Dépannage et débogage des problèmes liés au protocole NTP (Network Time Protocol)

Table des matières

Introduction

Ce document décrit comment dépanner les problèmes de protocole NTP (Network Time Protocol) avec les debug commandes et la show ntp commande.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Commandes show NTP

Avant d'examiner la cause des problèmes NTP, vous devez comprendre l'utilisation et le résultat de ces commandes :

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

Remarque : utilisez l'outil Command Lookup Tool afin d'obtenir plus d'informations sur les commandes utilisées dans cette section. Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils internes.

Remarque : l'outil Output Interpreter prend en charge certaines commandes show. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie . Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils internes.

show ntp association

Une association NTP peut être une association d'homologues (un système est prêt à se synchroniser avec l'autre système ou à permettre à l'autre système de se synchroniser avec lui) ou une association de serveur (un seul système se synchronise avec l'autre système et non l'inverse).

Voici un exemple du résultat de la commande 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
```

Terme	Explication
	Les caractères situés avant l'adresse sont définis comme suit : * Synchronisé avec cet homologue # Presque synchronisé avec cet homologue + Homologue sélectionné pour une synchronisation possible - Peer est un candidat à la sélection ~ L'homologue est configuré de manière statique
adresse	Il s'agit de l'adresse IP de l'homologue. Dans l'exemple, la première entrée affiche 127.127.7.1. Cela indique que l'ordinateur local s'est synchronisé avec lui-même. En général, seul un NTP principal se synchronise avec lui-même.
horloge ref	Il s'agit de l'adresse de l'horloge de référence de l'homologue. Dans l'exemple, les six premiers homologues/serveurs ont une adresse IP privée comme horloge de référence, de sorte que leurs principaux sont probablement des routeurs, des commutateurs ou des serveurs au sein du réseau local. Pour les quatre dernières entrées, l'horloge de référence est une adresse IP publique, de sorte que leurs primaires sont probablement une source temporelle publique.
st	NTP utilise le concept d'une strate afin de décrire la distance (en sauts NTP) d'une machine par rapport à une source temporelle faisant autorité. Par exemple, un serveur de temps de strate 1 est directement relié à une horloge radio ou atomique. Il envoie son temps à un serveur de temps de strate 2 via NTP, et ainsi de suite jusqu'à la strate 16. Une machine qui exécute NTP choisit automatiquement la machine avec le numéro de strate le plus bas avec laquelle elle peut communiquer et utilise NTP comme source de temps.
quand	Le temps écoulé depuis la réception du dernier paquet NTP d'un homologue est indiqué en secondes. Cette valeur doit être inférieure à l'intervalle d'interrogation.
vote	L'intervalle d'interrogation est signalé en secondes. L'intervalle commence généralement par des intervalles d'interrogation d'au moins 64 secondes. La RFC spécifie qu'aucune transaction NTP par minute n'est nécessaire pour synchroniser deux machines. Lorsque le protocole NTP devient stable entre un client et un serveur, l'intervalle d'interrogation peut augmenter par petites étapes de 64 secondes à 1024 secondes et se stabilise généralement quelque part entre les deux. Cependant, cette valeur change dynamiquement, en fonction des conditions réseau entre le client et le serveur et de la perte de paquets NTP. Si un serveur est

	inaccessible pendant un certain temps, l'intervalle d'interrogation est augmenté par étapes à 1024 secondes afin de réduire la surcharge du réseau. Il n'est pas possible d'ajuster l'intervalle d'interrogation NTP sur un routeur, car l'intervalle interne est déterminé par des algorithmes heuristiques.
section droite	L'accessibilité de l'homologue est une chaîne de bits signalée comme une valeur octale. Ce champ indique si les huit derniers paquets ont été reçus par le processus NTP sur le logiciel Cisco IOS®. Les paquets doivent être reçus, traités et acceptés comme valides par le processus NTP et pas seulement par le routeur ou le commutateur qui reçoit les paquets IP NTP. Reach utilise l'intervalle d'interrogation pendant un certain temps afin de décider si un paquet a été reçu ou non. L'intervalle d'interrogation est le temps que NTP attend avant de conclure qu'un paquet a été perdu. L'heure d'interrogation peut être différente pour différents homologues, de sorte que l'heure avant la portée décide qu'un paquet a été perdu peut également être différente pour différents homologues. Dans l'exemple, il existe quatre valeurs de portée différentes : • 377 octal = 11111111 binaire, qui indique que le processus NTP a reçu les huit derniers paquets. • 0 octal = 00000000, ce qui indique que le processus NTP n'a reçu aucun paquet. • 1 octal = 00000001, ce qui indique que le processus NTP a reçu uniquement le dernier paquet. • 357 octal = 11101111, ce qui indique que le paquet avant les quatre derniers paquets a été perdu. La portée est un bon indicateur pour savoir si les paquets NTP sont abandonnés en raison d'une liaison médiocre, de problèmes de CPU et d'autres problèmes intermittents. Unit Converter est un convertisseur d'unités en ligne pour cette conversion et bien d'autres.
retard	Le délai de transmission aller-retour vers l'homologue est signalé en millisecondes. Afin de régler l'horloge avec plus de précision, ce retard est pris en compte lors du réglage de l'heure d'horloge.
décalage	Le décalage est la différence de temps d'horloge entre les homologues ou entre le principal et le client. Cette valeur est la correction qui est appliquée à une horloge client afin de la synchroniser. Une valeur positive indique que l'horloge du serveur est plus élevée. Une valeur négative indique que l'horloge du client est plus élevée.

immerger	La dispersion, rapportée en secondes, est la différence de temps d'horloge maximale jamais observée entre l'horloge locale et l'horloge du serveur. Dans l'exemple, la dispersion est de 0,3 pour le serveur 10.50.36.42, de sorte que la différence de temps maximale jamais observée localement entre l'horloge locale et l'horloge du serveur est de 0,3 seconde.
	
	Vous pouvez vous attendre à voir une valeur élevée lorsque les horloges sont synchronisées initialement. Mais, si la dispersion est trop élevée à d'autres moments, le processus NTP sur le client n'accepte pas les messages NTP du serveur. La dispersion maximale est 16000 ; dans l'exemple, il s'agit de la dispersion pour les serveurs 10.50.44.69 et 10.50.44.133, de sorte que le client local n'accepte pas le temps de ces serveurs.
	
	Si la portée est nulle et que la dispersion est très élevée, le client n'accepte probablement pas les messages provenant de ce serveur. Reportez-vous à la deuxième ligne de l'exemple :
	
	`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.`
	
	Même si le décalage est seulement de -4,26, la dispersion est très élevée (peut-être en raison d'un événement passé), et la portée est nulle, donc ce client n'accepte pas le temps de ce serveur.

show ntp association detail

Voici un exemple de résultat de la commande 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
```

