Solucionar problemas e depurar problemas do Network Time Protocol (NTP)

Contents

Introdução

Este documento descreve como solucionar problemas do Network Time Protocol (NTP) com debug comandos e o show ntp comando.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Comandos show do NTP

Antes de examinar a causa dos problemas de NTP, você deve entender o uso e a saída desses comandos:

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

Observação: Use a Command Lookup Tool para obter mais informações sobre os comandos usados nesta seção. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas.

Observação: a Output Interpreter Tool oferece suporte a determinados comandos show. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show.. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas.

show ntp association

Uma associação NTP pode ser uma associação de peer (um sistema está disposto a sincronizar com o outro sistema ou a permitir que o outro sistema sincronize com ele) ou uma associação de servidor (apenas um sistema sincroniza com o outro sistema e não o contrário).

Este é um exemplo de saída do 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
```

Termo	Explicação
	Os caracteres antes do endereço têm estas definições: * Sincronizado com este par # Quase sincronizado com este par + Correspondente selecionado para possível sincronização - Peer é um candidato para seleção ~ O peer está configurado estaticamente
endereço	Este é o endereço IP do peer. No exemplo, a primeira entrada mostra 127.127.7.1. Isso indica que a máquina local foi sincronizada com ela mesma. Geralmente, apenas um NTP primário é sincronizado com ele mesmo.
ref clock	Este é o endereço do relógio de referência para o peer. No exemplo, os primeiros seis peers/servidores têm um IP privado como o relógio de referência, de modo que seus primários são provavelmente roteadores, switches ou servidores dentro da rede local. Para as últimas quatro entradas, o relógio de referência é um IP público, portanto suas principais são provavelmente uma fonte de tempo pública.
st	O NTP usa o conceito de um stratum para descrever a distância (em saltos de NTP) que 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. Ele envia seu horário para um servidor de horário de estrato 2 através do NTP e assim por diante até o estrato 16. Uma máquina que executa o NTP escolhe automaticamente a máquina com o menor número de stratum com a qual pode se comunicar e usa o NTP como sua origem de tempo.
quando	O tempo desde que o último pacote NTP foi recebido de um peer é relatado em segundos. Este valor deve ser inferior ao intervalo de sondagem.
pesquisa	O intervalo de sondagem é relatado em segundos. O intervalo normalmente começa com um mínimo de intervalos de pesquisa de 64 segundos. O RFC especifica que não é necessária mais de uma transação de NTP por minuto para sincronizar duas máquinas. À medida que o NTP se torna estável entre um cliente e um servidor, o intervalo de pesquisa pode aumentar em pequenas etapas de 64 segundos até 1024 segundos e geralmente se estabiliza em algum ponto entre eles. No entanto, esse valor

	muda dinamicamente, com base nas condições de rede entre o cliente e o servidor e na perda de pacotes NTP. Se um servidor ficar inacessível por algum tempo, o intervalo de pesquisa será aumentado em etapas para 1024 segundos para reduzir a sobrecarga da rede. Não é possível ajustar o intervalo de poll do NTP em um roteador, porque o interno é determinado por algoritmos heurísticos.
alcance	A alcançabilidade do peer é uma sequência de bits relatada como um valor octal. Este campo mostra se os últimos oito pacotes foram recebidos pelo processo NTP no software Cisco IOS®. Os pacotes devem ser recebidos, processados e aceitos como válidos pelo processo NTP e não apenas pelo roteador ou switch que recebe os pacotes IP NTP. Reach usa o intervalo de poll para um tempo limite para decidir se um pacote foi recebido ou não. O intervalo de poll é o tempo que o NTP espera antes de concluir que um pacote foi perdido. O tempo de poll pode ser diferente para peers diferentes, de modo que o tempo antes do alcance decidir que um pacote foi perdido também pode ser diferente para peers diferentes. No exemplo, há quatro valores diferentes de alcance: • 377 octal = binário 11111111, que indica que o processo NTP recebeu os últimos oito pacotes. • 0 octal = 00000000, que indica que o processo NTP não recebeu nenhum pacote. • 1 octal = 00000001, que indica que o processo NTP recebeu apenas o pacote mais recente. • 357 octal = 11101111, que indica que o pacote antes dos últimos quatro pacotes foi perdido. Reach é um bom indicador de que os pacotes NTP são descartados devido a um link ruim, problemas de CPU e outros problemas intermitentes. Unit Converter é um conversor de unidade on-line para esta e muitas outras conversões.
atraso	O atraso de ida e volta para o peer é relatado em milissegundos. Para ajustar o relógio com mais precisão, esse atraso é levado em conta quando a hora do relógio é definida.
deslocamento	Deslocamento é a diferença de tempo do relógio entre os peers ou entre o primário e o cliente. Esse valor é a correção aplicada a um relógio do cliente para sincronizá-lo. Um valor positivo indica que o relógio do servidor está mais alto. Um valor negativo indica que o relógio do cliente está mais alto.

disp	A dispersão, relatada em segundos, é a diferença máxima de tempo de relógio que foi observada entre o relógio local e o relógio do servidor. No exemplo, a dispersão é 0,3 para o servidor 10.50.36.42, portanto, a diferença máxima de tempo observada localmente entre o relógio local e o relógio do servidor é de 0,3 segundos.
	
	Você pode esperar ver um valor alto quando os relógios estiverem sincronizados inicialmente. Mas, se a dispersão for muito alta em outros momentos, o processo NTP no cliente não aceitará mensagens NTP do servidor. A dispersão máxima é 16000; no exemplo, é a dispersão para servidores 10.50.44.69 e 10.50.44.133, portanto o cliente local não aceita o tempo desses servidores.
	
	Se o alcance for zero e a dispersão for muito alta, o cliente provavelmente não aceitará mensagens desse servidor. Consulte a segunda linha do exemplo:
	
	`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.`
	
	Mesmo que o deslocamento seja apenas -4,26, a dispersão é muito alta (talvez devido a um evento passado), e o alcance é zero, então este cliente não aceita tempo deste servidor.

show ntp association detail

Este é um exemplo de saída do 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
```

