Configurar o NTP em controladores de LAN sem fio

Contents

Introduction

Este documento descreve como configurar Controladoras Wireless LAN (WLC) AireOS para sincronizar data e hora com um servidor Network Time Protocol (NTP).

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico da configuração do Cisco WLC.
- Conhecimento básico de NTP.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco WLC 3504 que executa a versão de software 8.8.110.
- Switch Cisco Catalyst 3560-CX Series L3 que executa o Cisco IOS® Software versão 15.2(6)E2.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Gerencie a data e a hora do sistema no Wireless LAN Controller

Em uma WLC, a data e a hora do sistema podem ser configuradas manualmente na WLC ou configuradas para obter a data e a hora de um servidor NTP.

A data e a hora do sistema podem ser configuradas manualmente no assistente de configuração da CLI ou na GUI/CLI da WLC.

Este documento fornece um exemplo de configuração para sincronizar a data e a hora do sistema WLC através de um servidor NTP.

O NTP é um protocolo de rede para sincronização de relógio entre sistemas de computadores em redes de dados de latência variável para sincronizar os relógios dos computadores com alguma referência de tempo. O RFC 1305 e o RFC 5905 fornecem informações detalhadas sobre a implementação de NTPv3 e NTPv4, respectivamente.

Uma rede NTP geralmente recebe seu tempo de uma fonte de tempo autorizada, como um rádio-relógio ou um relógio atômico conectado a um servidor de tempo. Em seguida, o NTP distribui esse tempo pela rede.

Um cliente NTP faz uma transação com seu servidor durante o intervalo de poll, que muda dinamicamente com o tempo e depende das condições de rede entre o servidor NTP e o cliente.

O NTP usa o conceito de um stratum para descrever quantos saltos de distância NTP uma máquina está de uma fonte de tempo autoritativa. Por exemplo, um servidor de tempo stratum 1 tem um rádio ou relógio atômico diretamente conectado a ele. Em seguida, ele envia seu horário para um servidor de horário de estrato 2 por meio do NTP e assim por diante.

Para obter mais informações sobre as práticas recomendadas para implantação de NTP, consulte Usar Melhores Práticas para o Network Time Protocol.

O exemplo neste documento usa um Cisco Catalyst 3560-CX Series L3 Switch como um servidor NTP. A WLC está configurada para sincronizar sua data e hora com este servidor NTP.

Configurar

Diagrama de Rede

Switch WLC ---- 3560-CX L3 ---- servidor NTP

Configurações

Configure o Switch L3 como um servidor NTP autoritativo

Use este comando no modo de configuração global se quiser que o sistema seja um servidor NTP autoritativo, mesmo que o sistema não esteja sincronizado com uma origem de tempo externa:

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

Configurar autenticação NTP

Se quiser autenticar as associações com outros sistemas para fins de segurança, use os comandos a seguir. O primeiro comando ativa o recurso de autenticação NTP.

O segundo comando define cada chave de autenticação. Cada chave tem um número de chave, um tipo e um valor. Atualmente, o único tipo de chave suportado é md5.

Terceiro, uma lista de chaves de autenticação confiáveis é definida. Se uma chave for confiável, o sistema estará pronto para sincronizar com um sistema que usa essa chave em seus pacotes NTP. Para configurar a autenticação NTP, use estes comandos no modo de configuração global:

```
#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
```

Aqui está um exemplo de configuração do servidor NTP no Switch 3560-CX L3. O switch é o NTP master, o que significa que o roteador atua como o servidor NTP autoritativo, mas obtém o tempo de outro servidor NTP **xxxx.xxx**.

