Risoluzione dei problemi e debug del protocollo NTP (Network Time Protocol)

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al protocollo NTP (Network Time Protocol) con debug i comandi e il show ntp comando.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

Comandi show NTP

Prima di esaminare la causa dei problemi NTP, è necessario comprendere l'utilizzo e l'output dei seguenti comandi:

- mostra associazione ntp
- mostra dettagli associazione ntp
- mostra stato ntp

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interni.

Nota: lo strumento Output Interpreter supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando show. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interni.

mostra associazione ntp

Un'associazione NTP può essere un'associazione peer (un sistema è disposto a sincronizzarsi con l'altro sistema o a consentire all'altro sistema di sincronizzarsi con esso) o un'associazione server (solo un sistema si sincronizza con l'altro sistema e non il contrario).

Questo è un esempio di output 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
```

Termine	Spiegazione
	I caratteri prima dell'indirizzo hanno le seguenti definizioni: * Sincronizzato con questo peer N. quasi sincronizzato con questo peer + Peer selezionato per la possibile sincronizzazione - Peer è un candidato alla selezione ~ Peer configurato in modo statico
indirizzo	Indirizzo IP del peer. Nell'esempio, la prima voce mostra 127.127.7.1. Ciò indica che il computer locale è sincronizzato con se stesso. In genere, solo un NTP primario esegue la sincronizzazione con se stesso.
orologio di riferimento	Indirizzo dell'orologio di riferimento per il peer. Nell'esempio, i primi sei peer/server hanno un IP privato come clock di riferimento, quindi i loro componenti primari sono probabilmente router, switch o server all'interno della rete locale. Per le ultime quattro voci, l'orologio di riferimento è un IP pubblico, quindi le loro primarie sono probabilmente una fonte di tempo pubblico.
st	La NTP utilizza il concetto di strato per descrivere quanto lontano (negli hop NTP) una macchina da una fonte temporale autorevole. Ad esempio, un server di riferimento ora di strato 1 ha un orologio radio o atomico direttamente collegato. Invia il suo tempo ad un server di tempo di strato 2 attraverso NTP, e così via fino allo strato 16. Una macchina che esegue NTP sceglie automaticamente la macchina con il numero più basso dello strato con cui può comunicare e utilizza NTP come sorgente del tempo.
quando	Il tempo trascorso dalla ricezione dell'ultimo pacchetto NTP da un peer viene segnalato in secondi. Questo valore deve essere inferiore all'intervallo di polling.
sondaggio	L'intervallo di polling è espresso in secondi. L'intervallo in genere inizia con un minimo di intervalli di polling di 64 secondi. L'RFC specifica che non è necessaria più di una transazione NTP al minuto per sincronizzare due computer. Quando l'NTP diventa stabile tra un client e un server, l'intervallo di polling può aumentare a piccoli intervalli da 64 secondi fino a 1024 secondi e in genere si stabilizza nel mezzo. Tuttavia, questo valore cambia in modo dinamico, in base alle condizioni di rete tra il

	client e il server e alla perdita di pacchetti NTP. Se un server non è raggiungibile per un certo periodo di tempo, l'intervallo di polling viene aumentato a intervalli di 1024 secondi per ridurre il sovraccarico della rete. Non è possibile modificare l'intervallo di polling NTP su un router, perché il valore interno è determinato da algoritmi euristici.
portata	La raggiungibilità del peer è una stringa di bit segnalata come valore ottale. In questo campo viene mostrato se gli ultimi otto pacchetti sono stati ricevuti dal processo NTP sul software Cisco IOS®. I pacchetti devono essere ricevuti, elaborati e accettati come validi dal processo NTP e non solo dal router o dallo switch che riceve i pacchetti IP NTP. Per stabilire se un pacchetto è stato ricevuto o meno, la porta usa l'intervallo di polling per il timeout. L'intervallo di polling è il tempo che il protocollo NTP attende prima di concludere che un pacchetto è stato perso. Poiché il tempo necessario per il sondaggio può variare a seconda del peer, anche il tempo prima che REACH decida che un pacchetto è andato perso può variare a seconda del peer. Nell'esempio, sono presenti quattro diversi valori reach: • 377 ottale = 1111111 binario, che indica che il processo NTP ha ricevuto gli ultimi otto pacchetti. • 0 ottale = 00000000, che indica che il processo NTP non ha ricevuto alcun pacchetto. • 1 ottale = 00000001, che indica che il processo NTP ha ricevuto solo il pacchetto più recente. • 357 ottale = 11101111, che indica il pacchetto precedente alla perdita degli ultimi quattro pacchetti. Il campo Reach (Router) è un buon indicatore che indica se i pacchetti NTP vengono scartati a causa di un collegamento scadente, problemi della CPU e altri problemi intermittenti. Unit Converter è un convertitore di unità online per questa e molte altre conversioni.
ritardo	Il ritardo di andata e ritorno al peer viene segnalato in millisecondi. Per impostare l'orologio in modo più accurato, questo ritardo viene preso in considerazione quando si imposta l'ora dell'orologio.
scostamento	L'offset è la differenza di tempo tra i peer o tra il client e il server principale. Questo valore è la correzione che viene applicata a un orologio client per sincronizzarlo. Un valore positivo indica che l'orologio del server è più alto. Un valore negativo indica che l'orologio del client è più alto.

disp	La dispersione, espressa in secondi, è la differenza massima tra l'orologio locale e l'orologio del server mai osservata. Nell'esempio, la dispersione è 0,3 per il server 10.50.36.42, quindi la differenza massima di tempo osservata localmente tra l'orologio locale e l'orologio del server è 0,3 secondi.
	
	Quando gli orologi vengono sincronizzati inizialmente, è possibile che venga visualizzato un valore elevato. Tuttavia, se la dispersione è troppo elevata in altri momenti, il processo NTP sul client non accetta messaggi NTP dal server. La dispersione massima è 16000; nell'esempio, la dispersione per i server è 10.50.44.69 e 10.50.44.133, quindi il client locale non accetta tempo da questi server.
	
	Se la portata è zero e la dispersione è molto elevata, è probabile che il client non accetti messaggi da quel server. Fare riferimento alla seconda riga dell'esempio:
	
	`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.`
	
	Anche se l'offset è appena -4,26, la dispersione è molto alta (forse a causa di un evento passato) e la portata è zero, quindi questo client non accetta tempo da questo server.

mostra dettagli associazione ntp

Questo è un esempio di output 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
```

