

ワイヤレス LAN コントローラでの NTP の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ワイヤレス LAN コントローラにおけるシステム日付と時刻の管理](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

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ためにワイヤレス 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。

- Lightweight アクセス ポイント (LAP) および 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くものです。

- ソフトウェア バージョン 7.0.116.0 が稼働している Cisco 4400 WLC
- Cisco 1230AG シリーズ LAP
- Cisco IOS® ソフトウェア リリース 12.4(11)T が稼働している Cisco 2800 シリーズ ルータ

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くものです。

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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく

必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

ワイヤレス LAN コントローラにおける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。

システム日付と時刻を手動で設定するには、CLI コンフィギュレーション ウィザードまたは WLC GUI/CLI を使用します。このドキュメントでは、WLC のシステム日付と時刻を NTP サーバで同期する設定例を示します。

NTP は、コンピュータのクロックを時間基準と同期するために使用するインターネット プロトコルです。NTP v3 実装の詳細については、[RFC 1305](#) で説明されています。[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。](#) NTP は、この時間をネットワーク全体に配信します。NTP クライアントは、それぞれのポーリング間隔 (64 ~ 1024 秒) でサーバとのトランザクションを行います。この間隔は、NTP サーバとクライアントの間のネットワーク状態によって動的に変化します。[不適切な NTP サーバ \(ばらつきが大きい NTP サーバなど\) とルータが通信するときは、別の状況となります。ルータはポーリング間隔を上げます。2 台のマシンを同期させるために、1 分あたり 2 回以上の NTP トランザクションを実行する必要はありません。ルータでの NTP ポーリング間隔の調整はできません。](#)

NTP では、信頼できるタイムソースから各マシンが何 NTP ホップ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、「[Network Time Protocol : ベストプラクティスホワイトペーパー](#)」を参照してください。このドキュメントの例では、Cisco 2800 ルータを NTP サーバとして使用します。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

NTP サーバとしての Cisco 2800 シリーズ ルータの設定

正規の NTP サーバとしてのルータの設定

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その他のシステムとの関連付けを認証する場合は、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 番目のコマンドにより、「信頼される」認証キーのリストが定義されます。キーを信頼できる場合、このシステムは、このキーを NTP パケット内で使用する別のシステムに同期できます。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
```

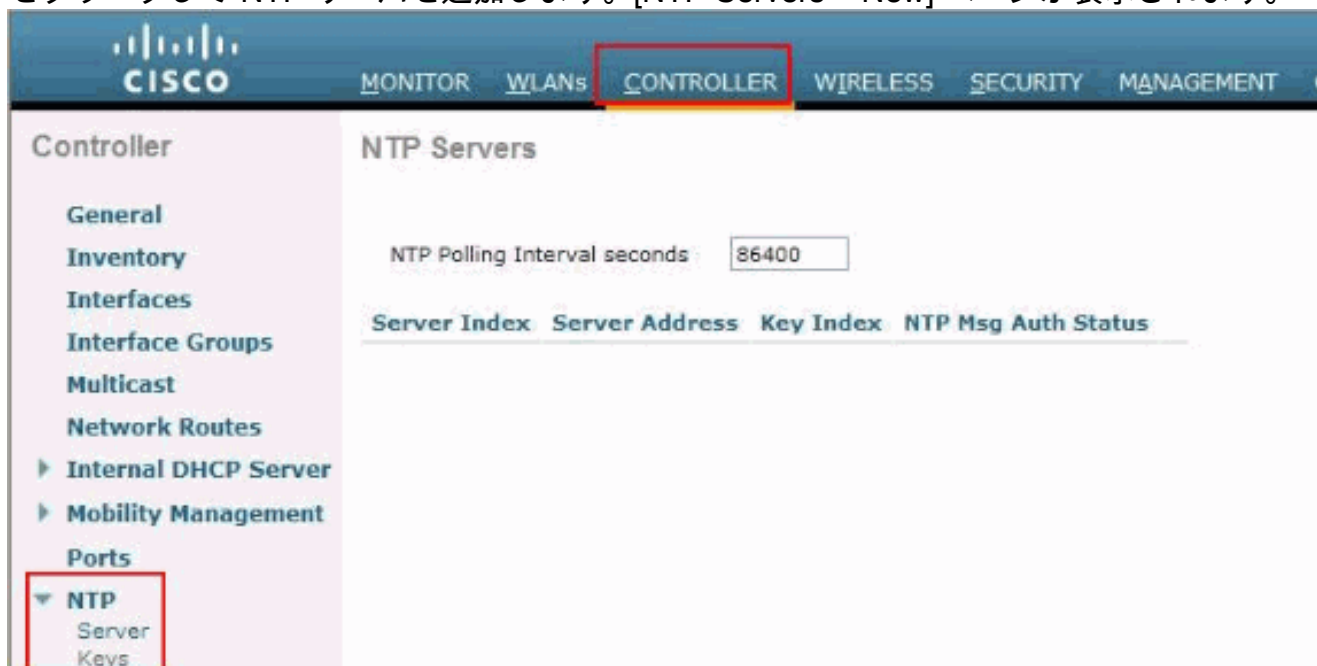
以下は、2800 シリーズ ルータで NTP サーバを設定する例です。このルータは NTP マスターです。つまり、このルータは正規の NTP サーバとして動作します。