Os termos já definidos na seção de exibição de associação não são repetidos aqui.

Termo	Explicação
configurado	Esta fonte de tempo NTP foi configurada para ser um servidor. Esse valor também pode ser dinâmico, onde o peer/servidor foi descoberto dinamicamente.
nosso_primário	O cliente local está sincronizado com este par.
selecionado	O peer/servidor é selecionado para possível sincronização, quando 'our_primary' falha ou o cliente perde a sincronização.
são	Os testes de sanidade são usados para testar o pacote NTP recebido de um servidor. Esses testes são especificados no RFC 1305, Especificação, implementação e análise do Network Time Protocol (Versão 3). Os testes são:

Teste	Máscara	Explicação
1	0x01	Pacote duplicado recebido
2	0x02	Pacote falso recebido
3	0x04	Protocolo não sincronizado
4	0x08	Falha na verificação de limite de atraso/dispersão de pares
5	0x10	Falha na autenticação de mesmo nível
6	0x20	Relógio de mesmo nível não sincronizado (comum para servidor não sincronizado)
7	0x40	Camada de mesmo nível fora do limite
8	0x80	Falha na verificação de limite de atraso/dispersão da raiz

Os dados do pacote serão válidos se os testes 1 a 4 forem aprovados. Os dados são usados para calcular o deslocamento, o atraso e a dispersão.

O cabeçalho do pacote é válido se os testes 5 a 8 forem aprovados. Somente pacotes com um cabeçalho válido podem ser usados para determinar se um peer pode ser selecionado para sincronização.

insano	As verificações de integridade falharam, portanto, o tempo do servidor não é aceito. O servidor não está sincronizado.

válido	A hora do par/servidor é válida. O cliente local aceitará desta vez se este peer se tornar o principal.
inválido	A hora do par/servidor é inválida e não pode ser aceita.
ID de referência	Cada peer/servidor recebe uma ID de referência (rótulo).
tempo	Hora é o último carimbo de data/hora recebido desse par/servidor.
nosso modo/ modo par	Este é o estado do cliente/peer local.
our poll intvl/ peer poll intvl	Este é o intervalo de sondagem de nossa sondagem para este peer ou do peer para a máquina local.
retardo de raiz	O atraso raiz é o atraso em milissegundos para a raiz da configuração do NTP. Os relógios do estrato 1 são considerados como estando na raiz de uma configuração/projeto de NTP. No exemplo, todos os três servidores podem ser a raiz porque estão no estrato 1.
dispersão de raiz	A dispersão raiz é a diferença de tempo de relógio máximo que foi observada entre o relógio local e o relógio raiz. Consulte a explicação de 'disp' em show up association para obter mais detalhes.
sync dist.	Essa é uma estimativa da diferença máxima entre o tempo na origem do stratum 0 e o tempo medido pelo cliente; ela consiste em componentes para o tempo de ida e volta, precisão do sistema e desvio do relógio desde a última leitura real da origem do stratum. Em uma configuração NTP grande (servidores NTP no estrato 1 na Internet, com servidores que originam horário em diferentes estratos) com servidores/clientes em vários estratos, a topologia de sincronização NTP deve ser organizada para produzir a maior precisão, mas nunca deve ser permitido formar um loop de sincronização de tempo. Um fator adicional é que cada incremento no estrato envolve um servidor de tempo potencialmente não confiável, que introduz erros de medição adicionais. O algoritmo de seleção usado no NTP usa uma variante do algoritmo de roteamento distribuído Bellman-Ford para calcular as spanning trees de peso mínimo enraizadas nos servidores principais. A métrica da distância usada pelo algoritmo consiste no estrato mais a distância de sincronização, que em si consiste na dispersão mais a metade do atraso absoluto. Assim, o caminho de sincronização sempre leva o número mínimo de servidores para a raiz; os vínculos são resolvidos com base no erro máximo.

