

Questions de Protocole NTP (Network Time Protocol) dépannant et déboguant le guide

Contenu

[Introduction](#)

[Commandes show de NTP](#)

[association de show ntp](#)

[détail d'association de show ntp](#)

[show ntp status](#)

[Dépannage du NTP avec des débogages](#)

[Paquets de NTP non reçus](#)

[Paquets de NTP non traités](#)

[Perte de synchronisation](#)

[validité de debug ntp](#)

[paquets de debug ntp](#)

[sync de debug ntp et événements de debug ntp](#)

[Ntp clock-period manuellement réglé](#)

[Informations connexes](#)

Introduction

Ce document décrit l'utilisation des débogages afin de dépanner des questions de Protocole NTP (Network Time Protocol), aussi bien que la sortie du **show ntp** principal commande.

Commandes show de NTP

Avant que vous regardiez la cause des problèmes de NTP, vous devriez comprendre l'utilisation de et la sortie de ces commandes :

- **association de show ntp**
- **détail d'association de show ntp**
- **show ntp status**

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Remarque: L'[Outil d'interprétation de sortie](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes d'affichage**. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

association de show ntp

Une association de NTP peut être une association de pair (un système est disposé à synchroniser à l'autre système ou à permettre à l'autre système pour synchroniser à lui) ou une association de serveur (seulement un système synchronise à l'autre système et pas à l'autre manière autour).

C'est un exemple de sortie de la commande d'association de show ntp :

```
CLA_PASA#sh ntp association
```

| address | ref clock | st | when | poll | reach | delay | offset | disp |
|----------------|---------------|----|-------|------|-------|-------|--------|--------|
| ~127.127.7.1 | 127.127.7.1 | 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 | 86.79.127.250 | 4 | 7 | 256 | 377 | 0.8 | -0.29 | 0.2 |
| *~10.50.36.42 | 86.79.127.250 | 4 | 188 | 256 | 377 | 0.7 | -0.17 | 0.3 |
| +~10.50.38.50 | 86.79.127.250 | 4 | 42 | 256 | 377 | 0.9 | 1.02 | 0.4 |
| +~10.50.36.50 | 86.79.127.250 | 4 | 20 | 256 | 377 | 0.7 | 0.87 | 0.5 |

* master (synced), # master (unsynced), + selected, - candidate, ~ configured

Terme Explication

Les caractères avant l'adresse ont ces définitions :

* Synchronisé à ce pair

presque synchronisé à ce pair

+ pair sélectionné pour la synchronisation possible

- Le pair est un candidat pour la sélection

| le pair est statiquement configuré

adresse C'est l'adresse IP du pair. Dans l'exemple, la première entrée affiche 127.127.7.1. Ceci indique que l'ordinateur local sync'd avec lui-même.

Généralement, seulement sync'd de ntp master avec lui-même.

horloge C'est l'adresse de l'horloge de référence pour le pair. Dans l'exemple, les six premiers pairs/serveurs ont un IP privé comme horloge de référence, ainsi leurs maîtres sont probablement des Routeurs, des Commutateurs, ou des serveurs dans le réseau local. Pour les quatre dernières entrées, l'horloge de référence est un IP de public, ainsi leurs maîtres sont probablement une source temporelle publique.

St Le NTP emploie le concept d'une strate afin de décrire à quelle distance loin (en sauts de NTP) un ordinateur est d'une source temporelle bien fondée. Par exemple, un Serveur de synchronisation de la strate 1 a une radio ou une horloge atomique directement reliée à elle. Il envoie son temps à un Serveur de synchronisation de strate 2 par le NTP, et ainsi de suite jusqu'à la strate 16. Un NTP courant d'ordinateur choisit automatiquement l'ordinateur avec le plus bas nombre de strate avec lequel il peut communiquer et utilise le NTP en tant que sa source temporelle.

quand Le temps puisque le dernier paquet de NTP a été reçu d'un pair est signalé en quelques secondes. Cette valeur devrait être inférieure à l'intervalle de sondage.

