在无线局域网控制器上配置NTP

目录

简介

本文档介绍如何配置AireOS无线局域网控制器(WLC)以与网络时间协议(NTP)服务器同步日期和时间。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- Cisco WLC配置的基本知识。
- NTP基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 8.8.110 的 Cisco WLC 3504。

- 运行Cisco IOS®软件版本15.2(6)E2的Cisco Catalyst 3560-CX系列L3交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

在无线LAN控制器上管理系统日期和时间

在WLC上，可以从WLC手动配置系统日期和时间，也可以配置系统从NTP服务器获取日期和时间。

可以在CLI配置向导或WLC GUI/CLI中手动配置系统日期和时间。

本文档提供了一个通过NTP服务器同步WLC系统日期和时间的配置示例。

NTP是一种网络协议，用于通过可变延迟数据网络实现计算机系统之间的时钟同步，以便将计算机的时钟同步到某个时间参考。RFC 1305和RFC 5905分别提供了有关NTPv3和NTPv4实施的详细信息。

NTP网络通常从权威时间源（例如连接到时间服务器的无线电时钟或原子时钟）接收其时间。NTP然后在整个网络中分配此时间。

NTP客户端在轮询间隔内与其服务器进行事务，该轮询间隔随时间动态变化并取决于NTP服务器和客户端之间的网络条件。

NTP使用层的概念描述机器旁边有多少NTP 跳来自可信的时间源。例如，第1层时钟服务器有无线电或原子时钟直接与它连接。然后通过NTP将其时间发送到第2层时间服务器，以此类推。

有关NTP部署的最佳实践的详细信息，请参阅使用网络时间协议的最佳实践。

本文档中的示例使用Cisco Catalyst 3560-CX系列L3交换机作为NTP服务器。WLC配置为与此NTP服务器同步其日期和时间。

配置

网络图

WLC ---- 3560-CX第3层交换机----NTP服务器

配置

将L3交换机配置为授权NTP服务器

如果您希望系统成为授权NTP服务器，即使系统未同步到外部时间源，请在全局配置模式下使用此命令：

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

配置NTP身份验证

如果要出于安全目的验证与其他系统的关联，请使用以下命令。第一个命令启用NTP身份验证功能。

第二个命令定义每个身份验证密钥。每个密钥都有一个密钥编号、类型和值。目前，唯一支持的密钥类型是md5。

第三，定义可信身份验证密钥列表。如果密钥受信任，则此系统已准备好同步到在其NTP数据包中使用此密钥的系统。要配置NTP身份验证，请在全局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交换机上的NTP服务器配置示例。交换机是NTP master，这意味着路由器充当权威NTP服务器，但路由器本身从另一个NTP服务器xxxx.xxx获取时间。

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

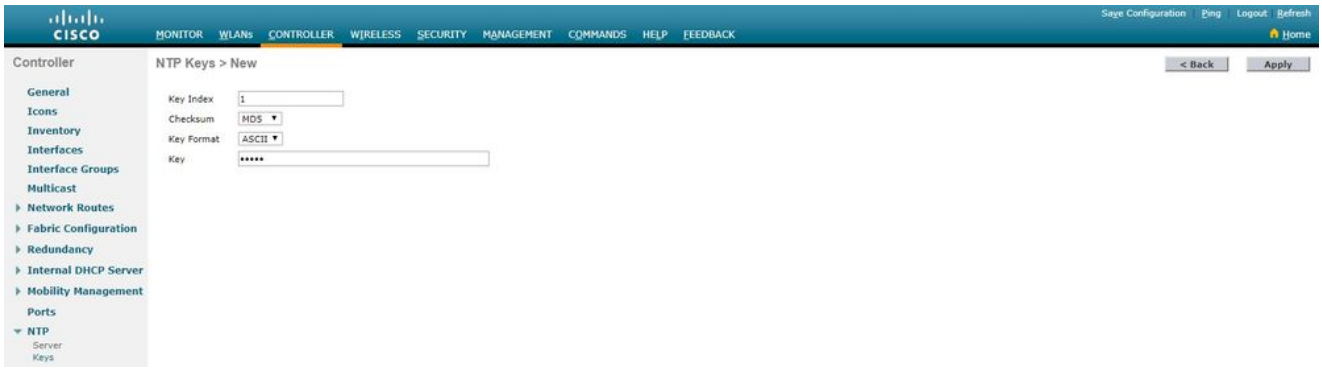
为NTP服务器配置WLC

从版本8.6开始，您可以启用NTPv4。您还可以在控制器和NTP服务器之间配置身份验证通道。

要在控制器GUI中配置NTP身份验证，请执行以下步骤：

1. 选择Controller > NTP > Keys。
2. 单击New以创建密钥。
3. 在“键索引”文本框中输入键索引。
4. 选择Key Checksum（MD5或SHA1）和Key Format下拉列表。