Les termes déjà définis dans la section show up association ne sont pas répétés ici.

Terme	Explication
configuré	Cette source d'horloge NTP a été configurée pour être un serveur. Cette valeur peut également être dynamique, lorsque l'homologue/serveur a été détecté de manière dynamique.
our_primary	Le client local est synchronisé avec cet homologue.
sélectionné	L'homologue/serveur est sélectionné pour une éventuelle synchronisation, lorsque 'our_primary' échoue ou que le client perd la synchronisation.
sain d'esprit	Des tests d'intégrité sont utilisés afin de tester le paquet NTP reçu d'un serveur. Ces tests sont spécifiés dans le document RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis. Les tests sont les suivants :

Essai	Masque	Explication
1	0x01	Paquet en double reçu
2	0x02	Faux paquet reçu
3	0x04	Protocole non synchronisé
4	0x08	Échec du contrôle des limites du délai/de la dispersion des homologues
5	0x10	Échec de l'authentification homologue
6	0x20	Horloge d'homologue non synchronisée (courante pour les serveurs non synchronisés)
7	0x40	Strate homologue hors limite
8	0x80	Échec de la vérification des limites du délai racine/dispersion

Les données de paquet sont valides si les tests 1 à 4 sont réussis. Les données sont ensuite utilisées pour calculer le décalage, le délai et la dispersion.

