Solucionar y depurar problemas del protocolo de tiempo de la red (NTP)

Contenido

Introducción

Este documento describe cómo resolver problemas de protocolo de tiempo de la red (NTP) con debug comandos y el show ntp comando.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Comandos show del NTP

Antes de analizar la causa de los problemas de NTP, debe comprender el uso y la salida de estos comandos:

- show ntp association
- show ntp association detail
- show ntp status

Nota: Utilice la Command Lookup Tool para obtener más información sobre los comandos utilizados en esta sección. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas.

Nota: La herramienta Output Interpreter Tool admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas.

show ntp association

Una asociación de NTP puede ser una asociación de pares (un sistema puede sincronizarse con otro sistema o permitir que otro sistema se sincronice con él) o una asociación de servidores (solo un sistema se sincroniza con otro sistema y esto no ocurre al revés).

Este es un ejemplo del resultado del comando show ntp association:

```
CLA_PASA#sh ntp association
      address         ref clock      st  when  poll reach  delay  offset    disp
 ~10.127.7.1       10.127.7.1       9    50    64  377     0.0    0.00     0.0
 ~10.50.44.69      10.50.36.106      5  21231  1024   0      3.8   -4.26  16000.
```

```
+~10.50.44.101     10.50.38.114      5    57    64    1     3.6   -4.30  15875.
+~10.50.44.37      10.50.36.50       5     1   256  377     0.8    1.24     0.2
 ~10.50.44.133     10.50.38.170      5  12142  1024    0     3.2    1.24  16000.
+~10.50.44.165     10.50.38.178      5    35   256  357     2.5   -4.09     0.2
+~10.50.38.42      10.79.127.250     4     7   256  377     0.8   -0.29     0.2
*~10.50.36.42      10.79.127.250     4   188   256  377     0.7   -0.17     0.3
+~10.50.38.50      10.79.127.250     4    42   256  377     0.9    1.02     0.4
+~10.50.36.50      10.79.127.250     4    20   256  377     0.7    0.87     0.5
 * primary (synced), # primary (unsynced), + selected, - candidate, ~ configured
```

Término	Explicación
	Los caracteres antes de la dirección tienen las siguientes definiciones: * Sincronizado con este par. # Casi sincronizado con este par. + Par seleccionado para posible sincronización. - El par es un candidato para la selección. ~ El par está configurado estáticamente.
address (dirección)	Esta es la dirección IP del par. En el ejemplo, la primera entrada muestra 127.127.7.1. Esto indica que la máquina local se ha sincronizado consigo misma. Generalmente, sólo un primario NTP se sincroniza consigo mismo.
ref clock (reloj de referencia)	Esta es la dirección del reloj de referencia para el par. En el ejemplo, los primeros seis peers/servidores tienen una IP privada como reloj de referencia, por lo que sus principales son probablemente routers, switches o servidores dentro de la red local. Para las últimas cuatro entradas, el reloj de referencia es una IP pública, por lo que sus principales son probablemente una fuente de tiempo pública.
st (estrato)	El NTP utiliza el concepto de estrato para describir a cuántos saltos (NTP) se encuentra una máquina de una fuente de hora autorizada. Por ejemplo, un servidor de tiempo de estrato 1 tiene una radio o un reloj atómico conectados directamente a él. Envía su tiempo a un servidor de tiempo del estrato 2 a través del NTP y así sucesivamente hasta el estrato 16. Una máquina que ejecuta NTP automáticamente elige la máquina con el número de estrato más bajo con el que puede comunicarse y utiliza NTP como su fuente de tiempo.
when (cuándo)	Tiempo desde que el último paquete NTP se recibió desde el par informado en segundos. Este valor debe ser inferior al intervalo de sondeo.
poll (sondeo)	El intervalo de sondeo se informa en segundos. El intervalo generalmente comienza con un mínimo de intervalos de sondeo de 64 segundos. La RFC especifica que no se necesita más de una transacción de NTP por minuto para sincronizar dos máquinas. A medida que NTP se vuelve estable entre un cliente y un servidor, el intervalo de sondeo puede aumentar en pequeños pasos de 64 segundos a 1024 segundos y generalmente se estabiliza en algún punto intermedio. Pero este valor

	cambia dinámicamente según las condiciones de red entre el cliente y el servidor y la pérdida de paquetes NTP. Si un servidor es inalcanzable por algún tiempo, el intervalo de sondeo se incrementa en pasos a 1024 segundos para reducir la sobrecarga de la red. No es posible ajustar el intervalo de sondeo del NTP en un router, ya que el intervalo está determinado por algoritmos heurísticos.
reach (alcance)	El alcance entre pares es una cadena de bits notificada como un valor octal. Este campo muestra si el proceso del NTP recibió los últimos ocho paquetes en el software Cisco IOS®. El proceso del NTP, no solo el router o el switch que recibe los paquetes IP del NTP, recibe, procesa y acepta como válidos los paquetes. El alcance utiliza el intervalo de sondeo durante un tiempo de espera para decidir si se recibió un paquete o no. El intervalo de sondeo es el tiempo que el NTP espera antes de concluir que se perdió un paquete. El tiempo de sondeo puede ser diferente para los distintos pares, por lo que el tiempo anterior a que el alcance decida que un paquete se perdió también puede ser diferente para los distintos pares. En el ejemplo, hay cuatro valores de alcance diferentes: • 377 octal = 11111111 binario, que indica que el proceso del NTP recibió los últimos ocho paquetes. • 0 octal = 00000000, que indica que el proceso del NTP no recibió ningún paquete. • 1 octal = 00000001, que indica que el proceso del NTP recibió solo el último paquete. • 357 octal = 11101111, que indica el paquete antes de que se perdieran los últimos cuatro paquetes. Reach es un buen indicador de si los paquetes NTP se descartan debido a un link deficiente, problemas de CPU y otros problemas intermitentes. Convertidor de unidades es un conversor de unidades en línea para esta y muchas otras conversiones.
demora	La demora de ida y vuelta al par se informa en milisegundos. Para configurar el reloj con mayor precisión, esta demora se tiene en cuenta cuando se configura la hora del reloj.
offset (desplazamiento)	El desplazamiento es la diferencia de tiempo de reloj entre los pares o entre el principal y el cliente. Este valor es la corrección que se aplica al reloj de un cliente para sincronizarlo. Un valor positivo indica que el reloj del servidor es más

	alto. Un valor negativo indica que el reloj del cliente es más alto.

disp (dispersión)	La dispersión, informada en segundos, es la diferencia máxima de tiempo de reloj que se haya observado entre el reloj local y el reloj del servidor. En el ejemplo, la dispersión es 0,3 para el servidor 10.50.36.42, por lo que la diferencia horaria máxima observada localmente entre el reloj local y el reloj del servidor es de 0,3 segundos.
	