balayage L'intervalle de sondage est signalé en quelques secondes. D'intervalle les débuts habituellement avec un minimum d'intervalles entre deux invitations à émettre 64-second. Le RFC spécifie que pas plus d'une transaction de NTP par minute est nécessaire afin de synchroniser deux ordinateurs. Pendant que le NTP devient stable entre un client et un serveur, l'intervalle entre deux

invitations à émettre peut augmenter dans les petits pas de 64 secondes jusqu'à 1024 secondes et stabilise généralement quelque part dans l'intervalle. Mais, cette valeur change dynamiquement, basé sur le réseau conditionne entre le client et le serveur et la perte de paquets de NTP. Si un serveur est inaccessible pendant quelque temps, l'intervalle entre deux invitations à émettre est grimpé dans les étapes jusqu'à 1024 secondes afin de réduire le temps système de réseau.

Il n'est pas possible d'ajuster l'intervalle entre deux invitations à émettre de NTP sur un routeur, parce que l'intervalle est déterminé par les algorithmes heuristiques.

portée L'accessibilité de pair est une chaîne binaire signalée comme valeur octale. Ce champ affiche si les huit derniers paquets ont été reçus par le processus de NTP sur le logiciel de Cisco IOS®. Les paquets doivent être reçus, traités, et reçus comme valides par le processus de NTP et pas simplement par le routeur ou le commutateur qui reçoit les paquets IP de NTP.

La portée emploie l'intervalle entre deux invitations à émettre pour une minuterie afin de décider si un paquet a été reçu ou pas. L'intervalle entre deux invitations à émettre est le temps que le NTP attend avant qu'il conclue qu'un paquet a été perdu. Le temps de balayage peut être différent pour différents pairs, ainsi le temps avant que la portée décide qu'un paquet a été perdu peut également être différent pour différents pairs.

Dans l'exemple, il y a quatre valeurs différentes de portée :

- la binaire 377 = 11111111 octale, qui indique le processus de NTP a reçu les huit derniers paquets.
- 0 = 00000000 octaux, qui indique le processus de NTP n'ont reçu aucun paquet.
- 1 = 00000001 octaux, qui indique le processus de NTP ont reçu seulement le dernier paquet.
- 357 = 11101111 octaux, qui indique le paquet avant que les derniers quatre paquets aient été perdus.

La portée est un bon indicateur de si des paquets de NTP sont lâchés en raison d'un lien pauvre, CPU émet et d'autres problèmes intermittents.

[Conversion octale < - > la binaire](#) est un convertisseur en ligne d'unité pour ceci et beaucoup d'autres conversions.

retard Le délai d'aller-retour à scruter est signalé en quelques millisecondes. Afin de régler l'horloge plus exactement, ce retard est pris en considération quand le temps d'horloge est placé.

décalage Le décalage est la différence de temps d'horloge entre les pairs ou entre le maître et le client. Cette valeur est la correction qui est appliquée à une horloge de client afin de la synchroniser. Une valeur positive indique que l'horloge de serveur est plus élevée. Une valeur négative indique que l'horloge de client est plus élevée.

DISP La dispersion, signalée en quelques secondes, est la différence de temps maximum d'horloge qui a été jamais observée entre l'horloge locale et l'horloge de serveur. Dans l'exemple, la dispersion est 0.3 pour le serveur 10.50.36.42, ainsi la différence de temps maximum jamais observée localement entre l'horloge locale et l'horloge de serveur est de 0.3 seconde.

Vous pouvez compter voir une valeur élevée quand les horloges syncing au commencement. Mais, si la dispersion est trop élevée à d'autres fois, le processus de NTP sur le client ne reçoit pas des messages de NTP du serveur. La dispersion maximum est 16000 ; dans l'exemple, c'est la dispersion pour des serveurs 10.50.44.69 et 10.50.44.133, ainsi le client local ne reçoit pas le temps

de ces serveurs.

