NTP auf Wireless LAN-Controllern konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die AireOS Wireless LAN-Controller (WLC) so konfigurieren, dass Datum und Uhrzeit mit einem NTP-Server (Network Time Protocol) synchronisiert werden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Grundkenntnisse der Konfiguration des Cisco WLC.
- Grundkenntnisse von NTP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco WLC 3504 mit der Softwareversion 8.8.110.
- Cisco Catalyst L3-Switch der Serie 3560-CX mit Cisco IOS® Software, Version 15.2(6)E2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

möglichen Auswirkungen aller Befehle kennen.

Verwalten von Datum und Uhrzeit auf dem Wireless LAN Controller

Auf einem WLC können Datum und Uhrzeit des Systems manuell über den WLC konfiguriert oder so konfiguriert werden, dass Datum und Uhrzeit von einem NTP-Server abgerufen werden.

Datum und Uhrzeit des Systems können manuell im CLI-Konfigurationsassistenten oder in der WLC-GUI/CLI konfiguriert werden.

Dieses Dokument enthält ein Konfigurationsbeispiel für die Synchronisierung von Datum und Uhrzeit des WLC-Systems über einen NTP-Server.

NTP ist ein Netzwerkprotokoll zur Synchronisierung der Uhren zwischen Computersystemen über Datennetzwerke mit variabler Latenz, um die Uhren von Computern mit einer Zeitreferenz zu synchronisieren. Die Implementierungen RFC 1305 und RFC 5905 bieten detaillierte Informationen zur NTPv3- bzw. NTPv4-Implementierung.

Ein NTP-Netzwerk empfängt seine Zeit normalerweise von einer zuverlässigen Zeitquelle, z. B. einer Funkuhr oder einer Atomuhr, die mit einem Zeitserver verbunden ist. NTP verteilt diese Zeit dann über das Netzwerk.

Ein NTP-Client führt über das Abfrageintervall eine Transaktion mit seinem Server durch, die sich im Laufe der Zeit dynamisch ändert und von den Netzwerkbedingungen zwischen dem NTP-Server und dem Client abhängt.

Das NTP nutzt das Schichtenkonzept, um zu beschreiben, wie viele NTP-Hops ein Rechner von einer maßgeblichen Zeitquelle entfernt ist. Beispielsweise ist ein Schicht-1-Zeitserver direkt mit einer Funk- oder Atomuhr verbunden. Anschließend wird die Uhrzeit über NTP an einen Schicht-2-Zeitserver gesendet usw.

Weitere Informationen zu Best Practices für die NTP-Bereitstellung finden Sie unter Best Practices für die Verwendung des Network Time Protocol.

Im Beispiel in diesem Dokument wird ein Cisco Catalyst L3-Switch der Serie 3560-CX als NTP-Server verwendet. Der WLC ist so konfiguriert, dass Datum und Uhrzeit mit diesem NTP-Server synchronisiert werden.

Konfigurieren

Netzwerkdiagramm

WLC ---- 3560-CX L3 Switch ---- NTP-Server

Konfigurationen

Konfigurieren des L3-Switches als autorisierender NTP-Server

Verwenden Sie diesen Befehl im globalen Konfigurationsmodus, wenn das System ein autoritativer NTP-Server sein soll, auch wenn das System nicht mit einer externen Zeitquelle synchronisiert ist:

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

Konfigurieren der NTP-Authentifizierung

Wenn Sie die Zuordnungen zu anderen Systemen aus Sicherheitsgründen authentifizieren möchten, verwenden Sie die folgenden Befehle. Der erste Befehl aktiviert die NTP-Authentifizierungsfunktion.

Mit dem zweiten Befehl wird jeder der Authentifizierungsschlüssel definiert. Jeder Schlüssel hat eine Schlüsselnummer, einen Typ und einen Wert. Derzeit wird nur der Schlüsseltyp md5 unterstützt.