	Puede esperar ver un valor alto cuando los relojes están sincronizados inicialmente. Pero, si la dispersión es demasiado alta en otros momentos, el proceso del NTP en el cliente no acepta mensajes del NTP del servidor. La dispersión máxima es 16000; en el ejemplo, es decir, la dispersión para los servidores 10.50.44.69 y 10.50.44.133, por lo que el cliente local no acepta tiempo de estos servidores.
	
	Si el alcance es cero y la dispersión es muy alta, es probable que el cliente no acepte mensajes de ese servidor. Consulte la segunda línea del ejemplo:
	
	`address ref clock st when poll reach delay offset disp`
	`~10.50.44.69 10.50.36.106 5 21231 1024 0 3.8 -4.26 16000.`
	
	Aunque el desplazamiento es de -4,26, la dispersión es muy alta (quizás debido a un evento pasado) y el alcance es cero, por lo que este cliente no acepta la hora de este servidor.

show ntp association detail

Este es un ejemplo del resultado del comando show ntp association detail:

```
Router#sho ntp assoc detail
10.4.2.254 configured, our_primary, sane, valid, stratum 1
ref ID .GPS., time D36968AA.CC528FE7 (02:10:50.798 UTC Fri May 25 2012)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.44, reach 377, sync dist 207.565
delay 2.99 msec, offset 268.3044 msec, dispersion 205.54
precision 2**19, version 3
org time D36968B7.E74172BF (02:11:03.903 UTC Fri May 25 2012)
rcv time D36968B7.A2F44E2C (02:11:03.636 UTC Fri May 25 2012)
xmt time D36968B7.A21D3780 (02:11:03.633 UTC Fri May 25 2012)
filtdelay =     2.99    2.88  976.61  574.65  984.71  220.26  168.12    2.72
filtoffset =  268.30  172.15 -452.49 -253.59 -462.03  -81.98  -58.04   22.38
filterror =     0.02    0.99    1.95    1.97    2.00    2.01    2.03    2.04

10.3.2.254 configured, selected, sane, valid, stratum 1
ref ID .GPS., time D36968BB.B16C4A21 (02:11:07.693 UTC Fri May 25 2012)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 3.34, reach 377, sync dist 192.169
delay 0.84 msec, offset 280.3251 msec, dispersion 188.42
```

```
precision 2**19, version 3
org time D36968BD.E69085E4 (02:11:09.900 UTC Fri May 25 2012)
rcv time D36968BD.9EE9048B (02:11:09.620 UTC Fri May 25 2012)
xmt time D36968BD.9EA943EF (02:11:09.619 UTC Fri May 25 2012)
filtdelay =     0.84    0.75  663.68    0.67    0.72  968.05  714.07    1.14
filtoffset =  280.33  178.13 -286.52   42.88   41.41 -444.37 -320.25   35.15
filterror =     0.02    0.99    1.97    1.98    1.98    2.00    2.03    2.03

10.1.2.254 configured, insane, invalid, stratum 1
ref ID .GPS., time D3696D3D.BBB4FF24 (02:30:21.733 UTC Fri May 25 2012)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 4.15, reach 1, sync dist 15879.654
delay 0.98 msec, offset 11.9876 msec, dispersion 15875.02
precision 2**19, version 3
org time D3696D3D.E4C253FE (02:30:21.893 UTC Fri May 25 2012)
rcv time D3696D3D.E1D0C1B9 (02:30:21.882 UTC Fri May 25 2012)
xmt time D3696D3D.E18A748D (02:30:21.881 UTC Fri May 25 2012)
filtdelay =     0.98    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =   11.99    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.02 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
```

Los términos ya definidos en la sección de asociación de presentación no se repiten aquí.

Término	Explicación
configured (configurado)	Este origen de reloj del NTP se configuró para ser un servidor. Este valor también puede ser dinámico, donde el par/servidor se detectó dinámicamente.
our_primary	El cliente local está sincronizado con este par.
selected (seleccionado)	El par/servidor se selecciona para una posible sincronización, cuando 'our_primary' falla o el cliente pierde la sincronización.
sane (sanidad)	Las pruebas de sanidad se utilizan para probar el paquete NTP recibido de un servidor. Estas pruebas se especifican en RFC 1305: especificación, implementación y análisis del protocolo de tiempo de red (versión 3). Las pruebas son las siguientes:

Prueba	Máscara	Explicación
1	0x01	Se recibió un paquete duplicado
2	0x02	Falso paquete recibido
3	0x04	Protocolo no sincronizado
4	0x08	Verificación de límites de dispersión/demora entre pares
5	0x10	Error de autenticación de pares
6	0x20	Reloj de pares no sincronizado (común para el servidor no sincronizado)
7	0x40	El estrato entre pares está fuera del límite
8	0x80	Verificación de límites de dispersión/demora de raíz

Los datos del paquete son válidos si se pasan las pruebas 1 a 4. Los datos se utilizan para calcular el desplazamiento, la demora y la dispersión.