L’en-tête de paquet est valide si les tests 5 à 8 sont réussis. Seuls les paquets avec un en-tête valide peuvent être utilisés pour déterminer si un homologue peut être sélectionné pour la synchronisation.

dingue	Les contrôles de validité ont échoué, par conséquent, le temps passé à partir du serveur n'est pas accepté. Le serveur est désynchronisé.

valable	L'heure de l'homologue/serveur est valide. Le client local accepte ce délai si cet homologue devient le principal.
infirme	L'heure de l'homologue/serveur n'est pas valide et ne peut pas être acceptée.
ID de référence	Un ID de référence (étiquette) est attribué à chaque homologue/serveur.
Heure	L'heure est le dernier horodatage reçu de cet homologue/serveur.
notre mode / mode homologue	Il s'agit de l'état du client/homologue local.
notre sondage intvl/ peer poll intvl	Il s'agit de l'intervalle d'interrogation entre notre interrogation et cet homologue ou entre l'homologue et l'ordinateur local.
délai racine	Le délai racine est le délai en millisecondes à la racine de la configuration NTP. Les horloges de strate 1 sont considérées comme étant à la racine d'une configuration/conception NTP. Dans l'exemple, les trois serveurs peuvent être la racine, car ils se trouvent au niveau de la strate 1.
dispersion des racines	La dispersion racine est la différence de temps d'horloge maximale jamais observée entre l'horloge locale et l'horloge racine. Reportez-vous à l'explication de « disp » sous show up association pour plus de détails.
dist. synch.	Il s'agit d'une estimation de la différence maximale entre le temps sur la source de la strate 0 et le temps mesuré par le client ; elle comprend des composantes pour le temps aller-retour, la précision du système et la dérive d'horloge depuis la dernière lecture réelle de la source de la strate. Dans une configuration NTP de grande taille (serveurs NTP au niveau de la strate 1 sur Internet, avec des serveurs qui génèrent l'heure à différentes strates) avec des serveurs/clients à plusieurs strates, la topologie de synchronisation NTP doit être organisée afin de produire la plus grande précision, mais ne doit jamais être autorisée à former une boucle de synchronisation temporelle. Un autre facteur est que chaque incrément de strate implique un serveur de temps potentiellement non fiable, ce qui introduit des erreurs de mesure supplémentaires. L'algorithme de sélection utilisé dans NTP utilise une variante de l'algorithme de routage distribué Bellman-Ford afin de calculer les Spanning Tree de poids minimum enracinés sur les serveurs principaux. La métrique de distance utilisée par l'algorithme est constituée de la strate plus la distance de synchronisation, elle-même constituée de la dispersion plus la moitié du délai absolu. Ainsi, le chemin de synchronisation prend toujours le nombre minimum de serveurs à la racine ; les liens sont résolus sur la base de l'erreur

	maximale.
retard	Il s'agit du délai de transmission aller-retour vers l'homologue.
fidélité	Il s'agit de la précision de l'horloge homologue en Hz.
version	Il s'agit du numéro de version NTP utilisé par l'homologue.
heure de l'organisation	Il s'agit de l'horodatage de l'expéditeur du paquet NTP ; en d'autres termes, il s'agit de l'horodatage de l'homologue lorsqu'il a créé le paquet NTP, mais avant qu'il n'envoie le paquet au client local.

heure de retour à la normale	Il s'agit de l'horodatage de réception du message par le client local. La différence entre l'heure de l'organisation et l'heure de réception est le décalage pour cet homologue. Dans l'exemple, le réseau principal 10.4.2.254 a ces heures :
	
	`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 différence correspond au décalage de 268,3044 ms.

heure xmt	Il s'agit de l'horodatage de transmission pour le paquet NTP que le client local envoie à cet homologue/serveur.

retard
d'écoulement
filtoffset
terreur
cinématographique
	Il s'agit du délai d'aller-retour en millisecondes de chaque échantillon.
	Il s'agit du décalage d'horloge en millisecondes de chaque échantillon.
	Il s'agit de l'erreur approximative de chaque échantillon.
	
