NTP on Wireless LAN Controllers Configuration Example

Document ID: 113334

Contents

Introduction

This document explains how to configure wireless LAN controllers (WLCs) for synchronizing the date and time with a Network Time Protocol (NTP) server.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of the configuration of lightweight access points (LAPs) and Cisco WLCs
- Basic knowledge of NTP

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4400 WLC that runs software version 7.0.116.0
- Cisco 1230AG Series LAPs
- Cisco 2800 Series Router that runs Cisco IOS® Software release 12.4(11)T

The information in this document is based on these software and hardware versions:

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Managing System Date and Time on the Wireless LAN Controller

On a WLC, the system date and time can be manually configured from the WLC or configured to obtain the date and time from an NTP server.

The system date and time can be manually configured using the CLI configuration wizard or the WLC GUI/CLI. This document provides a configuration example for synchronizing the WLC system date and time through an NTP server.

NTP is an Internet protocol used to synchronize the clocks of computers to some time reference. RFC 1305 provides detailed information on NTP v3 implementation. An NTP network usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. An NTP client makes a transaction with its server over the polling interval (from 64 to 1024 seconds), which dynamically changes over time depending on the network conditions between the NTP server and the client. The other situation occurs when the router communicates to a bad NTP server (for example, NTP server with large dispersion). The router also increases the poll interval. No more than one NTP transaction per minute is needed to synchronize two machines. It is not possible to adjust the NTP poll interval on a router.

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. For example, a stratum 1 time server has a radio or atomic clock directly attached to it. It then sends its time to a stratum 2 time server through NTP, and so forth.

For more information on the best practices for NTP deployment, refer to Network Time Protocol: Best Practices White Paper. The example in this document uses a Cisco 2800 router as an NTP server. The WLC is configured to synchronize its date and time with this NTP server.

Configure

Configuring the Cisco 2800 series router as an NTP server

Configuring the Router as an Authoritative NTP Server

Use this command in global configuration mode if you want the system to be an authoritative NTP server, even if the system is not synchronized to an outside time source:

```
ntp master

!--- Makes the system an authoritative NTP server
```

Configuring NTP Authentication

If you want to authenticate the associations with other systems for security purposes, use the commands that follow. The first command enables the NTP authentication feature. The second command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently, the only key type supported is md5. Third, a list of "trusted" authentication keys is defined. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets. In order to configure NTP authentication, use these commands in global configuration mode:

```
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
```

Here is an example NTP Server configuration on the 2800 Series Router. The router is the NTP master, which means the router acts as the authoritative NTP server.

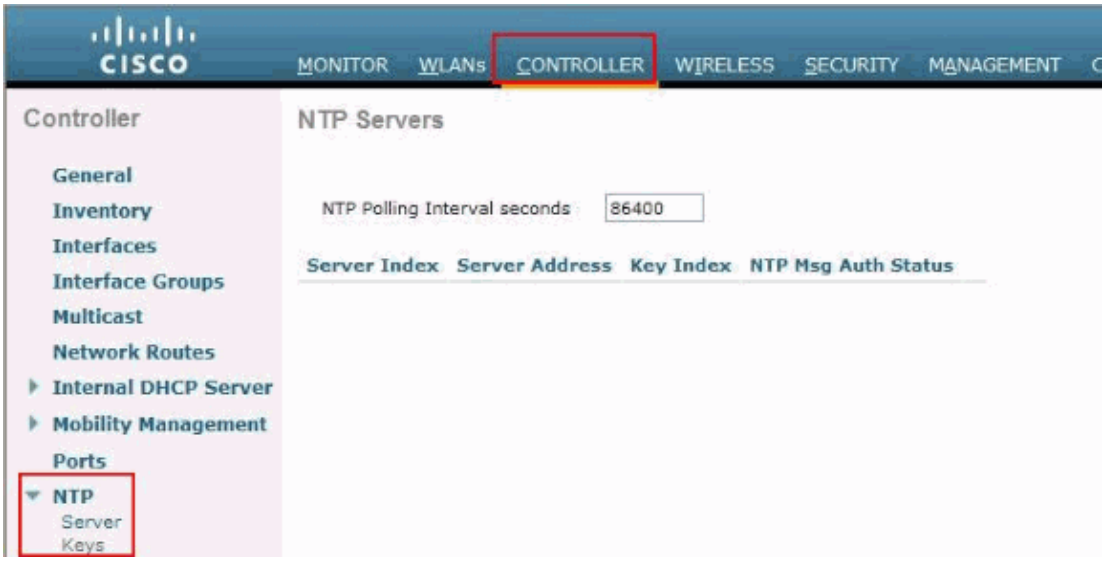
```
ntp master
ntp authenticate
ntp authentication-key 1 md5 0305480F0008 7
ntp trusted-key 1
```