El encabezado del paquete es válido si se pasan las pruebas 5 a 8. Solo los paquetes con un encabezado válido se pueden utilizar para determinar si se puede seleccionar un par para la sincronización.

insane (desequilibrio)	Las verificaciones de estado han fallado, por lo que no se acepta el tiempo del servidor. El servidor no está sincronizado.
valid (válido)	La hora del par/servidor es válida. El cliente local acepta esta hora si este par se convierte en el principal.
invalid (no válido)	La hora del par/servidor no es válida y no se puede aceptar.
ref ID (ID de referencia)	A cada par/servidor se le asigna una ID de referencia (etiqueta).
hora	La hora es la última marca de hora recibida de ese par/servidor.
our mode/peer mode (nuestro modo/modo entre pares)	Este es el estado del cliente/par local.
our poll intvl/peer poll intvl (nuestro intervalo de sondeo/intervalo de sondeo entre pares)	Este es el intervalo de sondeo de nuestro sondeo a este par o del par a la máquina local.
root delay (demora de la raíz)	La demora de la raíz es la demora en milisegundos a la raíz de la configuración del NTP. Los relojes del estrato 1 se consideran la raíz de una configuración/diseño del NTP. En el ejemplo, los tres servidores pueden ser la raíz porque están en el estrato 1.
root dispersion (dispersión raíz)	La dispersión raíz es la diferencia máxima de tiempo de reloj que se observó entre el reloj local y el reloj raíz. Consulte la explicación de 'disp' en show up association para obtener más detalles.
sync dist. (dispersión de la sincronización)	Se trata de una estimación de la diferencia máxima entre el tiempo de la fuente del estrato 0 y el tiempo medido por el cliente; consta de componentes para el tiempo de ida y vuelta, la precisión del sistema y la desviación del reloj desde la última lectura real de la fuente del estrato.

	En una configuración NTP grande (servidores NTP en el estrato 1 en Internet, con servidores que originan el tiempo en diferentes estratos) con servidores/clientes en estratos múltiples, la topología de sincronización NTP se debe organizar para producir la precisión más alta, pero nunca se debe permitir que forme un loop de sincronización de tiempo. Un factor adicional es que cada incremento en el estrato implica un servidor de tiempo potencialmente poco confiable que introduce errores de medición adicionales. El algoritmo de selección utilizado en el NTP utiliza una variante del algoritmo de routing distribuido de Bellman-Ford para calcular los árboles de expansión de peso mínimo enraizados en los servidores principales. La métrica de distancia utilizada por el algoritmo consta del estrato más la distancia de sincronización, que a su vez consiste en la dispersión más la mitad del retraso absoluto. Por lo tanto, la trayectoria de sincronización siempre lleva el número mínimo de servidores a la raíz; los lazos se resuelven sobre la base del error máximo.
demora	Esta es la demora de ida y vuelta entre pares.
precision (precisión)	Esta es la precisión del reloj par en Hz.
versión	Este es el número de versión del NTP que utiliza el par.
org time (tiempo del originador)	Ésta es la marca de tiempo del creador del paquete NTP; en otras palabras, es la marca de tiempo del par cuando creó el paquete NTP pero antes de enviar el paquete al cliente local.

rcv time (tiempo de recepción)	Esta es la marca de tiempo cuando el cliente local recibió el mensaje. La diferencia entre el tiempo de organización y el tiempo de recepción es el desplazamiento para este par. En el ejemplo, el 10.4.2.254 primario tiene estos tiempos:
	
	`org time D36968B7.E74172BF (02:11:03.903 UTC Fri May 25 2012)`
	`rcv time D36968B7.A2F44E2C (02:11:03.636 UTC Fri May 25 2012)`
	
	La diferencia es el desplazamiento de 268.3044 ms.

xmt time (tiempo de transmisión)	Esta es la marca de tiempo de transmisión para el paquete NTP que el cliente local envía a este par/servidor.
filtdelay (demora de filtro) filtoffset (desplazamiento de filtro) filterror (error de filtro)	Esta es la demora de ida y vuelta en milisegundos de cada muestra. Este es el desplazamiento del reloj en milisegundos de cada muestra. Este es el error aproximado de cada muestra. Una muestra es el último paquete NTP recibido. En el ejemplo, el principal 10.4.2.254 tiene estos valores:

	filtdelay = 2.99 2.88 976.61 574.65 984.71 220.26 168.12 2.72 filtoffset = 268.30 172.15 -452.49 -253.59 -462.03 -81.98 -58.04 22.38 filterror = 0.02 0.99 1.95 1.97 2.00 2.01 2.03 2.04 Estos ocho ejemplos corresponden al valor del campo de alcance, que muestra si el cliente local recibió los últimos ocho paquetes NTP.

show ntp status

Este es un ejemplo del resultado del comando show ntp status:

```
USSP-B33S-SW01#sho ntp status
Clock is synchronized, stratum 2, reference is 10.4.2.254
nominal freq is 250.0000 Hz, actual freq is 250.5630 Hz, precision is 2**18
reference time is D36968F7.7E3019A9 (02:12:07.492 UTC Fri May 25 2012)
clock offset is 417.2868 msec, root delay is 2.85 msec
root dispersion is 673.42 msec, peer dispersion is 261.80 msec
```

Los términos ya definidos en la sección show up association o en la sección show ntp association detail no se repiten.

Término	Explicación
precision (precisión)	La precisión se determina automáticamente y se mide como una potencia de dos. En el ejemplo, 2 ** 18 significa 2^ (-18) o 3,8 microsegundos.

	La pérdida de sincronización entre pares NTP o entre un cliente y un cliente primario puede deberse a una variedad de causas. NTP evita la sincronización con una máquina cuyo tiempo puede ser ambiguo de las siguientes maneras: 1. El NTP nunca se sincroniza con una máquina que no está sincronizada. 1. El NTP compara la hora que informan varias máquinas y no se sincroniza con una máquina cuya hora es significativamente diferente del resto, incluso si su estrato es menor.

Solucionar problemas de NTP con depuraciones

Algunas de las causas más comunes de problemas del NTP son:

- Los paquetes NTP no se reciben.
- Los paquetes NTP se reciben, pero no son procesados por el proceso NTP en el Cisco IOS.
- Los paquetes NTP se procesan, pero los factores o datos de paquetes erróneos provocan la pérdida de sincronización.
- El período de reloj del NTP se establece manualmente.

Entre los comandos de depuración importantes que ayudan a aislar la causa de estos problemas se incluyen los siguientes:

- debug ip packets <acl>
- debug ntp packets
- debug ntp validity
- debug ntp sync
- debug ntp events

Las siguientes secciones ilustran el uso de depuraciones para resolver estos problemas comunes.