Si la portée est zéro et la dispersion est très élevée, le client ne reçoit probablement pas des messages de ce serveur. Référez-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.
```

Quoique le décalage soit juste -4.26, la dispersion est très élevée (peut-être en raison d'a après l'événement), et la portée est zéro, ainsi ce client ne reçoit pas le temps de ce serveur.

détail d'association de show ntp

C'est un exemple de sortie de la commande de **détail d'association de show ntp** :

```
Router#sho ntp assoc detail
10.4.2.254 configured, our_master, 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
```

Des termes déjà définis dans la [section d'association de show ntp](#) ne sont pas répétés.

| Terme | Explication | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------|---|---|---------------|--------------------|---|------|----------------------|---|------|---------------------|---|------|--------------------------|---|------|---|---|------|-------------------------------------|---|------|---|---|------|-------------------------------|---|------|---|
| configuré | Ce clock source de NTP a été configuré pour être un serveur. Cette valeur peut également être dynamique, où le pair/serveur a été dynamiquement découvert. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| our_master | Le client local est synchronisé à ce pair. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| sélectionné | Le pair/serveur est sélectionné pour la synchronisation possible, quand le « our_master » échoue ou le client perd le sync. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| raisonnable | Des tests de validité sont utilisés afin de tester le paquet de NTP reçu d'un serveur. Ces tests sont spécifiés dans RFC 1305, Network Time Protocol (spécification, implémentation et analyse de version 3) . Les tests sont : | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <table border="0"> <thead> <tr> <th>Test</th> <th>Masque</th> <th>Explication</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0x01</td> <td>Paquet dupliqué reçu</td> </tr> <tr> <td>2</td> <td>0x02</td> <td>Paquet factice reçu</td> </tr> <tr> <td>3</td> <td>0x04</td> <td>Protocol non synchronisé</td> </tr> <tr> <td>4</td> <td>0x08</td> <td>Le retard/dispersion de pair a manqué contrôle de borne</td> </tr> <tr> <td>5</td> <td>0x10</td> <td>Échec de l'authentification de pair</td> </tr> <tr> <td>6</td> <td>0x20</td> <td>Horloge de pair non synchronisée (commun pour le serveur unsynched)</td> </tr> <tr> <td>7</td> <td>0x40</td> <td>Strate de pair hors de limite</td> </tr> <tr> <td>8</td> <td>0x80</td> <td>Le retard/dispersion de racine a manqué contrôle de borne</td> </tr> </tbody> </table> <p>Les données de paquets sont valides si les tests 1 4 sont passés. Les données sont alors utilisées afin de calculer le décalage, le retard, et la dispersion.</p> <p>L'en-tête de paquet est valide si les tests 5 8 sont passés. Seulement des paquets avec une en-tête valide peuvent être utilisés pour déterminer si un pair peut être sélectionné pour la synchronisation.</p> | Test | Masque | Explication | 1 | 0x01 | Paquet dupliqué reçu | 2 | 0x02 | Paquet factice reçu | 3 | 0x04 | Protocol non synchronisé | 4 | 0x08 | Le retard/dispersion de pair a manqué contrôle de borne | 5 | 0x10 | Échec de l'authentification de pair | 6 | 0x20 | Horloge de pair non synchronisée (commun pour le serveur unsynched) | 7 | 0x40 | Strate de pair hors de limite | 8 | 0x80 | Le retard/dispersion de racine a manqué contrôle de borne |
| Test | Masque | Explication | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 0x01 | Paquet dupliqué reçu | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 0x02 | Paquet factice reçu | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 0x04 | Protocol non synchronisé | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 0x08 | Le retard/dispersion de pair a manqué contrôle de borne | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | 0x10 | Échec de l'authentification de pair | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | 0x20 | Horloge de pair non synchronisée (commun pour le serveur unsynched) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | 0x40 | Strate de pair hors de limite | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 0x80 | Le retard/dispersion de racine a manqué contrôle de borne | | | | | | | | | | | | | | | | | | | | | | | | | | |