Configuring the WLC for the NTP server

Starting with the 7.0.116.0 release, you can also configure an authentication channel between the controller and the NTP server. In order to configure NTP authentication using the controller GUI, perform these steps:

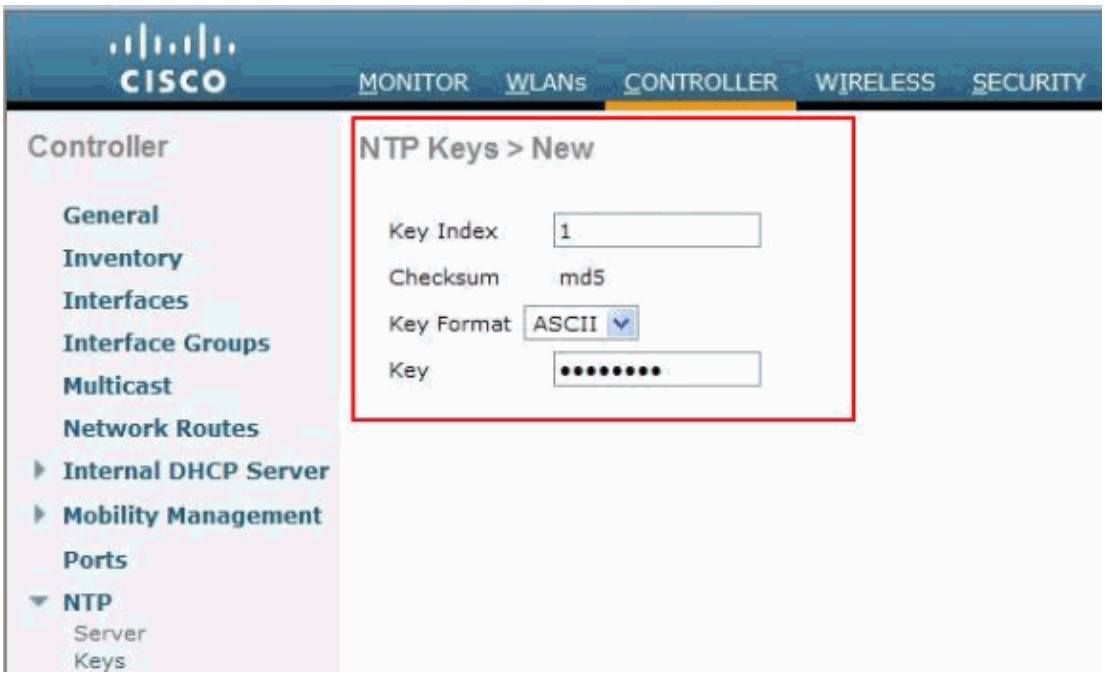
1. Choose **Controller > NTP > Servers** to open the NTP Servers page. Click **New** to add an NTP server.

   The **NTP Servers > New page** appears.



2. Choose a server priority from the **Server Index (Priority)** drop−down list.
3. Enter the NTP server IP Address in the **Server IPAddress** text box.
4. Enable NTP server authentication by selecting the NTP Server Authentication check box.

5. Click **Apply**.
6. Choose **Controller** > **NTP** > **Keys**.
7. Click **New** to create a key.
8. Enter the key index in the **Key Index** text box.
9. Choose the key format from the **Key Format** drop−down list.
10. Enter the Key in the **Key** text box.



Verify

You can use these commands from the WLC CLI to verify the configuration:

```
(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
```

Troubleshoot

You can use the **debug ntp detail enable** command to view the sequence of events that occur once the NTP server configuration is done on the WLC.

```
*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,
 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=0.0

*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=12
*sntpReceiveTask: Nov 23 15:08:24.363: Packet of length 68 received from 10.78.177.30 UDPp
*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

*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=3531

*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
```

Related Information

- **Network Time Protocol: Best Practices White Paper**
- **Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0**
- **Technical Support & Documentation − Cisco Systems**