Configurazione di NTP sui controller LAN wireless

Sommario

Introduzione

In questo documento viene descritto come configurare i Wireless LAN Controller (WLC) di AireOS per sincronizzare data e ora con un server Network Time Protocol (NTP).

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base della configurazione di Cisco WLC.
- Conoscenze base di NTP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco WLC 3504 con software versione 8.8.10.
- Switch Cisco Catalyst serie 3560-CX L3 con software Cisco IOS® versione 15.2(6)E2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei

comandi.

Gestire la data e l'ora del sistema sul controller LAN wireless

Su un WLC, la data e l'ora del sistema possono essere configurate manualmente dal WLC o configurate per ottenere la data e l'ora da un server NTP.

La data e l'ora del sistema possono essere configurate manualmente nella configurazione guidata CLI o nella GUI/CLI del WLC.

Questo documento fornisce un esempio di configurazione per sincronizzare la data e l'ora del sistema WLC tramite un server NTP.

NTP è un protocollo di rete per la sincronizzazione dell'orologio tra sistemi di computer su reti di dati a latenza variabile per sincronizzare gli orologi dei computer con qualche riferimento temporale. La RFC 1305 e la RFC 5905 forniscono informazioni dettagliate sull'implementazione di NTPv3 e NTPv4, rispettivamente.

Una rete NTP di solito riceve il proprio tempo da una fonte oraria autorevole, come un orologio radio o un orologio atomico collegato a un server di riferimento orario. NTP quindi distribuisce il tempo in rete.

Un client NTP esegue una transazione con il proprio server nell'intervallo di polling, che cambia in modo dinamico nel tempo e dipende dalle condizioni di rete tra il server NTP e il client.

La tecnologia NTP utilizza il concetto di strato per descrivere quanti hop NTP distano una macchina da una fonte temporale autorevole. Ad esempio, un server di riferimento ora di strato 1 ha un orologio radio o atomico direttamente collegato. Quindi invia il suo tempo ad un server di tempo di Stratum 2 attraverso NTP, e così via.

Per ulteriori informazioni sulle procedure consigliate per l'installazione NTP, fare riferimento a Utilizzare le procedure consigliate per il protocollo NTP.

Nell'esempio riportato in questo documento viene usato uno switch Cisco Catalyst serie 3560-CX L3 come server NTP. Il WLC è configurato per sincronizzare la data e l'ora con questo server NTP.

Configurazione

Esempio di rete

WLC â€” Switch 3560-CX L3 â€” Server NTP

Configurazioni

Configurazione dello switch L3 come server NTP autorevole

Utilizzare questo comando in modalità di configurazione globale se si desidera che il sistema sia un server NTP autorevole, anche se il sistema non è sincronizzato con un'origine del tempo esterna:

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

Configura autenticazione NTP

Se si desidera autenticare le associazioni con altri sistemi per motivi di sicurezza, utilizzare i comandi seguenti. Il primo comando attiva la funzione di autenticazione NTP.

Il secondo comando definisce ciascuna chiave di autenticazione. Ogni chiave ha un numero di chiave, un tipo e un valore. Al momento, l'unico tipo di chiave supportato è md5.

In terzo luogo, viene definito un elenco di chiavi di autenticazione attendibili. Se una chiave è attendibile, il sistema è pronto per la sincronizzazione con un sistema che la utilizza nei pacchetti NTP. Per configurare l'autenticazione NTP, utilizzare questi comandi in modalità di configurazione globale:

```
#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
```