atraso	Este é o atraso de ida e volta para o correspondente.
precisão	Esta é a precisão do relógio par em Hz.
versão	Esse é o número da versão do NTP usado pelo peer.
tempo org	Esse é o carimbo de data/hora do originador do pacote NTP; em outras palavras, é o carimbo de data/hora do peer quando ele criou o pacote NTP, mas antes de enviá-lo ao cliente local.

tempo de rcv	Este é o carimbo de data/hora quando o cliente local recebeu a mensagem. A diferença entre o tempo da organização e o tempo de recepção é o deslocamento desse peer. No exemplo, o 10.4.2.254 principal tem estes tempos:
	
	`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)`
	
	A diferença é o deslocamento de 268,3044 ms.

tempo de xmt	Esse é o carimbo de data/hora de transmissão do pacote NTP que o cliente local envia a esse peer/servidor.

filtdelay
filtoffset
filterror
	Esse é o atraso de ida e volta em milissegundos de cada amostra.
	Este é o deslocamento do relógio em milissegundos de cada amostra.
	Este é o erro aproximado de cada amostra.
	
	Um exemplo é o último pacote NTP recebido. No exemplo, o 10.4.2.254 principal tem estes 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`
	
	Essas oito amostras correspondem ao valor do campo reach, que mostra se o cliente local recebeu os últimos oito pacotes NTP.

show ntp status

Este é um exemplo de saída do 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
```

Os termos já definidos na seção show up association ou na seção show ntp association detail não são repetidos.

Termo	Explicação
precisão	A precisão é determinada automaticamente e é medida como uma potência de dois. No exemplo, 2**18 significa 2^(-18), ou 3,8 microssegundos. A perda de sincronização entre peers NTP ou entre um primário e um cliente pode ser devido a uma variedade de causas. O NTP evita a sincronização com uma máquina cujo tempo pode ser ambíguo das seguintes maneiras: 1. O NTP nunca é sincronizado com uma máquina que não esteja sincronizada.

	1. O NTP compara o tempo que é relatado por várias máquinas e não sincroniza com uma máquina cujo tempo é significativamente diferente das outras, mesmo que seu estrato seja menor.

Solucionar problemas de NTP com depurações

Algumas das causas mais comuns de problemas de NTP são:

- Os pacotes NTP não são recebidos.
- Os pacotes NTP são recebidos, mas não são processados pelo processo NTP no Cisco IOS.
- Os pacotes NTP são processados, mas fatores errados ou dados de pacote causam a perda de sincronização.
- O período de relógio do NTP é definido manualmente.

Os comandos debug importantes que ajudam a isolar a causa desses problemas incluem:

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

As próximas seções ilustram o uso de depurações para resolver esses problemas comuns.

Observação: Use a Command Lookup Tool para obter mais informações sobre os comandos usados nesta seção. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Pacotes NTP não recebidos

Use o comando debug ip packet para verificar se os pacotes NTP são recebidos e enviados. Como a saída de depuração pode ser inativa, você pode limitar a saída de depuração com o uso de Listas de Controle de Acesso (ACLs). O NTP usa a porta 123 do User Datagram Protocol (UDP).

1. Criar ACL 101:

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

Os pacotes NTP geralmente têm uma porta origem e destino de 123, portanto isso ajuda a:

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

2. Use esta ACL para limitar a saída do comando debug ip packet:

```
debug ip packet 101
```

3. Se o problema estiver em determinados peers, restrinja a ACL 101 a esses peers. Se o peer for 172.16.1.1, altere a ACL 101 para:

```
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
```

Esta saída de exemplo indica que os pacotes não são enviados:

```
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
```

Depois de confirmar que os pacotes NTP não são recebidos, você deve:

- Verifique se o NTP está configurado corretamente.
- Verifique se uma ACL bloqueia pacotes NTP.
- Verifique se há problemas de roteamento para o IP origem ou destino.

Pacotes NTP não processados

Com os comandos debug ip packet e debug ntp packets habilitados, você pode ver os pacotes que são recebidos e transmitidos e pode ver que o NTP atua nesses pacotes. Para cada pacote NTP recebido (como mostrado por debug ip packet), há uma entrada correspondente gerada por debug ntp packets .

Esta é a saída de depuração quando o processo NTP funciona em pacotes recebidos:

```
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 é um exemplo em que o NTP não funciona em pacotes recebidos. Embora os pacotes NTP sejam recebidos (como mostrado por debug ip packets), o processo NTP não age neles. Para pacotes NTP enviados, uma saída de depuração de pacotes ntp correspondente está presente, pois o processo NTP tem que gerar o pacote. O problema é específico para pacotes NTP recebidos que não são processados.

```
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 FAL
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 FAL
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#
```

Perda de sincronização

Pode ocorrer perda de sincronização se o valor de dispersão e/ou atraso de um servidor for muito alto. Valores altos indicam que os pacotes demoram muito para chegar ao cliente a partir do servidor/peer em referência à raiz do relógio. Portanto, a máquina local não pode confiar na precisão do tempo presente no pacote, porque não sabe quanto tempo o pacote levou para chegar aqui.

O NTP é meticuloso em relação ao tempo e não pode sincronizar com outro dispositivo no qual ele não possa confiar ou não possa ajustar-se de forma a ser confiável.

Se houver um link saturado e o buffer ocorrer ao longo do caminho, os pacotes serão atrasados à medida que chegarem ao cliente NTP. Assim, o timestamp contido em um pacote NTP subsequente pode variar muito ocasionalmente, e o cliente local não pode realmente ajustar essa variação.

O NTP não oferece um método para desativar a validação desses pacotes, a menos que você use o SNTP (Simple Network Time Protocol). O SNTP não é uma grande alternativa, pois não é amplamente suportado no software.

Se ocorrer perda de sincronização, você deverá verificar os links:

- Eles estão saturados?
- Há algum tipo de queda nos links da rede de longa distância (WAN)?
- A criptografia ocorre?

Monitore o valor de alcance do comando show ntp associations detail. O valor mais alto é 377. Se o valor for 0 ou baixo, os pacotes NTP são recebidos intermitentemente e o cliente local sai de sincronia com o servidor.

debug ntp valid

O comando debug ntp valid indica se o pacote NTP falhou nas verificações de sanidade ou validade e revela o motivo da falha. Compare essa saída com os testes de sanidade especificados no RFC1305 que são usados para testar o pacote NTP recebido de um servidor. São definidos oito testes:

Teste	Máscara	Explicação
1	0x01	Pacote duplicado recebido
2	0x02	Pacote falso recebido
3	0x04	Protocolo não sincronizado

4	0x08	Falha na verificação de limite de atraso/dispersão de pares
5	0x10	Falha na autenticação de mesmo nível
6	0x20	Relógio de mesmo nível não sincronizado (comum para servidor não sincronizado)
7	0x40	Camada de mesmo nível fora do limite
8	0x80	Falha na verificação de limite de atraso/dispersão da raiz

Este é um exemplo de saída do comando debug ntp valid:

```
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

Você pode usar o comando debug ntp packets para ver o tempo que o peer/servidor lhe dá no pacote recebido. A máquina local de hora também informa a hora em que ela é informada ao peer/servidor no pacote transmitido.

Campo	Pacote rcv	Pacote xmit
org	Carimbo de data/hora do originador, que é a hora do servidor.	Carimbo de data/hora do originador (cliente) ao enviar o pacote. (O cliente origina um pacote para o servidor.)
Cons	Carimbo de data/hora no cliente quando ele recebeu o pacote.	Hora atual do cliente.

Nesta saída de exemplo, os carimbos de data/hora no pacote recebido do servidor e no pacote enviado para outro servidor são os mesmos, o que indica que o NTP do cliente está em sincronia.

```
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 é um exemplo de saída quando os relógios não estão em sincronia. Observe a diferença de tempo entre o pacote de saída e o pacote rcv. A dispersão do peer pode estar no valor máximo de 16000, e o alcance do peer pode 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 e debug ntp events

O comando debug ntp sync produz saídas de uma linha que mostram se o relógio foi sincronizado ou se a sincronização foi alterada. O comando é geralmente habilitado com debug ntp events.