I termini già definiti nella sezione Mostra associazione non vengono ripetuti in questa sezione.

Termine	Spiegazione
configurato	Questa origine dell'orologio NTP è stata configurata come server. Questo valore può anche essere dinamico, in cui il peer/server è stato individuato dinamicamente.
nostro_primario	Il client locale è sincronizzato con questo peer.
selezionato	Il peer/server è selezionato per la possibile sincronizzazione quando 'our_primary' non riesce o il client perde la sincronizzazione.
sano	I test di integrità vengono usati per verificare il pacchetto NTP ricevuto da un server. Questi test sono specificati nella RFC 1305, Network Time Protocol (versione 3) Specification, Implementation and Analysis. I test sono i seguenti:

Test	Maschera	Spiegazione
1	0x01	Ricevuto pacchetto duplicato
2	0x02	Pacchetto fittizio ricevuto
3	0x04	Protocollo non sincronizzato
4	0x08	Controllo limite non riuscito di ritardo/dispersione peer
5	0x10	Autenticazione peer non riuscita
6	0x20	Orologio peer non sincronizzato (comune per i server non sincronizzati)
7	0x40	Strato peer fuori limite
8	0x80	Controllo limite di dispersione/ritardo radice non riuscito

I dati del pacchetto sono validi se vengono superati i test da 1 a 4. I dati vengono quindi utilizzati per calcolare offset, ritardo e dispersione.

