feb 08 11:26:53.896: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: Key Id = 1 found at Local Index = 0

*sntpReceiveTask: Feb 08 11:26:58.143: Initiating time sequence

*sntpReceiveTask: Feb 08 11:26:58.143: Fetching time from:192.168.100.254

*sntpReceiveTask: Feb 08 11:26:58.143: Started=3758614018.143350 2019 Feb 08 11:26:58.143

*sntpReceiveTask: Feb 08 11:26:58.143: hostname=192.168.100.254 hostIdx=1 hostNum=0
*sntpReceiveTask: Feb 08 11:26:58.143: Looking for the socket addresses

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6. Outgoing packet on NTP Server on socket 0:

*sntpReceiveTask: Feb 08 11:26:58.143: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000
```

```
*sntpReceiveTask: Feb 08 11:26:58.143: ori=0.000000 rec=0.000000
*sntpReceiveTask: Feb 08 11:26:58.143: tra=3758614018.143422 cur=3758614018.143422

*sntpReceiveTask: Feb 08 11:26:58.143: Host Supports NTP authentication with Key Id = 1

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Auth Key Id = 1 Key Length = 5

*sntpReceiveTask: Feb 08 11:26:58.143: MD5 Hash and Key Id added in NTP Tx packet

*sntpReceiveTask: Feb 08 11:26:58.143: 00000000: 1b 0f 08 00 00 00 00 00 00 00 00 00 00 00 00 ......
*sntpReceiveTask: Feb 08 11:26:58.143: 00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ......
*sntpReceiveTask: Feb 08 11:26:58.143: 00000020: 00 00 00 00 00 00 00 00 e0 07 e6 02 24 b7 50 00 ......
*sntpReceiveTask: Feb 08 11:26:58.143: 00000030: 00 00 00 01 e4 35 f3 1a 89 f0 93 c5 51 c7 c5 23 .....5
*sntpReceiveTask: Feb 08 11:26:58.143: 00000040: 01 dd 67 e0 ..g.
*sntpReceiveTask: Feb 08 11:26:58.143: Flushing outstanding packets

*sntpReceiveTask: Feb 08 11:26:58.143: Flushed 0 packets totalling 0 bytes

*sntpReceiveTask: Feb 08 11:26:58.143: Packet of length 68 sent to ::ffff:192.168.100.254 UDPport=123
*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = 0

*emWeb: Feb 08 11:26:58.143: idx != 0 : ntp key Id = 1 Msg auth Status = 66

*sntpReceiveTask: Feb 08 11:26:58.146: Packet of length 68 received from ::ffff:192.168.100.254 UDPport
*sntpReceiveTask: Feb 08 11:26:58.146: Incoming packet on socket 0: has Authentication Enabled
*sntpReceiveTask: Feb 08 11:26:58.146: 00000000: 1c 04 08 eb 00 00 0e a0 00 00 0b 2e c3 16 11 07 ......
*sntpReceiveTask: Feb 08 11:26:58.146: 00000010: e0 07 e5 f8 d3 21 bf 57 e0 07 e6 02 24 b7 50 00 .....!
*sntpReceiveTask: Feb 08 11:26:58.146: 00000020: e0 07 e6 02 24 e5 e3 b4 e0 07 e6 02 24 f3 c7 5a ....$.
*sntpReceiveTask: Feb 08 11:26:58.146: 00000030: 00 00 00 01 32 e4 26 47 33 16 50 bd d1 37 63 b7 ....2.
*sntpReceiveTask: Feb 08 11:26:58.146: KeyId In Recieved NTP Packet 1

*sntpReceiveTask: Feb 08 11:26:58.146: KeyId 1 found in recieved NTP packet exists as part of the trust

*sntpReceiveTask: Feb 08 11:26:58.146: The NTP trusted Key Id 1 length = 5

*sntpReceiveTask: Feb 08 11:26:58.146: NTP Message Authentication - SUCCESS

*sntpReceiveTask: Feb 08 11:26:58.146: sta=0 ver=3 mod=4 str=4 pol=8 dis=0.043671 ref=3758614008.824734

*sntpReceiveTask: Feb 08 11:26:58.146: ori=3758614018.143422 rec=3758614018.144133
*sntpReceiveTask: Feb 08 11:26:58.146: Offset=-0.000683+/-0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: best=-0.000683+/-0.002787

*sntpReceiveTask: Feb 08 11:26:58.146: accepts=1 rejects=0 flushes=0

*sntpReceiveTask: Feb 08 11:26:58.146: Correction: -0.000683 +/- 0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: Setting clock to 2019 Feb 08 11:26:58.145 + 0.001 +/- 1.940 secs
*sntpReceiveTask: Feb 08 11:26:58.146: correction -0.001 +/- 1.938+0.003 secs - ignored


(Cisco Controller) >
```

# 相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。