| aliéné | Les contrôles de validité ont manqué, ainsi le temps du serveur n'est pas reçu. Le serveur unsynched. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| valide | Le temps de pair/serveur est valide. Le client local reçoit cette fois si ce pair devient le maître. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| non valide | Le temps de pair/serveur est non valide, et le temps ne sera pas reçu. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ID | Chaque pair/serveur est assigné un ID de référence (étiquette). | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| référence | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| temps | Le temps est le dernier groupe date/heure reçu de ces pair/serveur. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| notre mode | C'est l'état du client/du pair locaux. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| de pair de | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| mode | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| notre intvl | C'est l'intervalle entre deux invitations à émettre de notre balayage à ce | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| de | pair ou du pair à l'ordinateur local. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| balayage | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| de pair du | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| balayage | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| intvl/ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| retard de | Le retard de racine est le retard en quelques millisecondes à la racine de | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| racine | l'installation de NTP. Des horloges de la strate 1 sont considérées à la racine d'un NTP installé/conception. Dans l'exemple, chacun des trois serveurs peut être la racine parce qu'ils sont à la strate 1. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dispersion | La dispersion de racine est la différence de temps maximum d'horloge qui a | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| de racine | été jamais observée entre l'horloge locale et l'horloge de racine. Référez-vous à l'explication de la « DISP » sous la section d'association de show ntp pour plus de détails. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| dist de | C'est une évaluation de la différence maximum entre le moment sur la | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| sync. | source de la strate 0 et le moment mesuré par le client ; il se compose des | | | | | | | | | | | | | | | | | | | | | | | | | | | |

composants pour la durée d'aller-retour, la précision de système, et la dérive d'horloge puisque le dernier effectif a lu de la source de strate. Dans un grand NTP installé (des serveurs de NTP à strate 1 dans l'Internet, avec les serveurs qui temps de source à différentes strates) avec des serveurs/clients à de plusieurs strates, la topologie de synchronisation de NTP devrait être organisée afin de produire le de grande précision, mais doit ne jamais être laissée former une boucle de synchronisation horaire. Un facteur supplémentaire est que chaque incrément dans la strate fait participer un Serveur de synchronisation potentiellement peu fiable, qui introduit des erreurs de mesure supplémentaires. L'algorithme de sélection utilisé dans le NTP utilise une variante du Bellman-Ford distribué conduisant l'algorithme afin de calculer les spannings-tree de minimum-poids enracinés sur les serveurs primaires. La mesure de distance utilisée par l'algorithme comprend la strate plus la distance de synchronisation, qu'elle-même comprend la dispersion plus un demi- de retard absolu. Ainsi, le chemin de synchronisation porte toujours le nombre minimal de serveurs à la racine ; des liens sont résolus sur la base de l'erreur maximum.

retard C'est le délai d'aller-retour à scruter.
précision C'est la précision de l'horloge de pair dans l'hertz.
version C'est le numéro de version de NTP utilisé par le pair.
temps C'est le groupe date/heure du créateur de paquet de NTP ; en d'autres
d'org termes, c'est le groupe date/heure de ce pair quand il a créé le paquet de NTP mais avant qu'il a envoyé le paquet au client local.
temps C'est le groupe date/heure quand le client local a reçu le message. La
récepteur différence entre le moment d'org et le moment récepteur est le décalage pour ce pair. Dans l'exemple, 10.4.2.254 principal a ces périodes :