O comando debug ntp events mostra todos os eventos NTP que ocorrem, o que ajuda a determinar se uma alteração no NTP disparou um problema, como relógios fora de sincronia. (Em outras palavras, se seus relógios felizes sincronizados de repente enlouquecem, você sabe procurar uma mudança ou disparador!)

Este é um exemplo de ambas as depurações. Inicialmente, os relógios do cliente eram sincronizados. O comando debug ntp events mostra que ocorreu uma alteração de estrato de peer NTP e que os relógios, então, saíram de sincronia.

```
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)
```

NTP Clock-period Manually Set

O site Cisco.com avisa que:

"O comando ntp clock-period é gerado automaticamente para refletir o fator de correção que muda constantemente quando o comando copy running-configuration startup-configuration é inserido para salvar a configuração na NVRAM. Não tente usar manualmente o comando ntp clock-period. Certifique-se de remover essa linha de comando ao copiar os arquivos de configuração para outros dispositivos."

O valor do período do relógio depende do hardware, portanto difere para cada dispositivo.

O comando ntp clock-period aparece automaticamente na configuração quando você habilita o NTP. O comando é usado para ajustar o relógio do software. O 'valor de ajuste' compensa o intervalo de pulso de 4 ms, de modo que, com o ajuste secundário, você tenha 1 segundo no final do intervalo.

Se o dispositivo calculou que seu relógio do sistema perde tempo (talvez seja necessário haver uma compensação de frequência a partir do nível básico do roteador), ele adiciona automaticamente esse valor ao relógio do sistema para manter sua sincronia.

Observação: esse comando não deve ser alterado pelo usuário.

O período de relógio NTP padrão para um roteador é 17179869 e é usado essencialmente para iniciar o processo NTP.

A fórmula de conversão é 17179869 * 2^(-32) = 0,00399999995715916156768798828125, ou aproximadamente 4 milissegundos.

Por exemplo, descobriu-se que o relógio do sistema para os roteadores Cisco 2611 (um dos Cisco 2600 Series Routers) estava ligeiramente fora de sincronia e poderia ser ressincronizado com este comando:

```
ntp clock-period 17208078
```

Isso equivale a 17208078 * 2^(-32) = 0,00400656787678599935760498046875, ou um pouco mais de 4 milissegundos.

A Cisco recomenda que você deixe o roteador funcionar por uma semana ou mais em condições normais de rede e depois use o comando wr mem para salvar o valor. Isso fornece um número preciso para a próxima reinicialização e permite que o NTP sincronize mais rapidamente.

Use o comando no ntp clock-period quando salvar a configuração para uso em outro dispositivo, pois esse comando descarta o período de clock de volta ao padrão desse dispositivo específico. Você pode recalcular o valor verdadeiro (mas pode reduzir a precisão do relógio do sistema durante esse período de tempo de recálculo).

Lembre-se de que esse valor depende do hardware, portanto, se você copiar uma configuração e usá-la em dispositivos diferentes, poderá causar problemas. A Cisco planeja substituir o NTP versão 3 pela versão 4 para resolver esse problema.

Se você não estiver ciente desses problemas, poderá optar por alterar manualmente esse valor. Para migrar de um dispositivo para outro, você pode optar por copiar a configuração antiga e colá-la no novo dispositivo. Infelizmente, como o comando ntp clock-period aparece na configuração em execução e na configuração de inicialização, o período de tempo do NTP é colado no novo dispositivo. Quando isso acontece, o NTP no novo cliente sempre sai de sincronia com o servidor com um alto valor de dispersão de peer.

Em vez disso, limpe o NTP clock-period com o comando no ntp clock-period e salve a configuração. O roteador finalmente calcula um período de relógio apropriado para si mesmo.

O comando ntp clock-period não está mais disponível no software Cisco IOS versão 15.0 ou posterior; o analisador agora rejeita o comando com o erro:

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

Você não tem permissão para configurar o período do relógio manualmente, e o período do relógio não é permitido na configuração atual. Como o analisador rejeita o comando se ele estava na configuração de inicialização (em versões anteriores do Cisco IOS, como 12.4), o analisador rejeita o comando quando ele copia a configuração de inicialização para a configuração de execução na inicialização.

O novo comando de substituição é ntp clear drift.

Informações Relacionadas

- Thread do Fórum de Suporte: período de relógio NTP não configurado
- Network Time Protocol: White paper sobre práticas recomendadas
- Solucionar problemas do Network Time Protocol (NTP)
- 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.