	Un exemple est le dernier paquet NTP reçu. Dans l'exemple, le primaire 10.4.2.254 a les valeurs suivantes :
	
	`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`
	
	Ces huit échantillons correspondent à la valeur du champ reach, qui indique si le client local a reçu les huit derniers

	paquets NTP.

show ntp status

Voici un exemple de résultat de la commande 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
```

Les termes déjà définis dans la section show up association ou show ntp association detail ne sont pas répétés.

Terme	Explication
fidélité	La précision est déterminée automatiquement et mesurée comme une puissance de deux. Dans l'exemple, 2**18 signifie 2^(-18), soit 3,8 microsecondes. La perte de synchronisation entre les homologues NTP ou entre un client et un serveur principal peut être due à diverses causes. NTP évite la synchronisation avec une machine dont l'heure peut être ambiguë de ces manières :

	1. NTP ne se synchronise jamais sur une machine qui n'est pas elle-même synchronisée. 1. NTP compare l'heure qui est rapportée par plusieurs machines et ne se synchronise pas avec une machine dont l'heure est significativement différente des autres, même si sa strate est plus basse.

Dépannage de NTP avec des débogages

Les causes les plus courantes des problèmes NTP sont les suivantes :

- Les paquets NTP ne sont pas reçus.
- Les paquets NTP sont reçus, mais ne sont pas traités par le processus NTP sur Cisco IOS.
- Les paquets NTP sont traités, mais des facteurs ou des données de paquets erronés entraînent une perte de synchronisation.
- La période d'horloge NTP est définie manuellement.

Les commandes de débogage importantes qui permettent d'isoler la cause de ces problèmes sont les suivantes :

- debug ip packets <acl>
- debug ntp packets

- debug ntp valid
- debug ntp sync
- debug ntp events

Les sections suivantes illustrent l'utilisation des débogages afin de résoudre ces problèmes courants.

Remarque : utilisez l'outil Command Lookup Tool afin d'obtenir plus d'informations sur les commandes utilisées dans cette section. Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils internes.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d’utiliser les commandes de débogage.

Paquets NTP non reçus

Utilisez la commande debug ip packet afin de vérifier si les paquets NTP sont reçus et envoyés. Puisque la sortie de débogage peut être bavarde, vous pouvez limiter la sortie de débogage avec l'utilisation de listes de contrôle d'accès (ACL). NTP utilise le port 123 du protocole UDP (User Datagram Protocol).

1. Créer ACL 101 :

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

Les paquets NTP ont généralement un port source et de destination de 123, ce qui permet de :

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

2. Utilisez cette liste de contrôle d’accès afin de limiter le résultat de la commande debug ip packet :

```
debug ip packet 101
```

3. Si le problème concerne des homologues particuliers, limitez la liste de contrôle d'accès 101 à ces homologues. Si l'homologue est 172.16.1.1, remplacez ACL 101 par :

```
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
```

Cet exemple de résultat indique que les paquets ne sont pas envoyés :

```
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 FALS
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
```

Une fois que vous avez confirmé que les paquets NTP ne sont pas reçus, vous devez :

- Vérifiez si le protocole NTP est correctement configuré.
- Vérifiez si une liste de contrôle d'accès bloque les paquets NTP.
- Vérifiez les problèmes de routage vers l'adresse IP source ou de destination.

Paquets NTP non traités

Avec les commandes debug ip packet et debug ntp packets activées, vous pouvez voir les paquets qui sont reçus et transmis, et vous pouvez voir que NTP agit sur ces paquets. Pour chaque paquet NTP reçu (comme indiqué par debug ip packet), il y a une entrée correspondante générée par debug ntp packets .

Voici la sortie de débogage quand le processus NTP fonctionne sur les paquets reçus :

```
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)
```

Voici un exemple où NTP ne fonctionne pas sur les paquets reçus. Bien que les paquets NTP soient reçus (comme indiqué par debug ip packets), le processus NTP n'agit pas sur eux. Pour les paquets NTP qui sont envoyés, une sortie debug ntp packets correspondante est présente, parce que le processus NTP doit générer le paquet. Le problème est spécifique aux paquets NTP reçus qui ne sont pas traités.