Nota: Utilice la Command Lookup Tool para obtener más información sobre los comandos utilizados en esta sección. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Paquetes NTP no recibidos

Utilice el comando debug ip packet para verificar si los paquetes NTP se reciben y se envían. Dado que el resultado de la depuración puede ser locuaz, puede limitar el resultado de la depuración con el uso de listas de control de acceso (ACL). El NTP utiliza el puerto 123 del protocolo de datagrama del usuario (UDP).

1. Cree la ACL 101:

```
access-list 101 permit udp any any eq 123
access-list 101 permit udp any eq 123 any
```

Los paquetes NTP generalmente tienen un puerto 123 de origen y destino, lo que permite:

```
permit udp any eq 123 any eq 123
```

2. Utilice esta ACL para limitar el resultado del comando debug ip packet:

```
debug ip packet 101
```

3. Si el problema es con pares en particular, reduzca la ACL 101 a esos pares. Si el par es 172.16.1.1, cambie la ACL 101 a:

```
access-list 101 permit udp host 172.16.1.1 any eq 123
access-list 101 permit udp any eq 123 host 172.16.1.1
```

Este ejemplo de salida indica que los paquetes no se envían:

```
241925: Apr 23 2012 15:46:26.101 ETE: IP: s=10.50.38.70 (Tunnel99), d=10.50.44.101, len 76, input featu
241926: Apr 23 2012 15:46:26.101 ETE:     UDP src=123, dst=123, Ingress-NetFlow(13), rtype 0, forus FAL
sendself FALSE, mtu 0
241927: Apr 23 2012 15:46:26.101 ETE: IP: s=10.50.38.70 (Tunnel99), d=10.50.44.101, len 76, input featu
241928: Apr 23 2012 15:46:26.101 ETE:     UDP src=123, dst=123, MCI Check(55), rtype 0, forus FALSE,
sendself FALSE, mtu 0
```

Una vez que confirme que los paquetes NTP no se reciben, debe:

- Compruebe si el NTP está configurado correctamente.
- Verifique si una ACL bloquea los paquetes NTP.
- Revise si hay problemas de routing con la IP de origen o destino.

Paquetes NTP no procesados

Con los comandos debug ip packet y debug ntp packets habilitados, puede ver los paquetes recibidos y transmitidos, y puede ver que NTP actúa sobre esos paquetes. Para cada paquete NTP recibido (como lo muestra debug ip packet), existe una entrada correspondiente generada por debug ntp packets .

Este es el resultado de la depuración cuando el proceso del NTP funciona en los paquetes recibidos:

```
Apr 20 00:16:34.143 UTC: IP: tableid=0, s=10.3.2.31 (local), d=10.1.2.254 (Vlan2), routed via FIB
.Apr 20 00:16:34.143 UTC: IP: s=10.3.2.31 (local), d=10.1.2.254 (Vlan2), len 76, sending
.Apr 20 00:16:34.143 UTC: IP: s=10.3.2.31 (local), d=10.1.2.254 (Vlan2), len 76, sending full packet
.Apr 20 00:16:34.143 UTC: NTP: xmit packet to 10.1.2.254:
.Apr 20 00:16:34.143 UTC:  leap 3, mode 3, version 3, stratum 0, ppoll 64
.Apr 20 00:16:34.143 UTC:  rtdel 0021 (0.504), rtdsp 1105E7 (17023.056), refid 0A0102FE (10.1.2.254)
.Apr 20 00:16:34.143 UTC:  ref D33B2922.24FEBDC7 (00:15:30.144 UTC Fri Apr 20 2012)
.Apr 20 00:16:34.143 UTC:  org 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
.Apr 20 00:16:34.143 UTC:  rec 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
.Apr 20 00:16:34.143 UTC:  xmt D33B2962.24CAFAD1 (00:16:34.143 UTC Fri Apr 20 2012)
.Apr 20 00:16:34.143 UTC: IP: s=10.1.2.254 (Vlan2), d=10.3.2.31, len 76, rcvd 2
.Apr 20 00:16:34.143 UTC: NTP: rcv packet from 10.1.2.254 to 10.3.2.31 on Vlan2:
.Apr 20 00:16:34.143 UTC:  leap 0, mode 4, version 3, stratum 1, ppoll 64
.Apr 20 00:16:34.143 UTC:  rtdel 0000 (0.000), rtdsp 009D (2.396), refid 47505300 (10.80.83.0)
.Apr 20 00:16:34.143 UTC:  ref D33B2952.4CC11CCF (00:16:18.299 UTC Fri Apr 20 2012)
.Apr 20 00:16:34.143 UTC:  org D33B2962.24CAFAD1 (00:16:34.143 UTC Fri Apr 20 2012)
.Apr 20 00:16:34.143 UTC:  rec D33B2962.49D3724D (00:16:34.288 UTC Fri Apr 20 2012)
.Apr 20 00:16:34.143 UTC:  xmt D33B2962.49D997D0 (00:16:34.288 UTC Fri Apr 20 2012)
.Apr 20 00:16:34.143 UTC:  inp D33B2962.25010310 (00:16:34.144 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC: IP: tableid=0, s=10.3.2.31 (local), d=10.8.2.254 (Vlan2), routed via FIB
.Apr 20 00:16:36.283 UTC: IP: s=10.3.2.31 (local), d=10.8.2.254 (Vlan2), len 76, sending
.Apr 20 00:16:36.283 UTC: IP: s=10.3.2.31 (local), d=10.8.2.254 (Vlan2), len 76, sending full packet
.Apr 20 00:16:36.283 UTC: NTP: xmit packet to 10.8.2.254:
.Apr 20 00:16:36.283 UTC:  leap 3, mode 3, version 3, stratum 0, ppoll 64
.Apr 20 00:16:36.283 UTC:  rtdel 002F (0.717), rtdsp 11058F (17021.713), refid 0A0102FE (10.1.2.254)
.Apr 20 00:16:36.283 UTC:  ref D33B2962.25010310 (00:16:34.144 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC:  org 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
.Apr 20 00:16:36.283 UTC:  rec 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
.Apr 20 00:16:36.283 UTC:  xmt D33B2964.48947E87 (00:16:36.283 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC: IP: s=10.8.2.254 (Vlan2), d=10.3.2.31, len 76, rcvd 2
.Apr 20 00:16:36.283 UTC: NTP: rcv packet from 10.8.2.254 to 10.3.2.31 on Vlan2:
.Apr 20 00:16:36.283 UTC:  leap 0, mode 4, version 3, stratum 1, ppoll 64
.Apr 20 00:16:36.283 UTC:  rtdel 0000 (0.000), rtdsp 0017 (0.351), refid 47505300 (10.80.83.0)
.Apr 20 00:16:36.283 UTC:  ref D33B295B.8AF7FE33 (00:16:27.542 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC:  org D33B2964.48947E87 (00:16:36.283 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC:  rec D33B2964.4A6AD269 (00:16:36.290 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC:  xmt D33B2964.4A7C00D0 (00:16:36.290 UTC Fri Apr 20 2012)
.Apr 20 00:16:36.283 UTC:  inp D33B2964.498A755D (00:16:36.287 UTC Fri Apr 20 2012)
```

