ワイヤレスLANコントローラでのNTPの設定

内容

はじめに

このドキュメントでは、ネットワークタイムプロトコル(NTP)サーバと日時を同期するようにAireOSワイヤレスLANコントローラ(WLC)を設定する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco WLCの設定に関する基礎知識。
- NTP に関する基礎知識.

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン 8.8.110 を実行している Cisco WLC 3504。

- Cisco IOS®ソフトウェアリリース15.2(6)E2が稼働するCisco Catalyst 3560-CXシリーズL3スイッチ。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ワイヤレスLANコントローラでのシステム日付と時刻の管理

WLC では、システム日付と時刻を WLC から手動で設定するか、NTP サーバから日付と時刻を取得するように設定できます。

システムの日付と時刻は、CLIコンフィギュレーションウィザードまたはWLC GUI/CLIで手動で設定できます。

このドキュメントでは、NTPサーバを介してWLCシステムの日付と時刻を同期するための設定例を紹介します。

NTPは、可変遅延データネットワーク上のコンピュータシステム間でクロックを同期し、コンピュータのクロックを時間基準に同期させるためのネットワークプロトコルです。RFC 1305およびRFC 5905は、それぞれNTPv3およびNTPv4実装に関する詳細情報を提供します。

NTP のネットワークでは通常、タイム サーバに接続された電波時計や原子時計など正規の時刻源から時刻を取得します。その後、NTP はこの時刻をネットワーク全体に配信します。

NTPクライアントは、ポーリング間隔でサーバとのトランザクションを確立します。この間隔は、時間の経過とともに動的に変化し、NTPサーバとクライアント間のネットワーク状態に応じて変化します。

NTP では、正規の時刻源から各マシンが何段階隔たっているかを表すために、ストラタムという概念が使用されます。たとえば、ストラタム 1 のタイム サーバに電波時計または原子時計が直接接続されているとします。このタイム サーバはストラタム 2 のタイム サーバに NTP で時間を配信します。このサーバはさらに別のマシンへ時間を再配信します。

NTP導入のベストプラクティスの詳細については、『ネットワークタイムプロトコルのベストプラクティスの使用』を参照してください。

このドキュメントの例では、NTPサーバとしてCisco Catalyst 3560-CXシリーズL3スイッチを使用しています。この NTP サーバと日時を同期するように、WLC を設定します。

設定

ネットワーク図

WLC ---- 3560-CX L3スイッチ----NTPサーバ

コンフィギュレーション

L3スイッチを正規のNTPサーバとして設定する

システムを正規の NTP サーバにする場合は、グローバル コンフィギュレーション モードで次のコマンドを使用します。これは、システムが外部の時刻源と同期されていない場合でも同じです。

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

NTP認証の設定

セキュリティ上の目的で他のシステムとのアソシエーションを認証する場合は、次のコマンドを使用します。最初のコマンドにより、NTP 認証機能が有効になります。

2 番目のコマンドにより、それぞれの認証キーが定義されます。キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。現在サポートされているキー タイプは md5 だけです。

3番目に、信頼できる認証キーのリストを定義します。キーが信頼されている場合、このシステムはNTPパケットでこのキーを使用するシステムと同期する準備ができています。NTP 認証を設定するには、次のコマンドをグローバル コンフィギュレーション モードで使用します。

```
#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
```

次に、3560-CX L3スイッチでのNTPサーバの設定例を示します。スイッチはNTP masterです。つまり、ルータは正規のNTPサーバとして動作しますが、自身は別のNTPサーバxxxx.xxxから時刻を取得します。

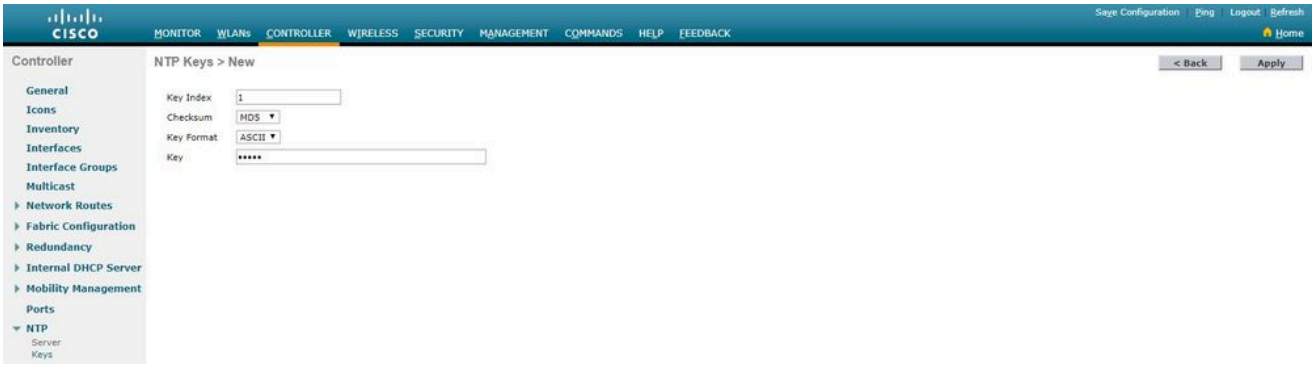
```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server xxxx.xxx
```