Di seguito è riportato un esempio di configurazione del server NTP sullo switch 3560-CX L3. Lo switch è il NTP master, il che significa che il router agisce come server NTP autorevole ma, a sua volta, riceve l'ora da un altro server NTP **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
```

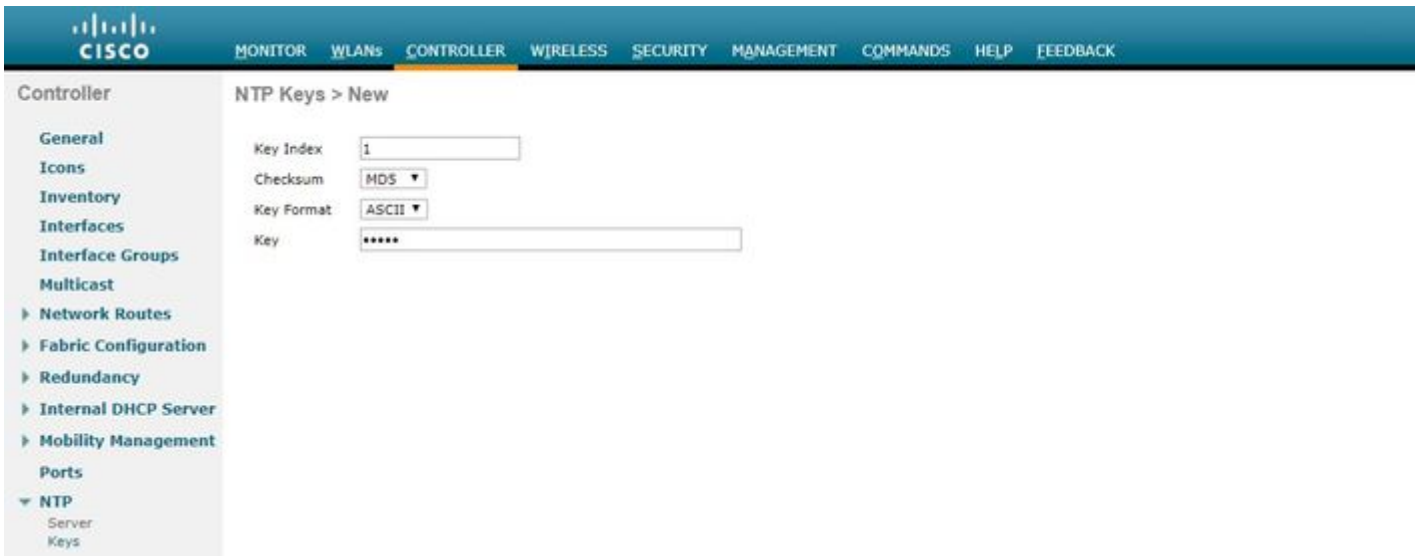
Configurare il WLC per il server NTP

A partire dalla versione 8.6 è possibile abilitare NTPv4. È inoltre possibile configurare un canale di autenticazione tra il controller e il server NTP.

Per configurare l'autenticazione NTP nell'interfaccia utente del controller, attenersi alla seguente procedura:

1. Scegliete **Controller** > **NTP** > **Chiavi**.
2. Fare clic su **Nuovo** per creare una chiave.
3. Immettere l'indice di chiave nella casella di testo **Indice chiave**.
4. Selezionare il **checksum** della **chiave** (MD5 o SHA1) e l'elenco a discesa **Formato chiave**.