Este es un ejemplo en el que el NTP no funciona en paquetes recibidos. Aunque los paquetes NTP se reciben (como se muestra en debug ip packets), el proceso del NTP no actúa sobre ellos. Para los paquetes NTP que se envían, está presente el resultado correspondiente debug ntp packets porque el proceso del NTP tiene que generar el paquete. El problema es específico de los paquetes NTP recibidos que no se procesan.

```
071564: Apr 23 2012 15:46:26.100 ETE: NTP: xmit packet to 10.50.44.101:
071565: Apr 23 2012 15:46:26.100 ETE:  leap 0, mode 1, version 3, stratum 5, ppoll 1024
071566: Apr 23 2012 15:46:26.100 ETE:  rtdel 07B5 (30.106), rtdsp 0855 (32.547), refid 0A32266A
(10.50.38.106)
071567: Apr 23 2012 15:46:26.100 ETE:  ref D33FDB05.1A084831 (15:43:33.101 ETE Mon Apr 23 2012)
071568: Apr 23 2012 15:46:26.100 ETE:  org 00000000.00000000 (01:00:00.000 HIVER Mon Jan 1 1900)
071569: Apr 23 2012 15:46:26.100 ETE:  rec 00000000.00000000 (01:00:00.000 HIVER Mon Jan 1 1900)
071570: Apr 23 2012 15:46:26.100 ETE:  xmt D33FDBB2.19D3457C (15:46:26.100 ETE Mon Apr 23 2012)
PCY_PAS1#
071571: Apr 23 2012 15:47:31.497 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, input featur
071572: Apr 23 2012 15:47:31.497 ETE:     UDP src=123, dst=123, Ingress-NetFlow(13), rtype 0, forus FALS
sendself FALSE, mtu 0
071573: Apr 23 2012 15:47:31.497 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, input featur
071574: Apr 23 2012 15:47:31.497 ETE:     UDP src=123, dst=123, MCI Check(55), rtype 0, forus FALSE,
sendself FALSE, mtu 0
071575: Apr 23 2012 15:47:31.497 ETE: FIBipv4-packet-proc: route packet from Tunnel99 src 10.50.38.78 d
10.50.44.69
071576: Apr 23 2012 15:47:31.497 ETE: FIBfwd-proc: base:10.50.44.69/32 receive entry
PCY_PAS1#
071577: Apr 23 2012 15:47:31.497 ETE: FIBipv4-packet-proc: packet routing failed
071578: Apr 23 2012 15:47:31.497 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, rcvd 2
071579: Apr 23 2012 15:47:31.497 ETE:     UDP src=123, dst=123
071580: Apr 23 2012 15:47:31.497 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, stop process
for forus packet
071581: Apr 23 2012 15:47:31.497 ETE:     UDP src=123, dst=123
PCY_PAS1#
071582: Apr 23 2012 16:03:30.105 ETE: NTP: xmit packet to 10.50.44.101:
071583: Apr 23 2012 16:03:30.105 ETE:  leap 0, mode 1, version 3, stratum 5, ppoll 1024
071584: Apr 23 2012 16:03:30.105 ETE:  rtdel 0759 (28.702), rtdsp 087D (33.157), refid 0A32266A
(10.50.38.106)
071585: Apr 23 2012 16:03:30.105 ETE:  ref D33FDF05.1B2CC3D4 (16:00:37.106 ETE Mon Apr 23 2012)
071586: Apr 23 2012 16:03:30.105 ETE:  org 00000000.00000000 (01:00:00.000 HIVER Mon Jan 1 1900)
071587: Apr 23 2012 16:03:30.105 ETE:  rec 00000000.00000000 (01:00:00.000 HIVER Mon Jan 1 1900)
071588: Apr 23 2012 16:03:30.105 ETE:  xmt D33FDFB2.1B1D5E7E (16:03:30.105 ETE Mon Apr 23 2012)
PCY_PAS1#
071589: Apr 23 2012 16:04:35.502 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, input featur
071590: Apr 23 2012 16:04:35.506 ETE:     UDP src=123, dst=123, Ingress-NetFlow(13), rtype 0, forus FALS
sendself FALSE, mtu 0
071591: Apr 23 2012 16:04:35.506 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, input featur
071592: Apr 23 2012 16:04:35.506 ETE:     UDP src=123, dst=123, MCI Check(55), rtype 0, forus FALSE,
sendself FALSE, mtu 0
071593: Apr 23 2012 16:04:35.506 ETE: FIBipv4-packet-proc: route packet from Tunnel99 src 10.50.38.78 d
10.50.44.69
071594: Apr 23 2012 16:04:35.506 ETE: FIBfwd-proc: base:10.50.44.69/32 receive entry
PCY_PAS1#
071595: Apr 23 2012 16:04:35.506 ETE: FIBipv4-packet-proc: packet routing failed
071596: Apr 23 2012 16:04:35.506 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, rcvd 2
071597: Apr 23 2012 16:04:35.506 ETE:     UDP src=123, dst=123
071598: Apr 23 2012 16:04:35.506 ETE: IP: s=10.50.38.78 (Tunnel99), d=10.50.44.69, len 76, stop process
for forus packet
071599: Apr 23 2012 16:04:35.506 ETE:     UDP src=123, dst=123
PCY_PAS1#
```

Pérdida de sincronización

Puede producirse una pérdida de sincronización si el valor de dispersión o retraso de un servidor es muy alto. Los valores altos indican que los paquetes tardan demasiado en llegar al cliente desde el servidor/peer en referencia a la raíz del reloj. Por lo tanto, la máquina local no puede confiar en la precisión del tiempo presente en el paquete porque no sabe cuánto tiempo tardó el paquete en llegar.