5. 在Key文本框中输入Key:

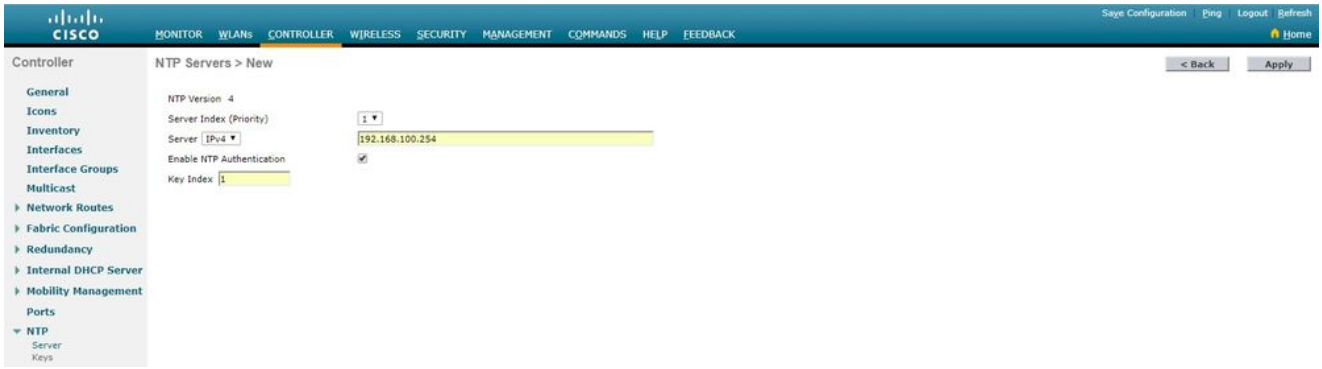


6. 选择Controller > NTP > Servers以打开NTP Servers页面。选择版本3或4，然后单击New以添加NTP服务器。系统将显示NTP Servers > New页面。

7. 选择Server Index(Priority)。

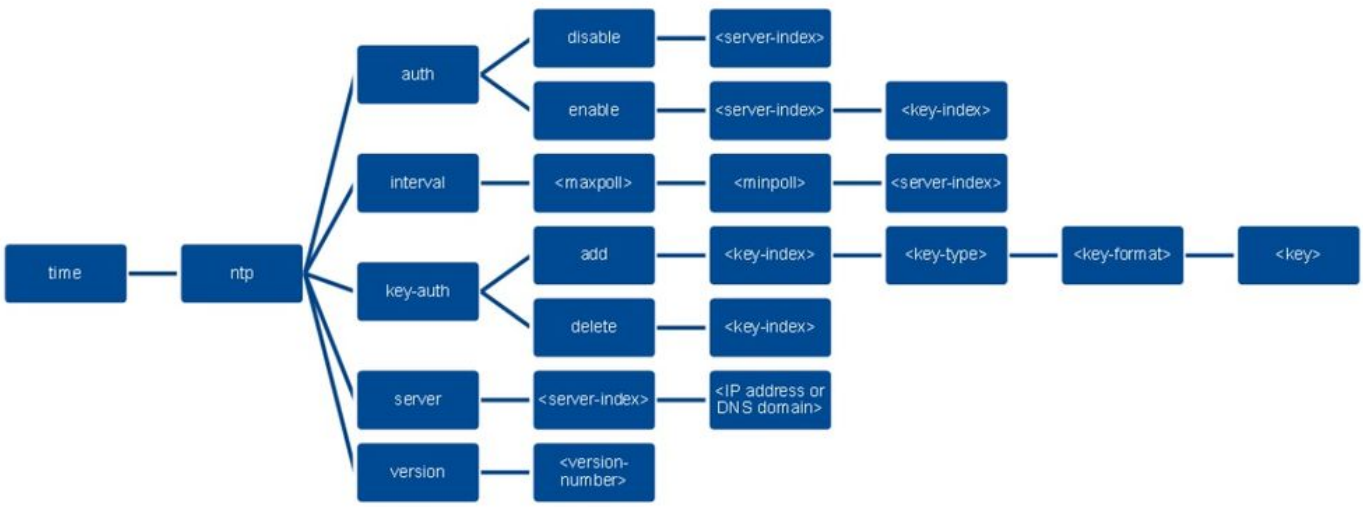
8. 在Server IP Address（服务器IP地址）文本框中输入NTP服务器IP地址。

9. 启用NTP服务器身份验证，选中NTP Server Authentication复选框，并选择之前配置的密钥索引。



10. 单击 Apply。

要通过控制器CLI配置NTP身份验证，请跟踪以下命令树：



```
>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
```

验证

在NTP服务器上

```
#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

当WLC建立通信时：

建立连接后：

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) >
```

故障排除

在运行Cisco IOS的NTP服务器端，您可以使用 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 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) >
```

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。