NTPサーバ用のWLCの設定

バージョン8.6から、NTPv4を有効にできます。コントローラとNTPサーバの間に認証チャネルを設定することもできます。

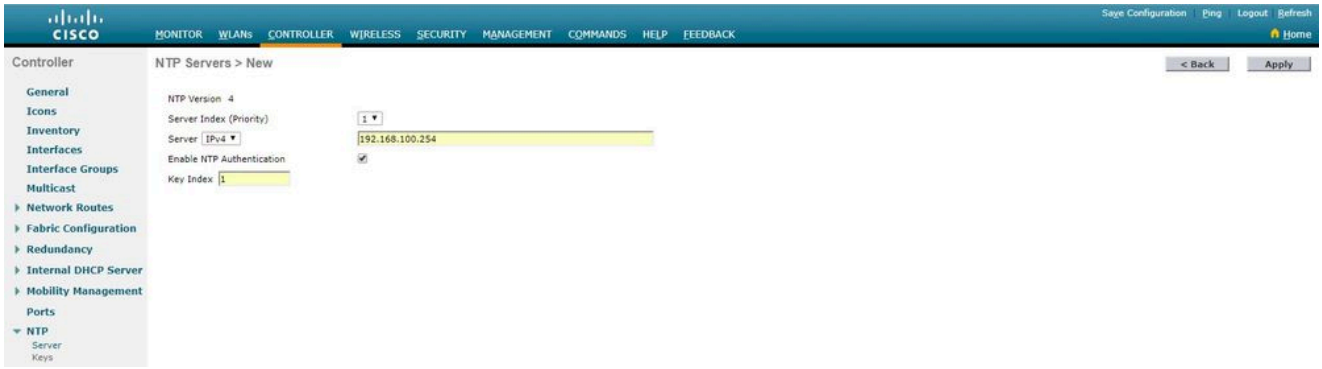
コントローラGUIでNTP認証を設定するには、次の手順を実行します。

- [Controller] > [NTP] > [Keys] を選択します。
- [New] をクリックして新しいキーを作成します。
- [Key Index] テキスト ボックスにキー インデックスを入力します。
- **Key Checksum**（MD5またはSHA1）および**Key Format**ドロップダウンリストを選択します。
- **Key**テキストボックスにキーを入力します。



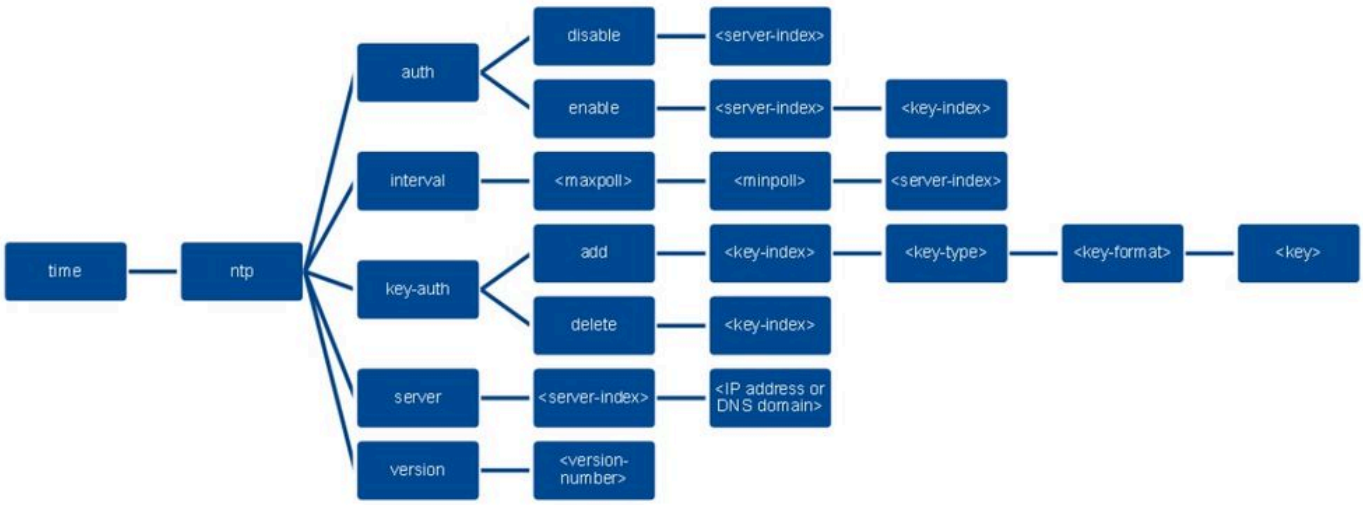
- [Controller] > [NTP] > [Servers] の順に選択して、[NTP Servers] ページを開きます。バージョン3または4を選択し、**New**をクリックしてNTPサーバを追加します。[NTP Servers > New] ページが表示されます。
- **Server Index (Priority)**を選択します。
- **Server IP Address**テキストボックスにNTPサーバのIPアドレスを入力します。

- NTPサーバ認証をイネーブルにし、**NTP Server Authentication** チェックボックスをオンにして、事前に設定したキーインデックスを選択します。



- [APPLY] をクリックします。

コントローラCLIを使用してNTP認証を設定するには、次のコマンドツリーを追跡します。




```
>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
```

確認

NTPサーバ

#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

WLC上

GUIの場合

WLCが通信を確立する間：

接続が確立された後

WLC CLIの場合

(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) >

トラブルシュート

Cisco IOSが稼働するNTPサーバ側では、 debug ntp all enable コマンドを使用できます。

#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).

WLC側：

>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 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 ....$.P.
*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......Q..#
*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=123
*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 .....!.W....$.P.
*sntpReceiveTask: Feb 08 11:26:58.146: 00000020: e0 07 e6 02 24 e5 e3 b4 e0 07 e6 02 24 f3 c7 5a ....$.......$..Z
*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.&G3.P..7c.
*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 trusted Key/s

*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) >

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。