```
ntp master
ntp authenticate
ntp authentication-key 1 md5 0305480F0008 7
ntp trusted-key 1
```

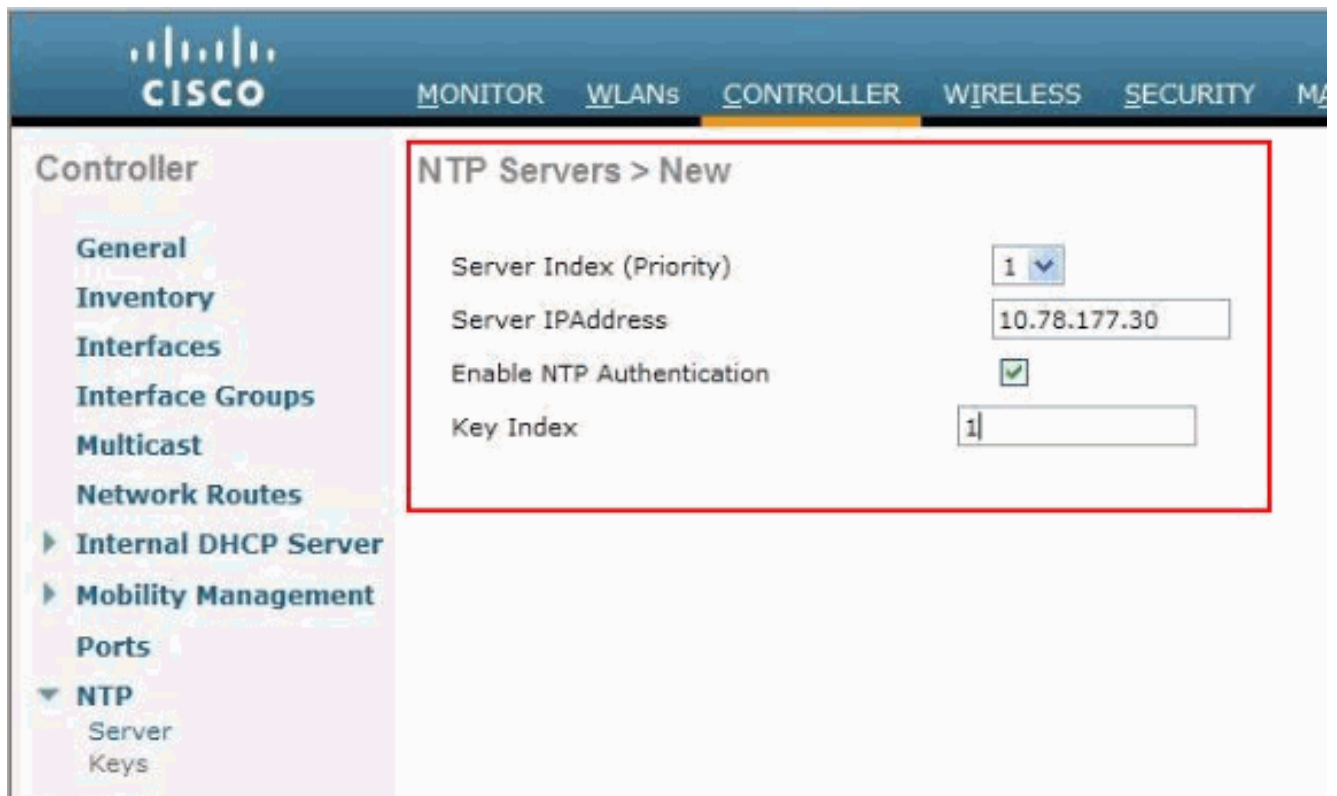
NTP サーバ用の WLC の設定

7.0.116.0 リリース以降、コントローラと NTP サーバの間でも認証チャンネルを設定できるようになりました。コントローラの GUI を使用して NTP 認証を設定するには、次の手順を実行します。

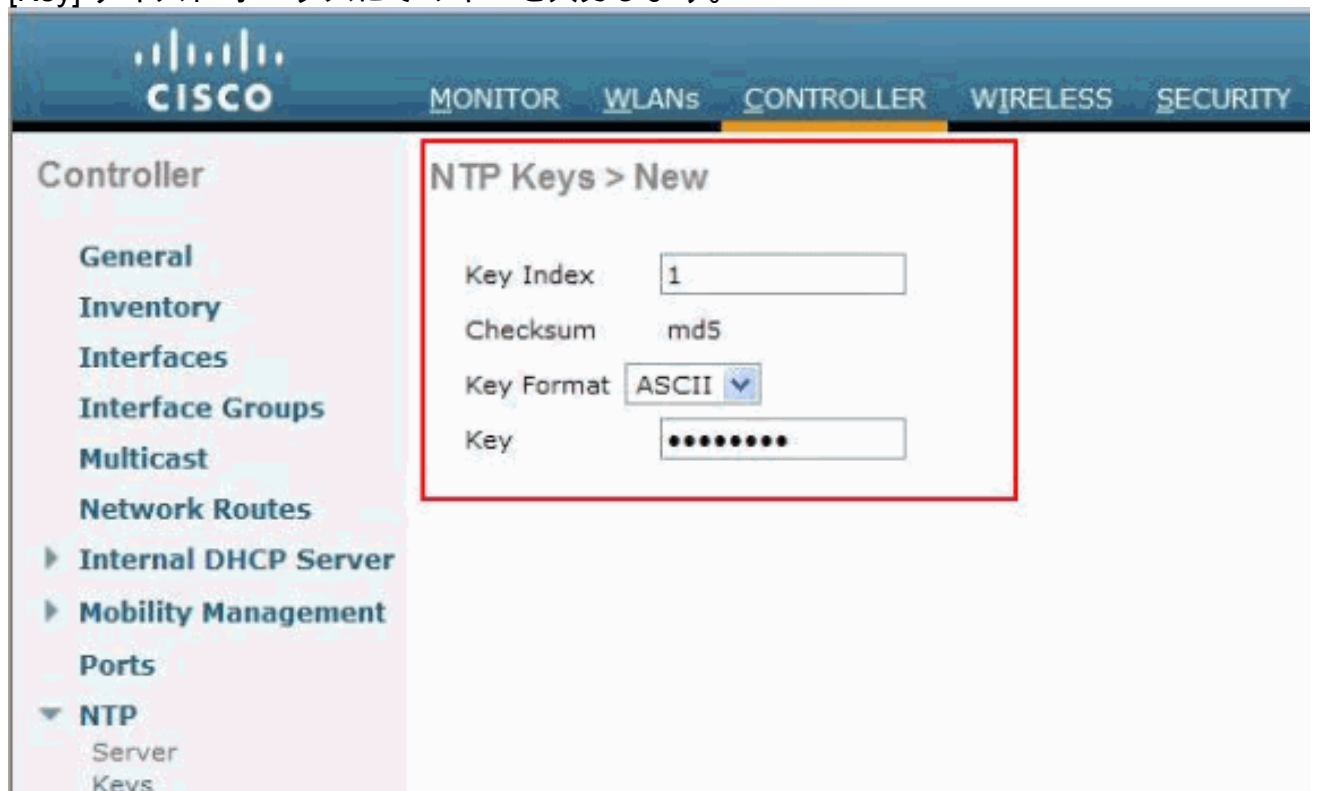
1. [Controller] > [NTP] > [Servers] の順に選択して、[NTP Servers] ページを開きます。[New] をクリックして NTP サーバを追加します。[NTP Servers > New] ページが表示されます。



2. [Server Index (Priority)] ドロップダウン リストからサーバの優先度を選択します。
3. [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。
4. [NTP Server Authentication] チェックボックスを選択して、NTP サーバの認証を有効にします。



5. [Apply] をクリックします。
6. [Controller] > [NTP] > [Keys] を選択します。
7. [New] をクリックして新しいキーを作成します。
8. [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。
9. [Key Format] ドロップダウン リストからキーの形式を選択します。
10. [Key] テキスト ボックスにそのキーを入力します。



確認

WLC の CLI から次のコマンドを使用し、設定を確認できます。