NTP es meticuloso en cuanto al tiempo y no puede sincronizarse con otro dispositivo en el que no puede confiar o no puede ajustarse de manera que pueda ser confiable.

Si hay un enlace saturado y se produce el almacenamiento en búfer en el camino, los paquetes se retrasan a medida que llegan al cliente NTP. Por lo tanto, la marca de hora contenida en un paquete NTP posterior a veces puede variar mucho y el cliente local no puede ajustarse realmente a esa variación.

El NTP no ofrece un método para desactivar la validación de estos paquetes a menos que utilice el protocolo simple de tiempo de red (SNTP). SNTP no es una gran alternativa porque no es ampliamente soportado en el software.

Si experimenta una pérdida de sincronización, debe comprobar los enlaces:

- ¿Están saturados?
- ¿Hay algún tipo de descarte en los enlaces de red de área extensa (WAN)?
- ¿Se produce el cifrado?

Monitoree el valor de alcance desde el comando show ntp associations detail. El valor más alto es 377. Si el valor es 0 o bajo, los paquetes NTP se reciben intermitentemente y el cliente local deja de estar sincronizado con el servidor.

debug ntp validity

El comando debug ntp validity indica si el paquete NTP falló en las comprobaciones de validez o sanidad y revela el motivo de la falla. Compare este resultado con las pruebas de estado especificadas en RFC 1305 que se utilizan para probar el paquete NTP recibido de un servidor. Se definen ocho pruebas:

Prueba Máscara	Explicación

1	0x01	Se recibió un paquete duplicado
2	0x02	Falso paquete recibido
3	0x04	Protocolo no sincronizado
4	0x08	Verificación de límites de dispersión/demora entre pares
5	0x10	Error de autenticación de pares
6	0x20	Reloj de pares no sincronizado (común para el servidor no sincronizado)
7	0x40	El estrato entre pares está fuera del límite
8	0x80	Verificación de límites de dispersión/demora de raíz

Este es el resultado de ejemplo del comando debug ntp validity:

```
PCY_PAS1#debug ntp validity
NTP peer validity debugging is on

009585: Mar  1 2012 09:14:32.670 HIVER: NTP: packet from 192.168.113.57 failed validity tests 52
009586: Mar  1 2012 09:14:32.670 HIVER: Authentication failed
009587: Mar  1 2012 09:14:32.670 HIVER: Peer/Server Stratum out of bound
PCY_PAS1#
009588: Mar  1 2012 09:14:38.210 HIVER: NTP: packet from 192.168.56.1 failed validity tests 14
009589: Mar  1 2012 09:14:38.210 HIVER: Authentication failed
PCY_PAS1#
009590: Mar  1 2012 09:14:43.606 HIVER: NTP: packet from 10.110.103.27 failed validity tests 14
009591: Mar  1 2012 09:14:43.606 HIVER: Authentication failed
PCY_PAS1#
009592: Mar  1 2012 09:14:48.686 HIVER: NTP: packet from 192.168.113.57failed validity tests 52
009593: Mar  1 2012 09:14:48.686 HIVER: Authentication failed
009594: Mar  1 2012 09:14:48.686 HIVER: Peer/Server Stratum out of bound
PCY_PAS1#
009596: Mar  1 2012 09:14:54.222 HIVER: NTP: packet from 10.110.103.35 failed validity tests 14
```

```
009597: Mar  1 2012 09:14:54.222 HIVER: Authentication failed
PCY_PAS1#
009598: Mar  1 2012 09:14:54.886 HIVER: NTP: synced to new peer 10.50.38.106
009599: Mar  1 2012 09:14:54.886 HIVER: NTP: 10.50.38.106 synced to new peer
PCY_PAS1#
009600: Mar  1 2012 09:14:59.606 HIVER: NTP: packet from 10.110.103.27 failed validity tests 14
009601: Mar  1 2012 09:14:59.606 HIVER: Authentication failed
PCY_PAS1#
009602: Mar  1 2012 09:15:04.622 HIVER: NTP: packet from 192.168.113.137 failed validity tests 52
009603: Mar  1 2012 09:15:04.622 HIVER: Authentication failed
009604: Mar  1 2012 09:15:04.622 HIVER: Peer/Server Stratum out of bound
PCY_PAS1#
009605: Mar  1 2012 09:15:10.238 HIVER: NTP: packet from 192.168.56.1 failed validity tests 14
009606: Mar  1 2012 09:15:10.238 HIVER: Authentication failed
PCY_PAS1#
009607: Mar  1 2012 09:15:15.338 HIVER: NTP: packet from 10.83.23.140 failed validity tests 52
009608: Mar  1 2012 09:15:15.338 HIVER: Authentication failed
009609: Mar  1 2012 09:15:15.338 HIVER: Peer/Server Stratum out of bound
PCY_PAS1#
009610: Mar  1 2012 09:15:20.402 HIVER: NTP: packet from 192.168.113.92 failed validity tests 74
009611: Mar  1 2012 09:15:20.402 HIVER: Authentication failed
009612: Mar  1 2012 09:15:20.402 HIVER: Peer/Server Clock unsynchronized
009613: Mar  1 2012 09:15:20.402 HIVER: Peer/Server Stratum out of bound
```

debug ntp packets

Puede utilizar el comando debug ntp packets para ver el tiempo que proporciona el par/servidor en el paquete recibido. La máquina de hora local también informa la hora conocida del par/servidor en el paquete transmitido.