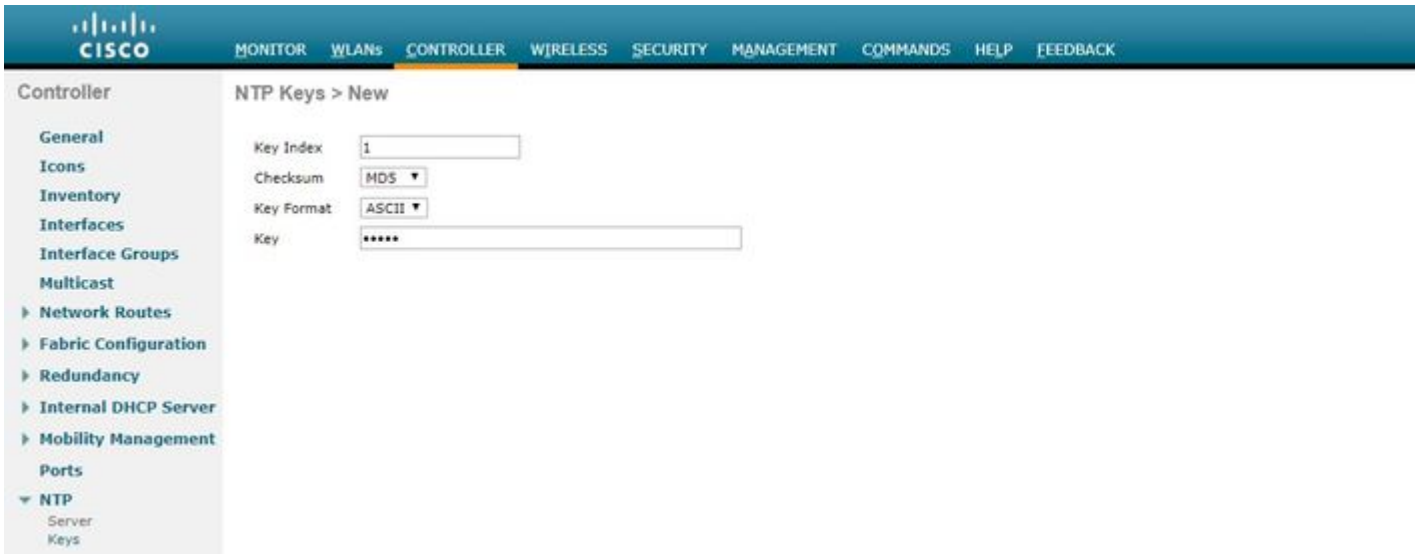
```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server xxxx.xxx
```

Configurar a WLC para o servidor NTP

A partir da versão 8.6, você pode habilitar o NTPv4. Você também pode configurar um canal de autenticação entre o controlador e o servidor NTP.

Para configurar a autenticação NTP na GUI do controlador, execute estas etapas:

1. Escolha **Controller > NTP > Keys**.
2. Clique em **Novo** para criar uma chave.
3. Insira o índice de chave na caixa de texto **Índice de chave**.
4. Escolha a soma de verificação da chave (MD5 ou SHA1) e a lista suspensa **Formato da chave**.
5. Insira a chave na caixa de texto **Chave**:

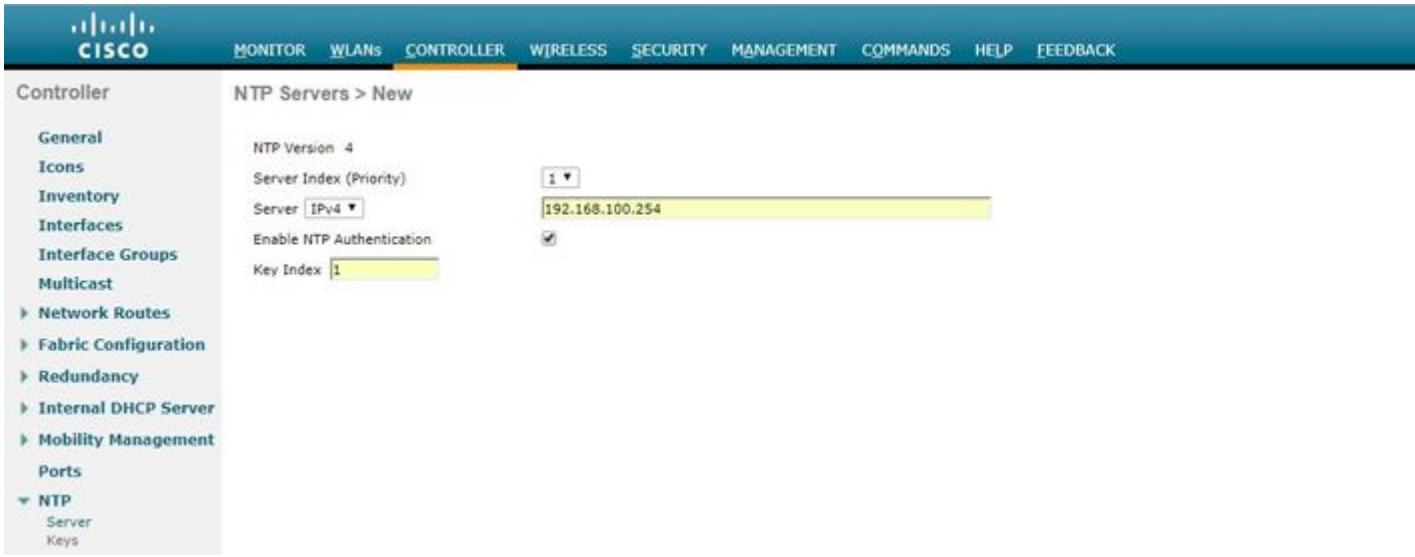


6. Escolha **Controller > NTP > Servers** para abrir a página NTP Servers. Selecione a versão 3 ou 4 e clique em **Novo** para adicionar um servidor NTP. A página **Servidores NTP > Novo** é exibida.