```
(Cisco Controller) >show time Time..... Wed Nov 23
15:31:27 2011 Timezone delta..... 0:0 Timezone
location..... (GMT -6:00) Central Time (US and Canada) NTP Servers
NTP Polling Interval..... 86400 Index NTP Key Index NTP Server NTP Msg Auth
Status ----- 1 1 10.78.177.30
AUTH SUCCESS
```

トラブルシューティング

NTP サーバ設定を WLC で行ってから発生した一連のイベントを表示するには、**debug ntp detail enable** コマンドを使用します。

```
*sntpReceiveTask: Nov 23 15:08:24.360: Started=3531049704.360568 2011 Nov 23 15:08:24.360
*sntpReceiveTask: Nov 23 15:08:24.360: Looking for the socket addresses
*sntpReceiveTask: Nov 23 15:08:24.360: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6.
  Outgoing packet on NTP Server on socket 0:
*sntpReceiveTask: Nov 23 15:08:24.360: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000
*sntpReceiveTask: Nov 23 15:08:24.361: ori=0.000000 rec=0.000000
*sntpReceiveTask: Nov 23 15:08:24.361: tra=3531049704.360889 cur=3531049704.360889
*sntpReceiveTask: Nov 23 15:08:24.361: Host Supports NTP authentication with Key Id = 1
*sntpReceiveTask: Nov 23 15:08:24.361: NTP Auth Key Id = 1 Key Length = 5
*sntpReceiveTask: Nov 23 15:08:24.361: MD5 Hash and Key Id added in NTP Tx packet
*sntpReceiveTask: Nov 23 15:08:24.361: Flushing outstanding packets
*sntpReceiveTask: Nov 23 15:08:24.361: Flushed 0 packets totalling 0 bytes
*sntpReceiveTask: Nov 23 15:08:24.361: Packet of length 68 sent to 10.78.177.30 UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: Packet of length 68 received from 10.78.177.30
UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: KeyId In Recieved NTP Packet 1
*sntpReceiveTask: Nov 23 15:08:24.363: KeyId 1 found in recieved NTP packet exists as part of
the trusted Key/s
*sntpReceiveTask: Nov 23 15:08:24.363: The NTP trusted Key Id 1 length = 5
*sntpReceiveTask: Nov 23 15:08:24.363: NTP Message Authentication - SUCCESS *sntpReceiveTask:
Nov 23 15:08:24.363: sta=0 ver=3 mod=4 str=8 pol=8 dis=3.875031 ref=3531071269.384065
*sntpReceiveTask: Nov 23 15:08:24.363: ori=3531049704.360889 rec=3531071270.103183
*sntpReceiveTask: Nov 23 15:08:24.363: tra=3531071270.103387 cur=3531049704.363251
```

関連情報

- [Network Time Protocol : ベスト プラクティスのホワイト ペーパー](#)
- [Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0.116.0](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)