5. Immettete la Chiave nella casella di testo **Chiave**:

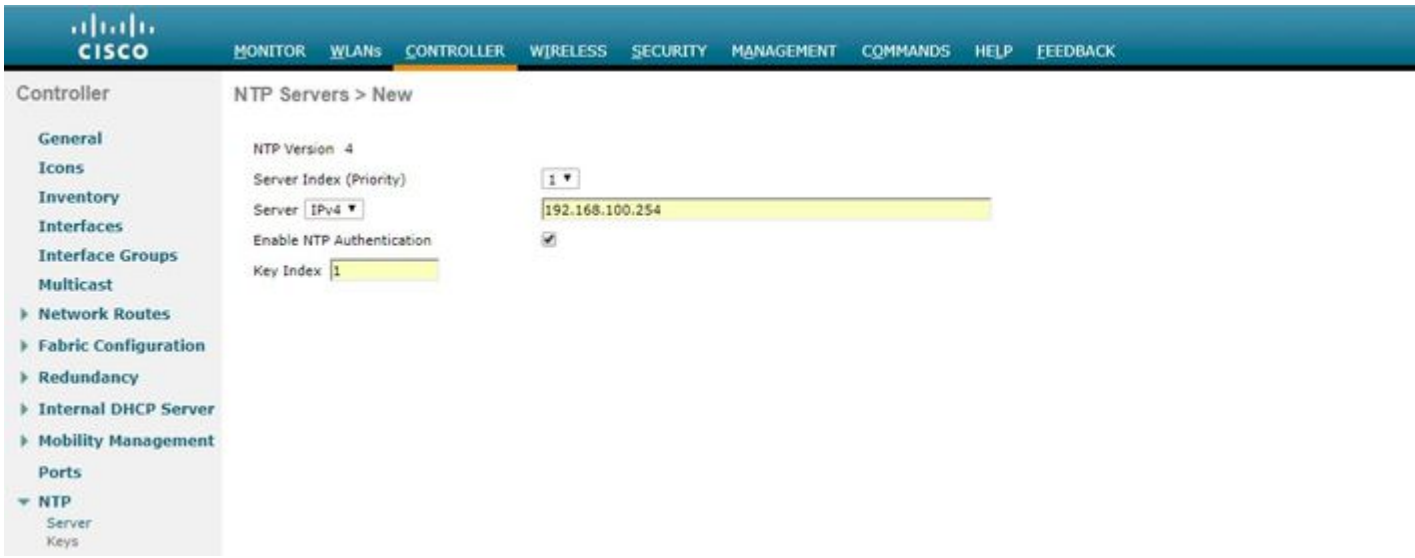


6. Scegliere **Controller > NTP > Server** per aprire la pagina Server NTP. Selezionare la versione 3 o 4, quindi fare clic su **Nuovo** per aggiungere un server NTP. Viene visualizzata la **pagina Server NTP > Nuovo**.

7. Selezionare l'**indice del server (priorità)**.

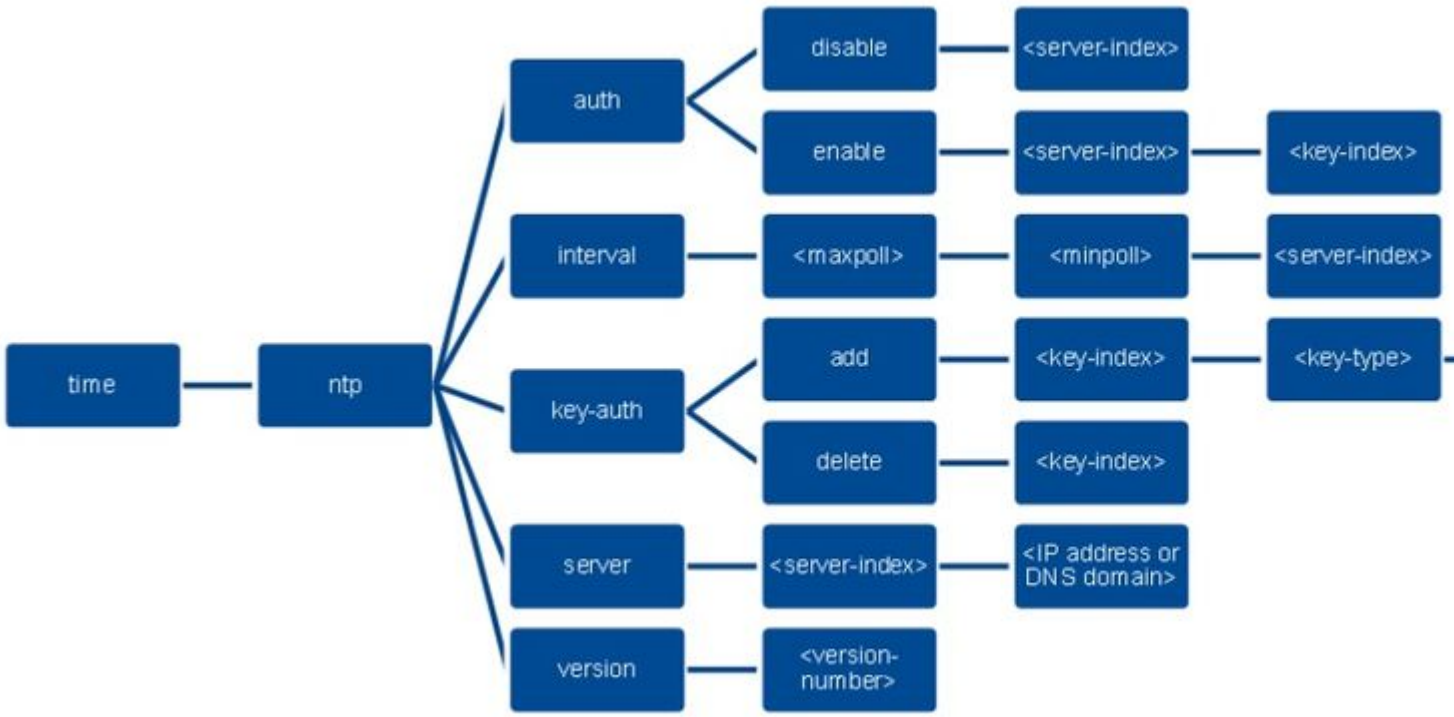
8. Immettere l'indirizzo IP del server NTP nella casella di testo **Indirizzo IP server**.

9. Abilitare l'autenticazione del server NTP, selezionare la casella di controllo **Autenticazione server NTP** e selezionare l'**indice chiavi** configurato in precedenza.



10. Fare clic su Apply (Applica).

Per configurare l'autenticazione NTP tramite la CLI del controller, tenere traccia di questo albero dei comandi:




```
>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
```

Verifica

Sul server NTP

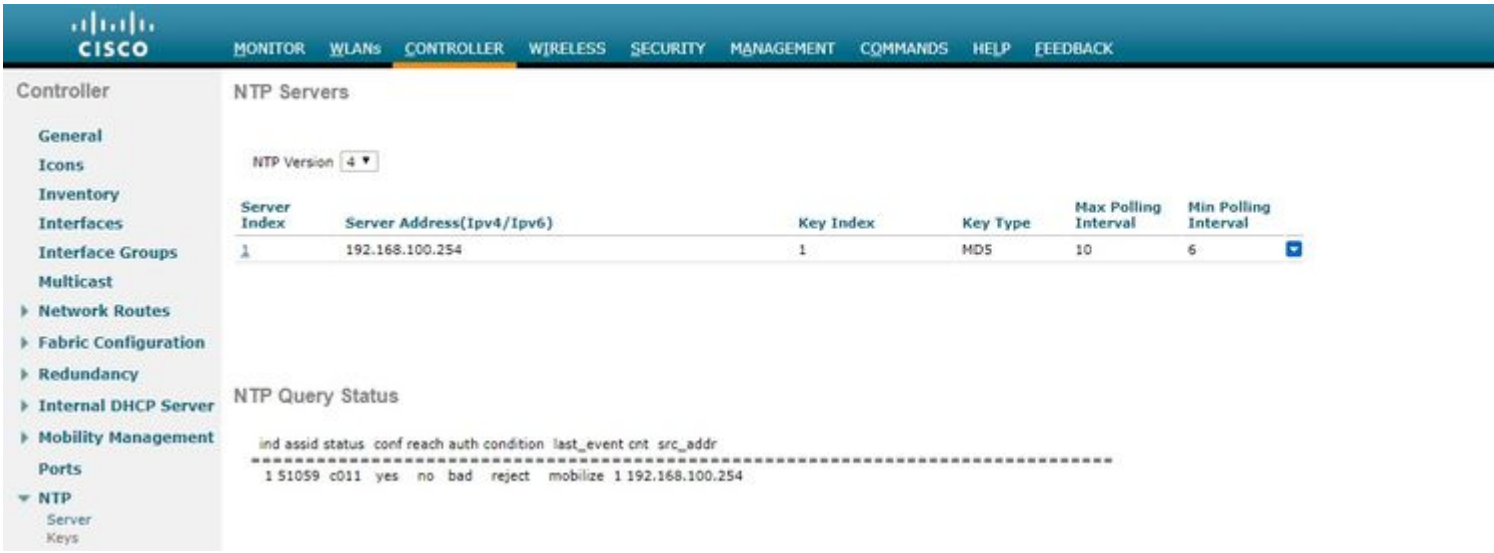
```
#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406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