L'intestazione del pacchetto è valida se vengono superati i test da 5 a 8. Per determinare se un peer può essere selezionato per la sincronizzazione, è possibile utilizzare solo pacchetti con un'intestazione valida.

pazzo	Le verifiche di integrità non sono riuscite, pertanto il tempo dal server non è accettato. Server non sincronizzato.

valido	Ora peer/server valida. Il client locale accetta questa ora se il peer diventa il principale.
non valido	Ora del peer/server non valida. Impossibile accettare l'ora.
ID riferimento	A ogni peer/server viene assegnato un ID di riferimento (etichetta).
tempo	L'ora è l'ultimo timestamp ricevuto dal peer/server.
modalità peer/ modalità peer	Questo è lo stato del client/peer locale.
sondaggio intvl/ peer poll intvl	Questo è l'intervallo di polling dal nostro polling a questo peer o dal peer al computer locale.
ritardo radice	Il ritardo principale è il ritardo in millisecondi alla radice dell'installazione NTP. Gli orologi di Stratum 1 sono considerati alla base di una configurazione/progettazione NTP. Nell'esempio, tutti e tre i server possono essere la directory principale perché si trovano nello strato 1.
dispersione della radice	La dispersione radice è la differenza massima di tempo di clock osservata tra l'orologio locale e l'orologio radice. Per ulteriori informazioni, vedere la spiegazione di 'disp' in Mostra associazione.
dist. sincronizzazione	Questa è una stima della differenza massima tra il tempo sull'origine dello strato 0 e il tempo misurato dal client; è costituita da componenti per il tempo di andata e ritorno, la precisione del sistema e la deriva del clock dall'ultima lettura effettiva dell'origine dello strato. In una configurazione NTP di grandi dimensioni (server NTP allo strato 1 in Internet, con server che generano il tempo a diversi strati) con server/client a più strati, la topologia di sincronizzazione NTP deve essere organizzata in modo da produrre la massima accuratezza, ma non deve mai essere consentito di formare un loop di sincronizzazione temporale. Un fattore aggiuntivo è che ogni incremento nello strato coinvolge un time server potenzialmente inaffidabile, che introduce ulteriori errori di misurazione. L'algoritmo di selezione utilizzato nell'NTP utilizza una variante dell'algoritmo di routing distribuito Bellman-Ford per calcolare gli alberi di spanning con peso minimo radicati sui server primari. La metrica della distanza utilizzata dall'algoritmo è costituita dallo strato più la distanza di sincronizzazione, che a sua volta è costituita dalla dispersione più la metà del ritardo assoluto. Pertanto, il percorso di sincronizzazione porta sempre alla radice il numero minimo di server; i legami vengono risolti in base all'errore massimo.

ritardo	Questo è il ritardo di andata e ritorno verso il peer.
precisione	Questa è la precisione dell'orologio peer in Hz.
version	Numero di versione NTP utilizzato dal peer.
ora org.	Questo è il timestamp del mittente del pacchetto NTP; in altre parole, è il timestamp del peer quando ha creato il pacchetto NTP, ma prima di inviare il pacchetto al client locale.

ora rcv	Timestamp della ricezione del messaggio da parte del client locale. La differenza tra l'ora dell'organizzazione e l'ora della ricezione è lo scostamento per questo peer. Nell'esempio, il valore 10.4.2.254 per l'elemento primario ha i seguenti valori:
	
	`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 differenza è la posizione relativa di 268,3044 msec.

tempo di trasmissione	Timestamp di trasmissione per il pacchetto NTP inviato dal client locale a questo peer/server.

ritardofiltro
scostamento filtro
	Questo è il ritardo di andata e ritorno in millisecondi di ciascun campione.
	Questo è l'offset dell'orologio in millisecondi di ciascun campione.
	Questo è l'errore approssimativo di ciascun campione.
	