Drittens wird eine Liste vertrauenswürdiger Authentifizierungsschlüssel definiert. Wenn ein Schlüssel vertrauenswürdig ist, kann dieses System mit einem System synchronisiert werden, das diesen Schlüssel in seinen NTP-Paketen verwendet. Um die NTP-Authentifizierung zu konfigurieren, verwenden Sie die folgenden Befehle im globalen Konfigurationsmodus:

```
#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
```

Nachfolgend finden Sie ein Beispiel für die NTP-Serverkonfiguration auf dem L3-Switch der Serie 3560-CX. Der Switch ist das NTP masterd. h. der Router agiert als autoritativer NTP-Server, erhält jedoch selbst die Zeit von einem anderen NTP-Server **xxxx.xxx**.

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

Konfigurieren des WLC für den NTP-Server

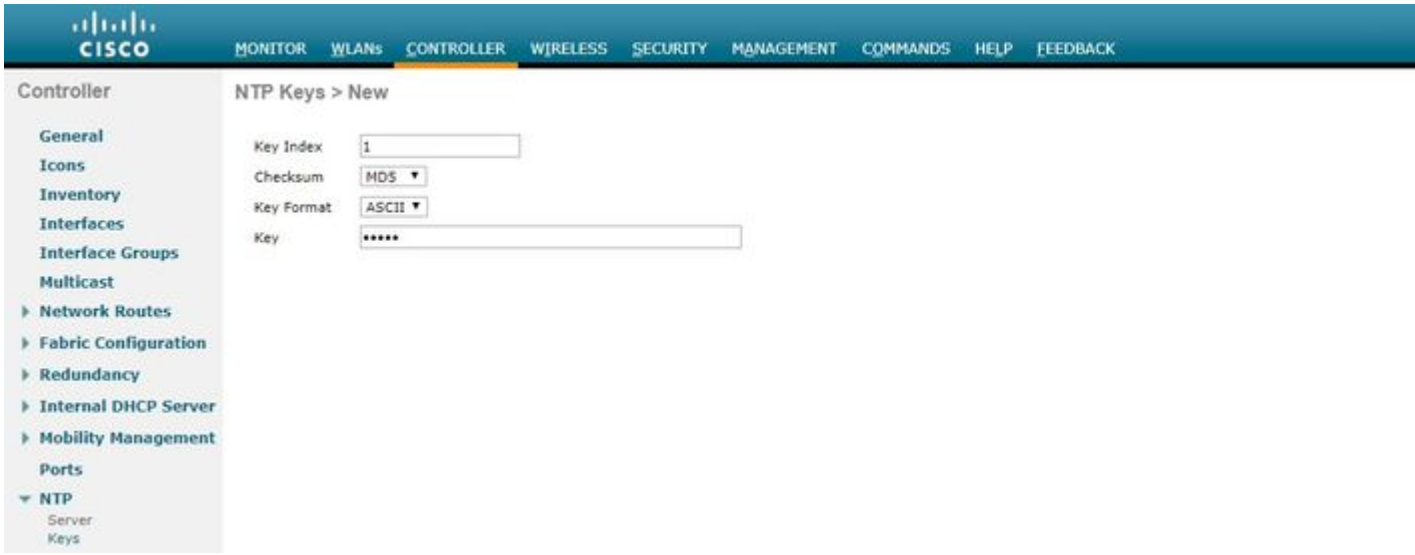
Ab Version 8.6 kann NTPv4 aktiviert werden. Sie können auch einen Authentifizierungskanal zwischen dem Controller und dem NTP-Server konfigurieren.

Führen Sie die folgenden Schritte aus, um die NTP-Authentifizierung in der Benutzeroberfläche des Controllers zu konfigurieren:

1. Wählen Sie **Controller > NTP > Keys aus**.
2. Klicken Sie auf **Neu**, um einen Schlüssel zu erstellen.
3. Geben Sie den Schlüsselindex in das Textfeld **Schlüsselindex** ein.