7. Selecione o **Índice de servidores (prioridade)**.

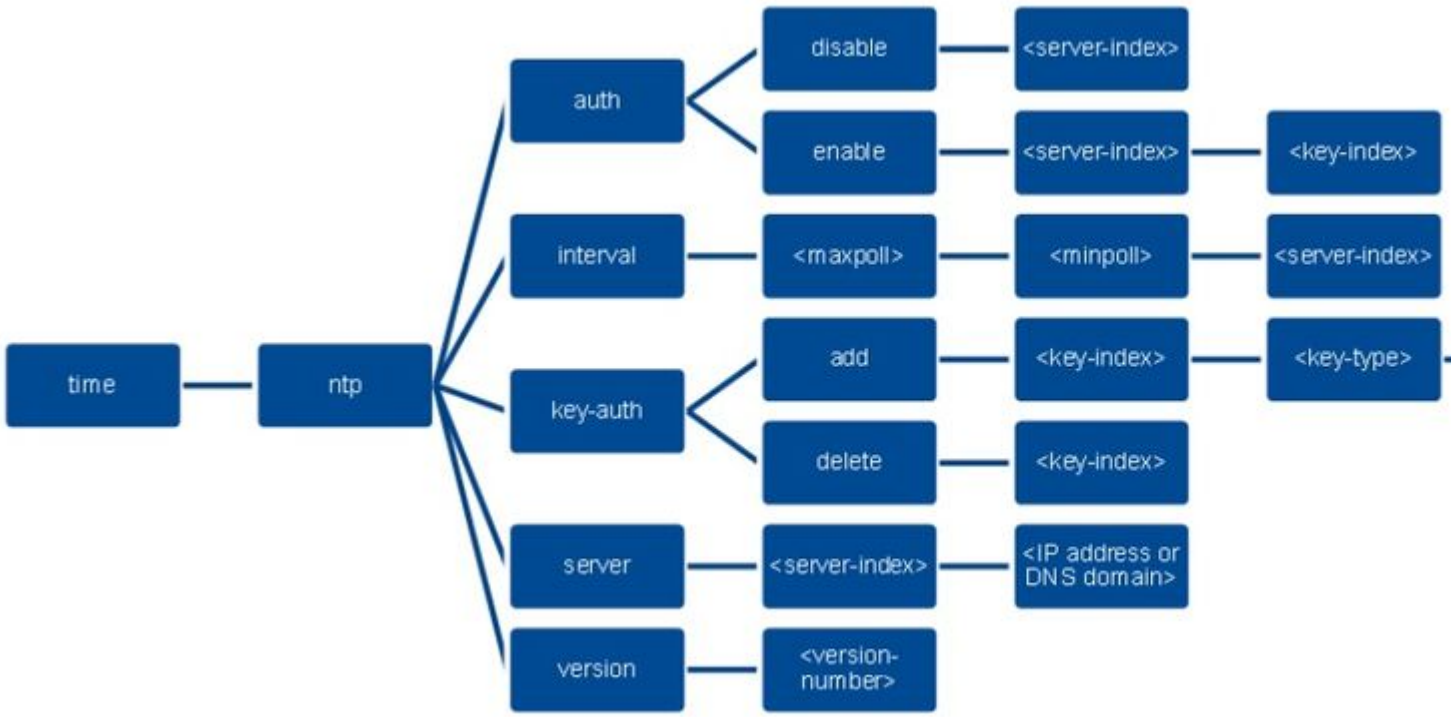
8. Insira o endereço IP do servidor NTP na caixa de texto **Endereço IP do servidor**.