	Un esempio è l'ultimo pacchetto NTP ricevuto. Nell'esempio, il valore della variabile primaria 10.4.2.254 è il seguente:
	
	`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`
	
	Questi otto esempi corrispondono al valore del campo reach che mostra se il client locale ha ricevuto gli ultimi otto pacchetti NTP.

mostra stato ntp

Questo è un esempio di output 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
```

I termini già definiti nella sezione di visualizzazione dell'associazione o nella sezione di visualizzazione dei dettagli dell'associazione ntp non vengono ripetuti.

Termine	Spiegazione
precisione	La precisione viene determinata automaticamente e viene misurata come potenza di due. Nell'esempio, 2**18 significa 2^(-18), o 3,8 microsecondi. La perdita di sincronizzazione tra peer NTP o tra un server primario e un client può essere dovuta a diverse cause. Il protocollo NTP evita la sincronizzazione con un computer il cui tempo può essere ambiguo nei seguenti modi: 1. NTP non esegue mai la sincronizzazione con un computer non sincronizzato.

	1. L'NTP confronta l'ora riportata da diverse macchine e non si sincronizza con una macchina il cui tempo è significativamente diverso dagli altri, anche se il suo strato è più basso.

Risoluzione dei problemi dell'NTP con i debug

Alcune delle cause più comuni dei problemi NTP sono:

- I pacchetti NTP non vengono ricevuti.
- I pacchetti NTP vengono ricevuti, ma non elaborati dal processo NTP sul sistema operativo Cisco IOS.
- I pacchetti NTP vengono elaborati, ma la perdita di sincronizzazione è causata da fattori o dati errati.
- Il periodo di clock NTP è impostato manualmente.

I comandi di debug importanti per isolare la causa di questi problemi includono:

- debug ip packets <acl>
- pacchetti debug ntp
- debug ntp validità
- debug ntp sync

- debug di eventi ntp

Nelle sezioni seguenti viene descritto l'utilizzo dei debug per risolvere i problemi comuni.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interni.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

Pacchetti NTP non ricevuti

Usare il comando debug ip packet per controllare se i pacchetti NTP vengono ricevuti e inviati. Poiché l'output del comando debug può essere richiamato tramite chat, è possibile limitare l'output del comando debug usando gli Access Control Lists (ACL). NTP utilizza la porta 123 UDP (User Datagram Protocol).

1. Creazione di ACL 101:

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

I pacchetti NTP in genere hanno una porta di origine e di destinazione di 123, quindi questo aiuta:

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

2. Usare questo ACL per limitare l'output del comando debug ip packet:

```
debug ip packet 101
```

3. Se il problema riguarda alcuni peer, restringere l'ACL 101 a questi peer. Se il peer è 172.16.1.1, modificare ACL 101 in:

```
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
```

Questo output di esempio indica che i pacchetti non vengono inviati:

```
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
```

Dopo aver confermato che i pacchetti NTP non vengono ricevuti, è necessario:

- Verificare che NTP sia configurato correttamente.
- Verificare se un ACL blocca i pacchetti NTP.
- Verificare la presenza di problemi di routing all'IP di origine o di destinazione.

Pacchetti NTP non elaborati

Se i comandi debug ip packet e debug ntp packets sono abilitati, è possibile visualizzare i pacchetti ricevuti e trasmessi e verificare che il protocollo NTP agisce su tali pacchetti. Per ogni pacchetto NTP ricevuto (come mostrato dal pacchetto ip di debug), è presente una voce corrispondente generata dai pacchetti ntp di debug.

Questo è l'output del comando debug quando il processo NTP funziona sui pacchetti ricevuti:

```
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)
```

Questo è un esempio di come il protocollo NTP non funzioni sui pacchetti ricevuti. Anche se i pacchetti NTP vengono ricevuti (come mostrato dai pacchetti ip di debug), il processo NTP non interviene su di essi. Per i pacchetti NTP inviati, è presente un output corrispondente dei pacchetti ntp di debug, in quanto il processo NTP deve generare il pacchetto. Il problema è specifico dei pacchetti NTP ricevuti che non vengono elaborati.