4. Wählen Sie die **Schlüsselprüfsumme** (MD5 oder SHA1) und die Dropdown-Liste **Schlüsselformat** aus.

5. Geben Sie den Schlüssel in das Textfeld **Schlüssel** ein:

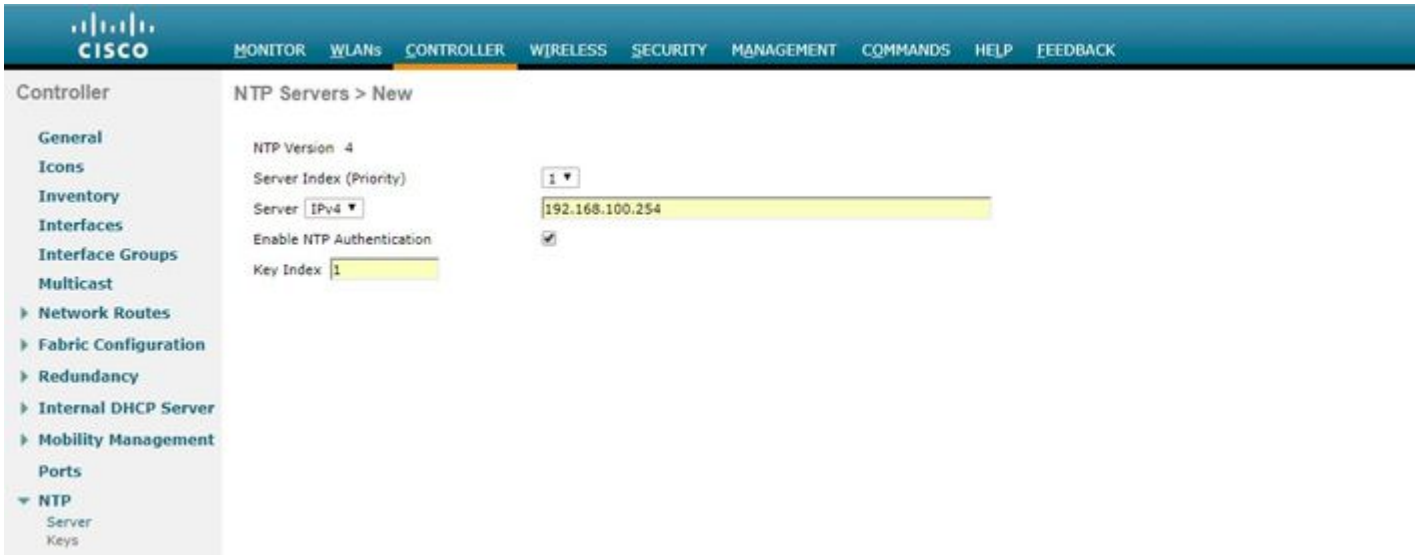


6. Wählen Sie **Controller > NTP > Servers** (Controller > NTP > Server), um die Seite NTP Servers (NTP-Server) zu öffnen. Wählen Sie Version 3 oder 4 aus, und klicken Sie dann auf **Neu**, um einen NTP-Server hinzuzufügen. Die **Seite NTP-Server > Neu** wird angezeigt.