Campo	Paquete recibido	Paquete transmitido
org (originador)	Marca de hora del originador, que es la hora del servidor.	Marca de hora del originador (cliente) cuando envió el paquete. (El cliente origina un paquete en el servidor).
rec (receptor)	Marca de hora en el cliente cuando recibió el paquete.	Hora actual del cliente.

En este resultado de ejemplo, las marcas de hora en el paquete recibido del servidor y el paquete enviado a otro servidor son iguales, lo que indica que el NTP del cliente está sincronizado.

```
USSP-B33S-SW01#debug ntp packets
NTP packets debugging is on
USSP-B33S-SW01#
May 25 02:21:48.182 UTC: NTP: rcv packet from 10.1.2.254 to 10.3.2.31 on Vlan2:
May 25 02:21:48.182 UTC:  leap 0, mode 4, version 3, stratum 1, ppoll 64
May 25 02:21:48.182 UTC:  rtdel 0000 (0.000), rtdsp 00F2 (3.693), refid 47505300 (10.80.83.0)
May 25 02:21:48.182 UTC:  ref D3696B38.B722C417 (02:21:44.715 UTC Fri May 25 2012)
May 25 02:21:48.182 UTC:  org D3696B3C.2EA179BA (02:21:48.182 UTC Fri May 25 2012)
May 25 02:21:48.182 UTC:  rec D3696B3D.E58DE1BE (02:21:49.896 UTC Fri May 25 2012)
May 25 02:21:48.182 UTC:  xmt D3696B3D.E594E7AF (02:21:49.896 UTC Fri May 25 2012)
May 25 02:21:48.182 UTC:  inp D3696B3C.2EDFC333 (02:21:48.183 UTC Fri May 25 2012)
May 25 02:22:46.051 UTC: NTP: xmit packet to 10.4.2.254:
May 25 02:22:46.051 UTC:  leap 0, mode 3, version 3, stratum 2, ppoll 64
May 25 02:22:46.051 UTC:  rtdel 00C0 (2.930), rtdsp 1C6FA (1777.252), refid 0A0402FE (10.4.2.254)
May 25 02:22:46.051 UTC:  ref D3696B36.33D43F44 (02:21:42.202 UTC Fri May 25 2012)
May 25 02:22:46.051 UTC:  org D3696B37.E72C75AE (02:21:43.903 UTC Fri May 25 2012)
May 25 02:22:46.051 UTC:  rec D3696B36.33D43F44 (02:21:42.202 UTC Fri May 25 2012)
May 25 02:22:46.051 UTC:  xmt D3696B76.0D43AE7D (02:22:46.051 UTC Fri May 25 2012)
```

Este es un ejemplo de resultado cuando los relojes no están sincronizados. Observe la diferencia horaria entre el paquete transmitido y el paquete recibido. La dispersión del par puede estar en el valor máximo de 16000 y el alcance del par puede mostrar 0.

```
USSP-B33S-SW01#
.May 25 02:05:59.011 UTC: NTP: xmit packet to 10.4.2.254:
.May 25 02:05:59.011 UTC:  leap 3, mode 3, version 3, stratum 0, ppoll 64
.May 25 02:05:59.011 UTC:  rtdel 00A3 (2.487), rtdsp 1104D0 (17018.799), refid 0A0402FE (10.4.2.254)
.May 25 02:05:59.011 UTC:  ref D3696747.03D8661A (02:04:55.015 UTC Fri May 25 2012)
.May 25 02:05:59.011 UTC:  org 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
.May 25 02:05:59.011 UTC:  rec 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
.May 25 02:05:59.011 UTC:  xmt D3696787.03105783 (02:05:59.011 UTC Fri May 25 2012)
.May 25 02:05:59.011 UTC: NTP: rcv packet from 10.4.2.254 to 10.3.2.31 on Vlan2:
.May 25 02:05:59.011 UTC:  leap 0, mode 4, version 3, stratum 1, ppoll 64
.May 25 02:05:59.011 UTC:  rtdel 0000 (0.000), rtdsp 0014 (0.305), refid 47505300 (10.80.83.0)
.May 25 02:05:59.011 UTC:  ref D3696782.C96FD778 (02:05:54.786 UTC Fri May 25 2012)
.May 25 02:05:59.011 UTC:  org D3696787.03105783 (02:05:59.011 UTC Fri May 25 2012)
.May 25 02:05:59.011 UTC:  rec D3696787.281A963F (02:05:59.156 UTC Fri May 25 2012)
.May 25 02:05:59.011 UTC:  xmt D3696787.282832C4 (02:05:59.156 UTC Fri May 25 2012)
.May 25 02:05:59.011 UTC:  inp D3696787.03C63542 (02:05:59.014 UTC Fri May 25 2012)
```

debug ntp sync and debug ntp events

El comando debug ntp sync produce resultados de una línea que muestran si el reloj se ha sincronizado o si la sincronización ha cambiado. El comando generalmente está habilitado con debug ntp events.

El comando debug ntp events muestra los eventos NTP que se producen, lo que le ayuda a determinar si un cambio en el NTP provocó un problema como relojes que no están sincronizados. (En otras palabras, si sus relojes sincronizados de repente se vuelven locos, debe buscar un cambio o un activador).