```
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#
```

Perte de synchronisation

Une perte de synchronisation peut se produire si la valeur de dispersion et/ou de délai d'un serveur devient très élevée. Les valeurs élevées indiquent que les paquets mettent trop de temps pour parvenir au client à partir du serveur/homologue en référence à la racine de l'horloge. Ainsi, la machine locale ne peut pas faire confiance à la précision du temps présent dans le paquet, car elle ne sait pas combien de temps il a fallu au paquet pour arriver ici.

NTP est méticuleux quant au temps et ne peut pas se synchroniser avec un autre périphérique auquel il ne peut pas faire confiance ou qu'il ne peut pas ajuster de manière à ce qu'il puisse être fiable.

S'il y a une liaison saturée et que la mise en mémoire tampon se produit en cours de route, les paquets sont retardés lorsqu'ils arrivent au client NTP. Ainsi, l'horodatage contenu dans un paquet NTP suivant peut parfois varier beaucoup, et le client local ne peut pas vraiment s'ajuster pour cette variance.

NTP ne propose pas de méthode pour désactiver la validation de ces paquets, sauf si vous utilisez le protocole SNTP (Simple Network Time Protocol). Le protocole SNTP n'est pas une alternative très intéressante, car il n'est pas largement pris en charge par les logiciels.

En cas de perte de synchronisation, vous devez vérifier les liens suivants :

- Sont-ils saturés ?
- Les liaisons de votre réseau étendu (WAN) comportent-elles des types de branchement ?
- Le chiffrement est-il effectué ?

Surveillez la valeur de portée à partir de la commande show ntp associations detail. La valeur maximale est 377. Si la valeur est 0 ou faible, les paquets NTP sont reçus par intermittence et le client local se désynchronise du serveur.

debug ntp valid

La commande debug ntp valid indique si le paquet NTP a échoué aux contrôles de validité ou de validité et indique la raison de l'échec. Comparez cette sortie aux tests de santé spécifiés dans la RFC1305 qui sont utilisés afin de tester le paquet NTP reçu d'un serveur. Huit tests sont définis :

Essai	Masque	Explication
1	0x01	Paquet en double reçu

2	0x02	Faux paquet reçu
3	0x04	Protocole non synchronisé
4	0x08	Échec du contrôle des limites du délai/de la dispersion des homologues
5	0x10	Échec de l'authentification homologue
6	0x20	Horloge d'homologue non synchronisée (courante pour les serveurs non synchronisés)
7	0x40	Strate homologue hors limite
8	0x80	Échec de la vérification des limites du délai racine/dispersion

Voici un exemple de sortie de la commande 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

Vous pouvez utiliser la commande debug ntp packets afin de voir l'heure que l'homologue/serveur vous donne dans le paquet reçu. La machine locale de temps indique également l'heure qu'elle connaît à l'homologue/serveur dans le paquet transmis.

Champ	Paquet rcv	Paquet de sortie
org	Horodatage de l'expéditeur, qui correspond à l'heure du serveur.	Horodatage de l’expéditeur (client) lors de l’envoi du paquet. (Le client envoie un paquet au serveur.)
rec	Horodatage sur le client lors de la réception du	Heure actuelle du client.

	paquet.	

Dans cet exemple de sortie, les horodatages du paquet reçu du serveur et du paquet envoyé à un autre serveur sont identiques, ce qui indique que le client NTP est synchronisé.

```
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)
```

Ceci est un exemple de sortie lorsque les horloges ne sont pas synchronisées. Notez la différence de temps entre le paquet xmit et le paquet rcv. La dispersion de l'homologue peut être égale à la valeur maximale 16000 et la portée de l'homologue peut être égale à 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 et debug ntp events

La commande debug ntp sync produit des sorties sur une ligne qui indiquent si l'horloge a été synchronisée ou si la synchronisation a changé. La

commande est généralement activée avec les événements debug ntp.

La commande debug ntp events affiche tous les événements NTP qui se produisent, ce qui vous aide à déterminer si une modification dans le NTP a déclenché un problème tel que des horloges qui ne sont pas synchronisées. (En d'autres termes, si vos horloges heureusement synchronisées deviennent soudainement folles, vous savez chercher un changement ou un déclencheur !)

Voici un exemple des deux débogages. Initialement, les horloges du client étaient synchronisées. La commande debug ntp events montre qu'un changement de strate d'homologue NTP s'est produit, et les horloges se sont désynchronisées.