7. Wählen Sie den **Serverindex (Priorität) aus**.

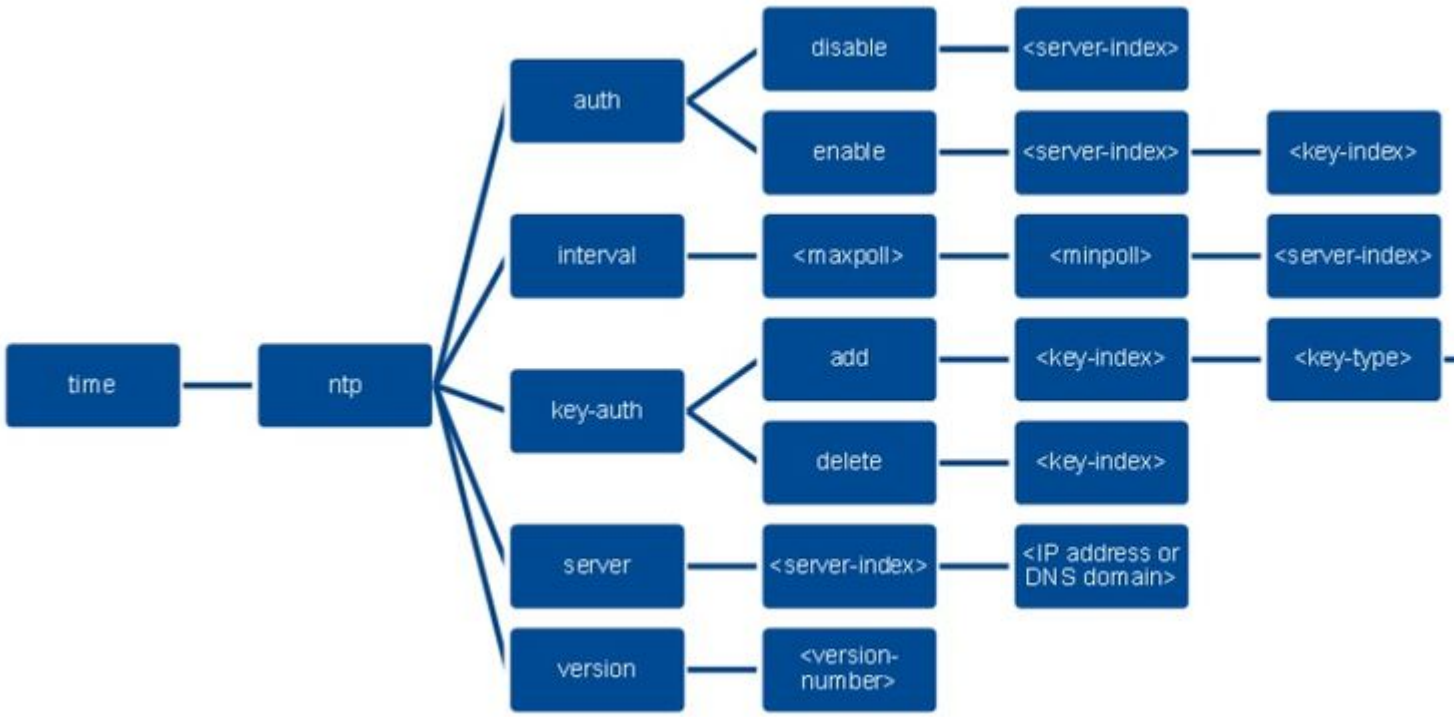
8. Geben Sie die IP-Adresse des NTP-Servers in das Textfeld **Server-IP-Adresse** ein.

9. Aktivieren Sie die NTP-Serverauthentifizierung, aktivieren Sie das Kontrollkästchen **NTP-Serverauthentifizierung**, und wählen Sie den zuvor konfigurierten **Schlüsselindex aus**.



10. Klicken Sie auf Apply (Anwenden).

Um die NTP-Authentifizierung über die CLI des Controllers zu konfigurieren, verfolgen Sie folgenden Befehlsbaum:




```
>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
```

Überprüfung

Auf dem NTP-Server

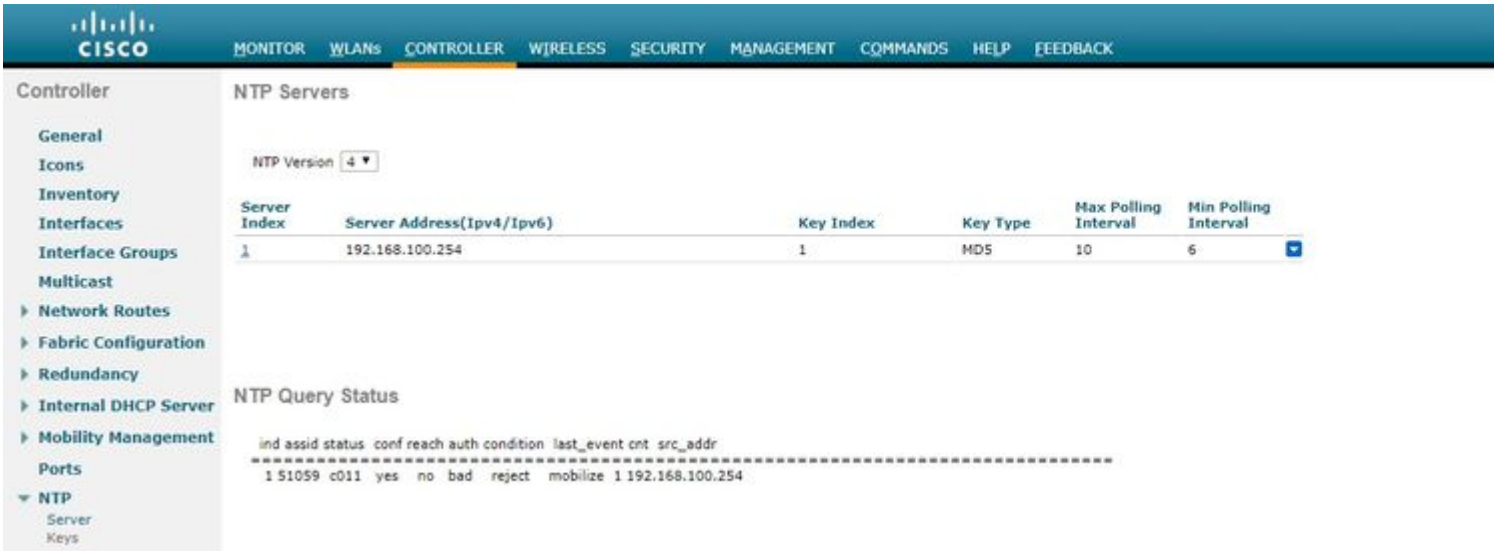
```
#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406 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
```