```
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#
```

Perdita di sincronizzazione

La perdita di sincronizzazione può verificarsi se la dispersione e/o il valore di ritardo di un server diventa molto elevato. Valori alti indicano che i pacchetti impiegano troppo tempo per raggiungere il client dal server/peer in riferimento alla radice dell'orologio. Il computer locale non può quindi fidarsi dell'accuratezza del tempo presente nel pacchetto, perché non sa quanto tempo è stato necessario affinché il pacchetto arrivasse qui.

NTP è meticoloso circa il tempo e non può sincronizzarsi con un altro dispositivo che non può considerare attendibile o non può regolare in modo tale da poter essere considerato attendibile.

Se si verifica un collegamento saturo e un buffering durante il percorso, i pacchetti vengono ritardati quando arrivano al client NTP. Pertanto,

l'indicatore orario contenuto in un pacchetto NTP successivo può variare occasionalmente molto e il client locale non è in grado di adattarsi a tale variazione.

Il protocollo NTP non offre un metodo per disattivare la convalida di questi pacchetti a meno che non si utilizzi il protocollo SNTP (Simple Network Time Protocol). L'SNTP non è un'alternativa valida perché non è ampiamente supportato nel software.

In caso di perdita della sincronizzazione, è necessario controllare i collegamenti:

- Sono sature?
- I collegamenti della rete WAN (Wide Area Network) presentano cadute di qualsiasi tipo
- Viene eseguita la crittografia?

Monitorare il valore reach dal comando show ntp association detail. Il valore più alto è 377. Se il valore è 0 o basso, i pacchetti NTP vengono ricevuti in modo intermittente e il client locale non è più sincronizzato con il server.

debug ntp validità

Il comando debug ntp invalid indica se il pacchetto NTP non ha superato i controlli di integrità o validità e indica la causa dell'errore. Confrontare questo output con i test di integrità specificati in RFC1305 e utilizzati per testare il pacchetto NTP ricevuto da un server. Sono definiti otto test:

Test	Maschera	Spiegazione
1	0x01	Ricevuto pacchetto duplicato
2	0x02	Pacchetto fittizio ricevuto

3	0x04	Protocollo non sincronizzato
4	0x08	Controllo limite non riuscito di ritardo/dispersione peer
5	0x10	Autenticazione peer non riuscita
6	0x20	Orologio peer non sincronizzato (comune per i server non sincronizzati)
7	0x40	Strato peer fuori limite
8	0x80	Controllo limite di dispersione/ritardo radice non riuscito

Di seguito viene riportato un esempio di output del 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
```

pacchetti debug ntp

È possibile usare il comando debug ntp packets per verificare il tempo che il peer/server restituisce all'utente nel pacchetto ricevuto. Il computer locale indica anche l'ora che conosce il peer/server nel pacchetto trasmesso.

Campo	RCV Packet	Emetti pacchetto
org	Timestamp del creatore, ovvero l'ora del server.	Timestamp del mittente (client) quando ha inviato il pacchetto. Il client invia un pacchetto al server.
cons	Timestamp sul client quando riceve il pacchetto.	Ora corrente client.

In questo output di esempio, i timestamp nel pacchetto ricevuto dal server e nel pacchetto inviato a un altro server sono gli stessi, il che indica

che l'NTP del client è sincronizzato.

```
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)
```

Questo è un esempio di output in cui gli orologi non sono sincronizzati. Si noti la differenza di tempo tra il pacchetto di uscita e il pacchetto rcv. La dispersione peer può essere al valore massimo di 16000 e la portata del peer può essere 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 ed debug ntp events

Il comando debug ntp sync produce output a riga singola che mostrano se l'orologio è stato sincronizzato o se la sincronizzazione è stata modificata. Il comando è generalmente abilitato con gli eventi debug ntp.

Il comando debug ntp events visualizza gli eventi NTP che si verificano, consentendo di determinare se una modifica del NTP ha causato un problema, ad esempio orologi che non sono più sincronizzati. (In altre parole, se gli orologi felicemente sincronizzati improvvisamente impazziscono, si sa per cercare un cambiamento o trigger!)

Questo è un esempio di entrambi i debug. Inizialmente, gli orologi dei client sono stati sincronizzati. Il comando debug ntp events indica che si è verificata una modifica dello strato peer NTP e che gli orologi non sono più sincronizzati.

```
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)
```

Impostazione manuale periodo di clock NTP

Il sito Web Cisco.com avverte che:

"Il comando ntp clock-period viene generato automaticamente per riflettere il fattore di correzione che cambia costantemente quando si immette il comando copy running-configuration startup-configuration per salvare la configurazione nella NVRAM. Non tentare di utilizzare manualmente il comando ntp clock-period. Assicurarsi di rimuovere questa riga di comando quando si copiano i file di configurazione su altri

dispositivi."