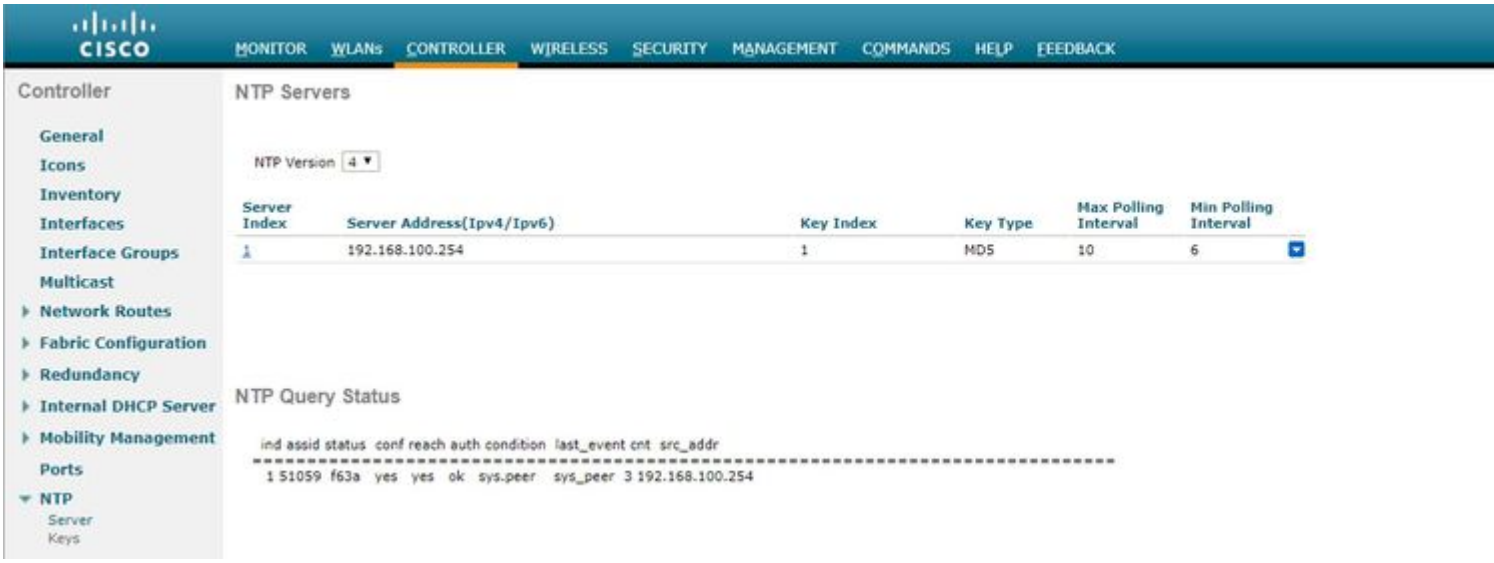
Sul WLC

Nella GUI

Mentre il WLC stabilisce la comunicazione:



Dopo aver stabilito la connessione:



Nella CLI del WLC

```
(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) >
```

Risoluzione dei problemi

Sul lato server NTP con Cisco IOS è possibile utilizzare debug ntp all enable comando:

```
#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).
```

Sul lato WLC:

```
 >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) >
```

Informazioni correlate

- **Supporto tecnico e download Cisco**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).