```
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 est le décalage de 268.3044 millisecondes.

temps de C'est le groupe date/heure de transmission pour le paquet de NTP que le
xmt client local envoie à ces pair/serveur.
filtdelay C'est le délai d'aller-retour en quelques millisecondes de chaque
filtoffset échantillon.
filterror C'est le décalage d'horloge en quelques millisecondes de chaque
échantillon.
C'est l'erreur approximative de chaque échantillon.
Un échantillon est le dernier paquet de NTP reçu. Dans l'exemple, 10.4.2.254 principal a ces valeurs :

```
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 de portée, qui affiche si le client local a reçu les huit derniers paquets de NTP.

show ntp status

C'est un exemple de sortie de la commande de **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
```

Des termes déjà définis dans la [section d'association de show ntp](#) ou la [section de détails d'association de show ntp](#) ne sont pas répétés.

Terme Explication

précision La précision est déterminée automatiquement et est mesurée comme unité de deux. Dans l'exemple, 2**18 signifie $2^{(-18)}$, ou 3.8 microsecondes. La perte de synchronisation entre les pairs de NTP ou entre un maître et un client peut être due à un grand choix de causes. Le NTP évite la synchronisation avec un ordinateur dont le temps pourrait être ambigu de ces manières :

1. Le NTP ne synchronise jamais à un ordinateur qui n'est pas synchronisé.
2. Le NTP compare le temps qui est signalé par plusieurs ordinateurs et ne synchronise pas à un ordinateur dont le temps est sensiblement différent des autres, même si sa strate est inférieure.

Dépannage du NTP avec des débogages

Certaines des la plupart des causes classiques des questions de NTP sont :

- Des paquets de NTP ne sont pas reçus.
- Des paquets de NTP sont reçus, mais ne sont pas traités par le processus de NTP sur l'IOS.
- Des paquets de NTP sont traités, mais les facteurs erronés ou les données de paquets entraîne la perte de synchronisation.
- Le ntp clock-period est manuellement placé.

Importantes commandes de débogage qu'isolat d'aide que la cause de ces questions incluent :

- **<acl> de paquets d'IP de débogage**
- **paquets de debug ntp**
- **validité de debug ntp**
- **sync de debug ntp**
- **événements de debug ntp**

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

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Remarque: Référez-vous à la section [Informations importantes sur les commandes Debug](#) avant d'utiliser les commandes [debug](#).

Paquets de NTP non reçus

Employez la commande de **debug ip packet** afin de vérifier si des paquets de NTP sont reçus et envoyés. Puisque la sortie de débogage peut être bavarde, vous pouvez limiter la sortie de débogage avec l'utilisation du Listes de contrôle d'accès (ACL). Port 123 de Protocole UDP (User Datagram Protocol) d'utilisations de NTP.

1. Créez l'ACL 101 :

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

Les paquets de NTP ont habituellement une source et une destination port de 123, ainsi ceci aide :

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

2. Employez cet ACL afin de limiter la sortie de la commande de **debug ip packet** :

```
debug ip packet 101
```

3. Si la question est avec les pairs particuliers, rétrécissez l'ACL 101 vers le bas à ces pairs. Si le pair est 172.16.1.1, changez l'ACL 101 à :

```
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 sortie indique que des 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 feature
241926: Apr 23 2012 15:46:26.101 ETE:      UDP src=123, dst=123, Ingress-NetFlow(13), rtype 0,
forus FALSE, 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 feature
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 confirmez que des paquets de NTP ne sont pas reçus, vous devriez :

- Vérifiez si le NTP est configuré correctement.
- Vérifiez si un ACL bloque des paquets de NTP.
- Vérifiez les questions de routage à l'IP de source ou de destination.

Paquets de NTP non traités

Les deux **debug ip packet** et commandes de **paquets de debug ntp** étant activé, vous pouvez voir les paquets qui sont reçus et transmis, et vous pouvez voir que le NTP agit sur ces paquets. Pour chaque paquet de NTP reçu (comme affiché par **debug ip packet**), il y a une entrée de correspondance générée par des **paquets de debug ntp**.

C'est la sortie de débogage quand les travaux par processus de NTP 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 (71.80.83.0)
.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 (71.80.83.0)
.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)
```

C'est un exemple où le NTP ne travaille pas aux paquets reçus. Bien que des paquets de NTP soient reçus (comme affiché par des **paquets d'IP de débogage**), le processus de NTP n'agit pas sur eux. Pour les paquets de NTP qui sont envoyés, un résultat correspondant de **paquets de debug ntp** est présent, parce que le processus de NTP doit générer le paquet. La question est spécifique aux paquets reçus de NTP 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 feature
071572: Apr 23 2012 15:47:31.497 ETE: UDP src=123, dst=123, Ingress-NetFlow(13), rtype 0,
```