Este es un ejemplo de ambas depuraciones. Inicialmente, se sincronizaron los relojes del cliente. El comando debug ntp events muestra que se produjo un cambio en el estrato de pares NTP y que los relojes quedaron fuera de sincronización.

```
USSP-B33S-SW01#debug ntp sync
NTP clock synchronization debugging is on
USSP-B33S-SW01#
USSP-B33S-SW01#
USSP-B33S-SW01#debug ntp events
NTP events debugging is on
USSP-B33S-SW01#
USSP-B33S-SW01#
May 25 02:25:57.620 UTC: NTP: xmit packet to 10.4.2.254:
May 25 02:25:57.620 UTC:  leap 0, mode 3, version 3, stratum 2, ppoll 64
May 25 02:25:57.620 UTC:  rtdel 00D4 (3.235), rtdsp 26B26 (2418.549), refid 0A0402FE (10.4.2.254)
May 25 02:25:57.620 UTC:  ref D3696BF5.C47EB880 (02:24:53.767 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  org D3696BF7.E5F91077 (02:24:55.898 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  rec D3696BF5.C47EB880 (02:24:53.767 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  xmt D3696C35.9ED1CE97 (02:25:57.620 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC: NTP: rcv packet from 10.4.2.254 to 10.3.2.31 on Vlan2:
May 25 02:25:57.620 UTC:  leap 0, mode 4, version 3, stratum 1, ppoll 64
May 25 02:25:57.620 UTC:  rtdel 0000 (0.000), rtdsp 000E (0.214), refid 47505300 (10.80.83.0)
May 25 02:25:57.620 UTC:  ref D3696C37.D528800E (02:25:59.832 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  org D3696C35.9ED1CE97 (02:25:57.620 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  rec D3696C37.E5C7AB3D (02:25:59.897 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  xmt D3696C37.E5D1F273 (02:25:59.897 UTC Fri May 25 2012)
May 25 02:25:57.620 UTC:  inp D3696C35.9F9EA2C4 (02:25:57.623 UTC Fri May 25 2012)
May 25 02:25:59.830 UTC: NTP: peer stratum change
May 25 02:25:59.830 UTC: NTP: clock reset
May 25 02:25:59.830 UTC: NTP: sync change
May 25 02:25:59.830 UTC: NTP: peer stratum change
May 25 02:26:05.817 UTC: NTP: xmit packet to 10.1.2.254:
May 25 02:26:05.817 UTC:  leap 3, mode 3, version 3, stratum 0, ppoll 64
May 25 02:26:05.817 UTC:  rtdel 00C2 (2.960), rtdsp 38E9C (3557.068), refid 0A0402FE (10.4.2.254)
May 25 02:26:05.817 UTC:  ref D3696C35.9F9EA2C4 (02:25:57.623 UTC Fri May 25 2012)
May 25 02:26:05.817 UTC:  org 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
May 25 02:26:05.817 UTC:  rec 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
May 25 02:26:05.817 UTC:  xmt D3696C3D.D12D0565 (02:26:05.817 UTC Fri May 25 2012)
```

Configuración manual del período de reloj del NTP

El sitio web Cisco.com advierte que:

"El comando ntp clock-period se genera automáticamente para reflejar el factor de corrección que cambia constantemente cuando se ingresa el comando copy running-configuration startup-configuration para guardar la configuración en la NVRAM. No intente utilizar manualmente el comando ntp clock-period. Asegúrese de quitar esta línea de comandos cuando copie archivos de configuración en otros dispositivos."

El valor del período de reloj depende del hardware, por lo que difiere para cada dispositivo.

El comando ntp clock-period aparece automáticamente en la configuración cuando se habilita el NTP. El comando se utiliza para ajustar el reloj del software. El 'valor de ajuste' compensa el intervalo de tics de 4 ms de modo que, con el ajuste menor, tiene 1 segundo al final del intervalo.

Si el dispositivo ha calculado que su reloj del sistema pierde tiempo (tal vez deba haber una compensación de frecuencia desde el nivel base del router), agrega automáticamente este valor al reloj del sistema para mantener su sincronía.

Nota: El usuario no debe cambiar este comando.

El período de reloj del NTP predeterminado para un router es 17 179 869 y se utiliza esencialmente para iniciar el proceso del NTP.

La fórmula de conversión es 17 179 869 * 2^ (- 32) = 0,003999999957159161567687988281 25 o aproximadamente 4 milisegundos.

Por ejemplo, se encontró que el reloj del sistema para los routers Cisco 2611 (uno de los routers Cisco de la serie 2600) estaba ligeramente fuera de sincronización y podía resincronizarse con este comando:

```
ntp clock-period 17208078
```

Esto equivale a 17 208 078 * 2^ (- 32) = 0,004006567876785993576049804687 5 o un poco más de 4 milisegundos.

Cisco recomienda que deje que el router se ejecute durante aproximadamente una semana en condiciones normales de red y que luego utilice el comando wr mempara guardar el valor. Esto le proporciona una cifra precisa para el próximo reinicio y permite que el NTP se sincronice más rápidamente.

Utilice el comando no ntp clock-period cuando guarde la configuración para utilizarla en otro dispositivo, ya que este comando regresa el período de reloj al valor predeterminado de ese dispositivo en particular. Puede volver a calcular el valor verdadero (pero puede reducir la precisión del reloj del sistema durante ese período de tiempo de nuevo cálculo).

Recuerde que este valor depende del hardware, por lo que si copia una configuración y la utiliza en diferentes dispositivos, puede causar problemas. Cisco planea reemplazar el NTP versión 3 por la versión 4 para resolver este problema.

Si no es consciente de estos problemas, puede decidir ajustar manualmente este valor. Para migrar de un dispositivo a otro, puede decidir copiar la configuración anterior y pegarla en el nuevo dispositivo. Desafortunadamente, debido a que el comando ntp clock-period aparece en running-config y startup-config, el período de reloj del NTP se pega en el nuevo dispositivo. Cuando esto sucede, el NTP en el nuevo cliente siempre se desincroniza con el servidor con un alto valor de dispersión de pares.

En cambio, borre el período de reloj del NTP con el comando no ntp clock-period y guarde la configuración. El router finalmente calcula un período de reloj adecuado para sí mismo.

El comando ntp clock-period ya no está disponible en la versión 15.0 o posterior del software del IOS de Cisco; el analizador ahora rechaza el comando con el error:

```
"%NTP: This configuration command is deprecated."
```

No tiene permiso para configurar el período de reloj manualmente, y el período de reloj no está permitido en running-config. Dado que el analizador rechaza el comando si estaba en la configuración de inicio (en versiones anteriores de Cisco IOS, como 12.4), el analizador rechaza el comando cuando copia la configuración de inicio en la configuración en ejecución en el arranque.

El nuevo comando de reemplazo es ntp clear drift.

Información Relacionada

- Subproceso del foro de soporte: período de reloj NTP no configurado
- Protocolo de tiempo de la red: informe técnico sobre prácticas recomendadas
- Solución de problemas del protocolo de tiempo de red (NTP)
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).