Il valore del periodo di clock dipende dall'hardware, quindi differisce per ogni dispositivo.

Il comando ntp clock-period viene visualizzato automaticamente nella configurazione quando si abilita NTP. Il comando è usato per regolare l'orologio del software. Il 'valore di regolazione' compensa l'intervallo di graduazione di 4 msec, in modo che, con la regolazione minore, si ottenga 1 secondo alla fine dell'intervallo.

Se il dispositivo ha calcolato che l'orologio di sistema perde tempo (è possibile che sia necessaria una compensazione della frequenza a partire dal livello base del router), aggiunge automaticamente questo valore all'orologio di sistema per mantenerne la sincronia.

Nota: questo comando non deve essere modificato dall'utente.

Il periodo di clock NTP predefinito per un router è 17179869 e viene usato essenzialmente per avviare il processo NTP.

La formula di conversione è 17179869 * 2^(-32) = 0,00399999957159161567687988281 25, ovvero circa 4 millisecondi.

Ad esempio, l'orologio di sistema per i router Cisco 2611 (uno dei router Cisco serie 2600) è risultato leggermente non sincronizzato e potrebbe essere risincronizzato con questo comando:

```
ntp clock-period 17208078
```

Equivale a 17208078 * 2^(-32) = 0,00400656787678599357604980468 75, o poco più di 4 millisecondi.

Cisco consiglia di lasciare in esecuzione il router per una settimana o giù di lì in condizioni di rete normali e quindi di utilizzare il comando wr mem per salvare il valore. In questo modo è possibile ottenere una cifra accurata per il riavvio successivo e sincronizzare più rapidamente NTP.

Quando si salva la configurazione per l'utilizzo su un altro dispositivo, usare il comando no ntp clock-period perché questo comando riporta il periodo di clock al valore predefinito di quel particolare dispositivo. È possibile ricalcolare il valore effettivo, ma è possibile ridurre la precisione dell'orologio di sistema durante il periodo di tempo di ricalcolo.

Tenere presente che questo valore dipende dall'hardware, quindi se si copia una configurazione e la si utilizza su dispositivi diversi, è possibile che si verifichino dei problemi. Per risolvere il problema, Cisco intende sostituire l'NTP versione 3 con la versione 4.

Se non si è a conoscenza di questi problemi, è possibile decidere di intervenire manualmente su questo valore. Per eseguire la migrazione da un dispositivo a un altro, è possibile scegliere di copiare la configurazione precedente e incollarla nel nuovo dispositivo. Purtroppo, poiché il comando ntp clock-period viene visualizzato in running-config e startup-config, il comando NTP clock-period viene incollato sul nuovo

dispositivo. In questo caso, l'NTP sul nuovo client non è sempre sincronizzato con il server con un valore di dispersione peer elevato.

Cancellare invece il periodo di clock NTP con il comando no ntp clock-period, quindi salvare la configurazione. Il router infine calcola il periodo di clock appropriato per se stesso.

Il comando ntp clock-period non è più disponibile nel software Cisco IOS versione 15.0 o successive; il parser rifiuta il comando con l'errore:

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

Non è consentito configurare manualmente il periodo di tempo né configurare il periodo di tempo nella configurazione in esecuzione. Poiché il parser rifiuta il comando se si trova nella configurazione di avvio (nelle versioni precedenti di Cisco IOS, ad esempio la 12.4), il parser rifiuta il comando quando copia la configurazione di avvio nella configurazione di avvio in esecuzione-config all'avvio.

Il nuovo comando di sostituzione è ntp clear drift.

Informazioni correlate

- Thread del forum di supporto: periodo di clock NTP non configurato
- Protocollo ora di rete: white paper sulle best practice
- Risoluzione dei problemi del protocollo Network Time Protocol (NTP)
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

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