```

forus FALSE, 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 feature
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 dst 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 pak 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 feature
071590: Apr 23 2012 16:04:35.506 ETE:      UDP src=123, dst=123, Ingress-NetFlow(13), rtype 0,
forus FALSE, 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 feature
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 dst 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 pak for forus packet
071599: Apr 23 2012 16:04:35.506 ETE:      UDP src=123, dst=123
PCY_PAS1#

```

Perte de synchronisation

La perte de synchronisation pourrait se produire si la valeur de dispersion et/ou de retard pour un serveur disparaît très élevée. Les valeurs élevées indiquent que les paquets prennent trop long pour arriver au client du serveur/du pair en référence à la racine de l'horloge. Ainsi, l'ordinateur local ne peut pas faire confiance à la précision du temps actuel dans le paquet, parce qu'il ne sait pas combien de temps il a pris pour que le paquet obtienne ici.

Le NTP est méticuleux au sujet du temps et ne synchronisera pas avec un autre périphérique qu'il ne peut pas faire confiance ou ne peut pas s'ajuster d'une manière de sorte qu'il puisse soient de confiance.

S'il y a un lien saturé et la mise en mémoire tampon se produit le long de la route, les paquets

obtiennent retardé comme ils sont livré au NTP le client. Ainsi, l'horodateur contenu dans un paquet ultérieur de NTP peut de temps en temps varier beaucoup, et le client local ne peut pas vraiment s'ajuster pour cette variance.

Le NTP n'offre pas une méthode pour arrêter la validation de ces paquets à moins que vous utilisiez SNTP (protocole de diffusion du temps en réseau (SNTP)). SNTP peut ne pas être beaucoup d'une alternative parce qu'il n'est pas largement pris en charge en logiciel.

Si vous éprouvez la perte de synchronisation, vous devriez vérifier les liens :

- Sont-ils saturés ?
- Y a il n'importe quels genres de baisses dans vos liens de réseau d'étendu (WAN)
- Le cryptage se produit-il ?

Surveillez la valeur de portée de la commande de **détail de show ntp associations**. La valeur la plus élevée est 377. Si la valeur est 0 ou bas, des paquets de NTP sont reçus par intermittence, et le client local sort du sync avec le serveur.

validité de debug ntp

La commande de **validité de debug ntp** indique si le paquet de NTP a manqué des contrôles de validité ou de validité et indique la raison pour la panne. Comparez cette sortie aux tests de validité spécifiés dans RFC1305 qui sont utilisés afin de tester le paquet de NTP reçu d'un serveur. Huit tests sont définis :

Test Masque Explication

| | | |
|---|------|---|
| 1 | 0x01 | Paquet dupliqué reçu |
| 2 | 0x02 | Paquet factice reçu |
| 3 | 0x04 | Protocol non synchronisé |
| 4 | 0x08 | Le retard/dispersion de pair a manqué contrôle de borne |
| 5 | 0x10 | Échec de l'authentification de pair |
| 6 | 0x20 | Horloge de pair non synchronisée (commun pour le serveur unsynched) |
| 7 | 0x40 | Strate de pair hors de limite |
| 8 | 0x80 | Le retard/dispersion de racine a manqué contrôle de borne |

C'est sortie témoin de la commande de **validité de debug ntp** :

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

```
009585: Mar 1 2012 09:14:32.670 HIVER: NTP: packet from 192.196.113.57 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 163.110.103.27 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 192.196.113.57 failed 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 163.110.103.35 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 163.110.103.27 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 192.196.113.137 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 163.83.23.140 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 192.196.113.92 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

```

paquets de debug ntp

Vous pouvez utiliser les **paquets de debug ntp** commandez afin de voir le temps que le pair/serveur te donne dans le paquet reçu. L'ordinateur local de temps indique également le temps où il sait au pair/au serveur dans le paquet transmis.

Champ paquet récepteur

org Groupe date/heure de créateur, qui est le temps de serveur.

REC Groupe date/heure sur le client quand il a reçu le paquet.

paquet de xmit

Groupe date/heure de créateur (client) quand il a envoyé le paquet. (Le client lance un paquet au serveur.)

Dans cette sortie témoin, les groupes date/heure dans le paquet reçu du serveur et le paquet envoyé à un autre serveur sont identiques, qui indiquent que le NTP de client est dans le sync.