9. Habilite a autenticação do servidor NTP, marque a caixa de seleção **Autenticação do servidor NTP** e selecione o **Índice de chave** configurado anteriormente.



10. Clique em Apply.

Para configurar a autenticação NTP através da CLI do controlador, rastreie esta árvore de comandos:




```
>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
```

Verificar

No servidor NTP

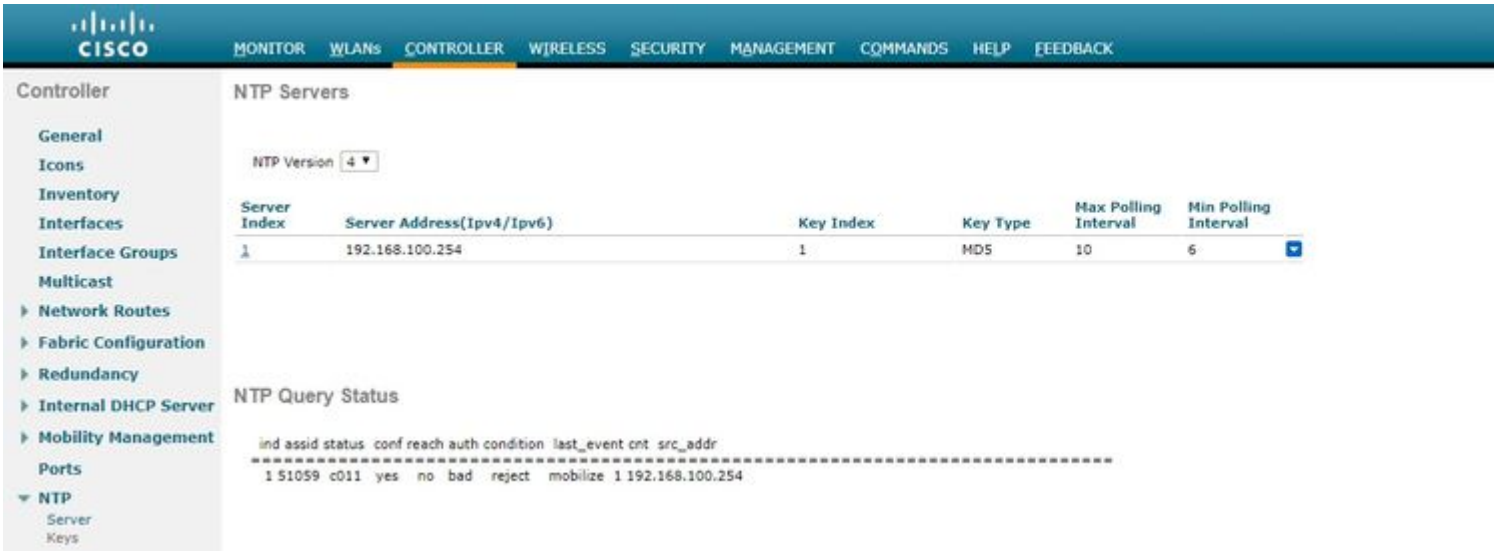
```
#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406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

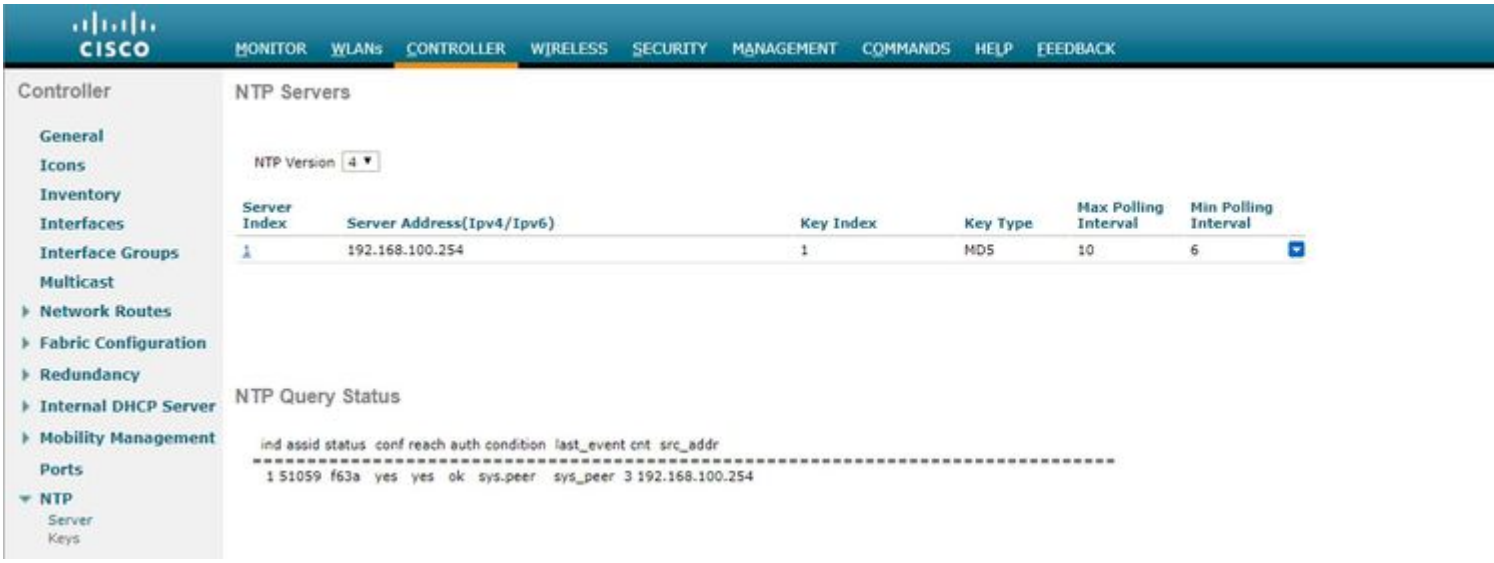
Na WLC

Na GUI

Enquanto a WLC estabelece a comunicação:



Após o estabelecimento da conexão:



Na CLI da 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) >
```

Troubleshoot

No lado do servidor NTP que executa o Cisco IOS, você pode usar 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).
```

No lado da 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) >
```

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.