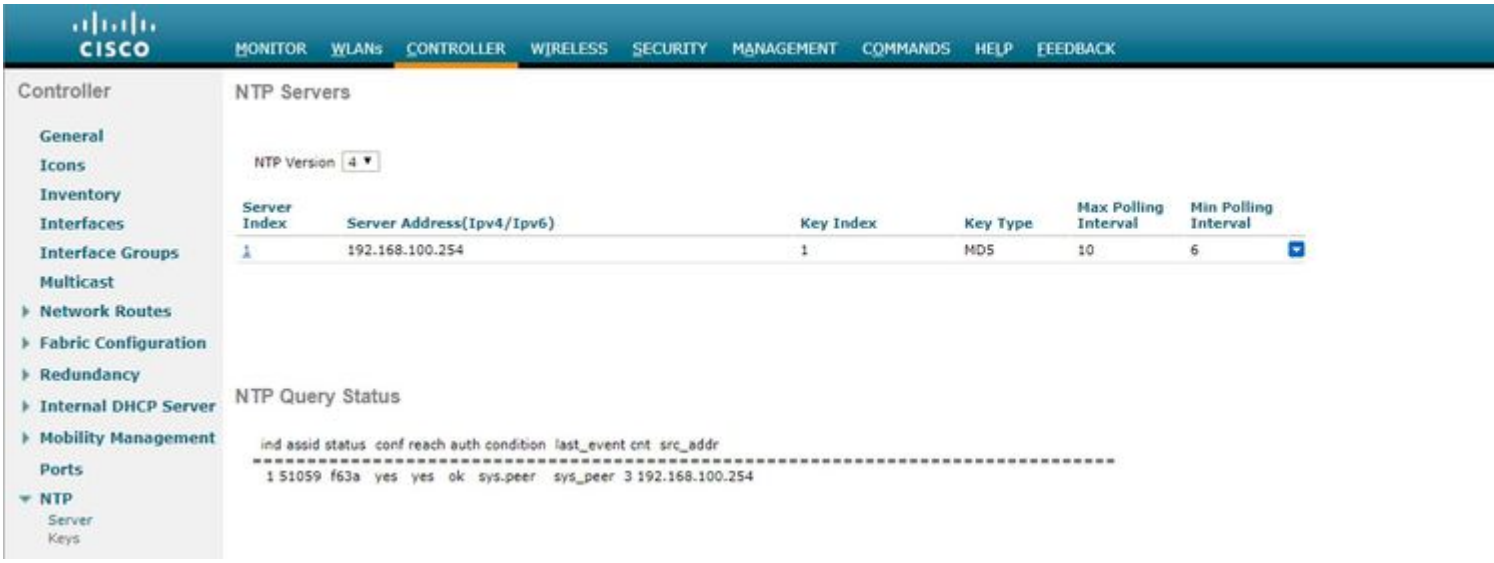
Auf dem WLC

In der GUI

Während der WLC die Kommunikation herstellt:



Nach Herstellung der Verbindung:



In der WLC-CLI

```
(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) >
```

Fehlerbehebung

Auf der NTP-Serverseite, auf der Cisco IOS ausgeführt wird, können Sie debug ntp all enable command:

```
#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).
```

Auf WLC-Seite:

```
 >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 ....2.8
```

```
*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 truste

*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) >
```

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.