```
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)
```

Période d'horloge NTP définie manuellement

Le site Web Cisco.com avertit que :

"La commande ntp clock-period est générée automatiquement pour refléter le facteur de correction qui change constamment lorsque la commande copy running-configuration startup-configuration est entrée pour enregistrer la configuration dans la mémoire NVRAM. N'essayez pas d'utiliser manuellement la commande ntp clock-period. Veillez à supprimer cette ligne de commande lorsque vous copiez des fichiers de configuration sur d'autres périphériques."

La valeur de la période d'horloge dépend du matériel, elle diffère donc pour chaque périphérique.

La commande ntp clock-period apparaît automatiquement dans la configuration lorsque vous activez NTP. La commande est utilisée afin de régler l'horloge du logiciel. La « valeur d'ajustement » compense l'intervalle de graduation de 4 ms, de sorte qu'avec l'ajustement mineur, vous avez 1 seconde à la fin de l'intervalle.

Si le périphérique a calculé que son horloge système perd du temps (il doit peut-être y avoir une compensation de fréquence à partir du niveau de base du routeur), il ajoute automatiquement cette valeur à l'horloge système afin de maintenir sa synchronicité.

Remarque : l'utilisateur ne doit pas modifier cette commande.

La période d'horloge NTP par défaut pour un routeur est 17179869 et est essentiellement utilisée pour démarrer le processus NTP.

La formule de conversion est 17179869 * 2^(-32) = 0,00399999995715916156768798828125, soit environ 4 millisecondes.

Par exemple, l'horloge système des routeurs Cisco 2611 (l'un des routeurs de la gamme Cisco 2600) est légèrement désynchronisée et peut être resynchronisée à l'aide de cette commande :

```
ntp clock-period 17208078
```

Cela équivaut à 17208078 * 2^(-32) = 0,00400656787678599357604980468750, soit un peu plus de 4 millisecondes.

Cisco recommande de laisser le routeur fonctionner pendant une semaine environ dans des conditions réseau normales, puis d'utiliser la commande wr mem afin d'enregistrer la valeur. Cela vous donne une figure précise pour le prochain redémarrage et permet à NTP de se synchroniser plus rapidement.

Utilisez la commande no ntp clock-period lorsque vous enregistrez la configuration pour l'utiliser sur un autre périphérique, car cette commande permet de rétablir la valeur par défaut de la période d'horloge de ce périphérique particulier. Vous pouvez recalculer la valeur vraie (mais vous pouvez réduire la précision de l'horloge système pendant cette période de recalcul).

N'oubliez pas que cette valeur dépend du matériel. Par conséquent, si vous copiez une configuration et que vous l'utilisez sur différents périphériques, vous risquez de provoquer des problèmes. Cisco prévoit de remplacer NTP version 3 par la version 4 afin de résoudre ce problème.

Si vous n'êtes pas au courant de ces problèmes, vous pouvez décider de modifier manuellement cette valeur. Afin de migrer d'un périphérique à un autre, vous pouvez décider de copier l'ancienne configuration et de la coller sur le nouveau périphérique. Malheureusement, comme la commande ntp clock-period apparaît dans les commandes running-config et startup-config, la période d'horloge NTP est collée sur le nouveau périphérique. Dans ce cas, le protocole NTP sur le nouveau client se désynchronise toujours du serveur avec une valeur de dispersion d'homologue élevée.

À la place, effacez la période d'horloge NTP avec la commande no ntp clock-period, puis enregistrez la configuration. Le routeur calcule finalement une période d'horloge appropriée pour lui-même.

La commande ntp clock-period n'est plus disponible dans la version 15.0 ou ultérieure du logiciel Cisco IOS ; l'analyseur rejette maintenant la commande avec l'erreur :

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

Vous n'êtes pas autorisé à configurer manuellement la période d'horloge et la période d'horloge n'est pas autorisée dans la configuration en cours. Puisque l'analyseur rejette la commande si elle était dans la configuration de démarrage (dans les versions antérieures de Cisco IOS telles que 12.4), l'analyseur rejette la commande lorsqu'il copie la configuration de démarrage dans la configuration en cours au démarrage.

La nouvelle commande de remplacement est ntp clear drift.

Informations connexes

- Support Forum Thread : période d'horloge NTP non configurée
- Livre blanc sur le protocole NTP (Network Time Protocol)
- Dépannage du protocole NTP (Network Time Protocol)
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.