```

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 (71.80.83.0)
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)
```

C'est un exemple de sortie quand les horloges ne sont pas dans le sync. Notez la différence de temps entre le paquet de xmit et le paquet récepteur. La dispersion de pair sera à la valeur maximum de 16000, et la portée pour le pair affichera 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 (71.80.83.0)
.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)
```

sync de debug ntp et événements de debug ntp

La commande de **sync de debug ntp** produit les sorties d'un-line qui affichent si l'horloge synced ou le sync a changé. La commande est généralement activée avec des **événements de debug ntp**.

Les événements de debug ntp commandent des expositions tous les événements de NTP qui se produisent, qui vous aide à déterminer si un changement du NTP déclençait une question telle que l'extinction d'horloges du sync. (En d'autres termes, si vos horloges heureusement synced deviennent folles soudainement, vous savez pour rechercher une modification ou un déclencheur !)

C'est un exemple des deux débogages. Au commencement, les horloges de client synced. La commande d'**événements de debug ntp** prouve qu'une modification de strate de ntp peer s'est produite, et les horloges puis sont sorties du sync.

```
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 (71.80.83.0)
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 manuellement réglé

Le site Web cisco.com avertit cela :

« La commande de **ntp clock-period** est automatiquement générée de refléter le facteur de correction constamment changeant quand la commande de **startup-configuration de configuration courante de copie** est sélectionnée de sauvegarder la configuration à NVRAM. Ne tentez pas d'utiliser manuellement la commande de **ntp clock-period**. Assurez-vous que vous retirez cette ligne de commande en copiant des fichiers de configuration sur d'autres périphériques. »

La valeur de horloge-période dépend du matériel, ainsi elle diffère pour chaque périphérique.

La commande de **ntp clock-period** apparaît automatiquement dans la configuration quand vous activez le NTP. La commande est utilisée afin d'ajuster l'horloge de logiciel. La « valeur de réglage » compense l'intervalle de coulis 4 millisecondes, de sorte que, avec le réglage mineur, vous ayez 1 seconde à la fin de l'intervalle.

Si le périphérique a calculé que son horloge système est perdante le temps (peut-être il faut une compensation de fréquence du niveau de base du routeur), il ajoute automatiquement cette valeur à l'horloge système afin de mettre à jour son synchronicity.

Remarque: Cette commande ne devrait pas être changée par l'utilisateur.

Le ntp clock-period par défaut pour un routeur est 17179869 et est essentiellement utilisé afin de commencer le processus de NTP.

La formule de conversion est de $17179869 * 2^{(-32)} = 0.00399999995715916156768798828125$, ou approximativement 4 millisecondes.

Par exemple, l'horloge système pour Cisco 2611 Routeurs (un des Routeurs de gamme Cisco 2600) s'est avérée légèrement -de-sync et pourrait être resynchronisée avec cette commande :

```
ntp clock-period 17208078
```

Ceci égale $17208078 * 2^{(-32)} = 0.0040065678767859935760498046875$, ou un peu plus de 4 millisecondes.

Cisco recommande que vous permettiez le routeur de s'exécuter pendant une semaine ou ainsi en états normaux de réseau et puis d'employer la commande de **mem de wr** afin de sauvegarder la valeur. Ceci te donne une figure précise pour la prochaine réinitialisation et permet au NTP pour synchroniser plus rapidement.

N'utilisez l'**aucune** commande de **ntp clock-period** quand vous sauvegardez la configuration pour l'usage sur un autre périphérique parce que cette commande relâche la horloge-période de nouveau au par défaut de ce périphérique particulier. La valeur vrai sera recalculée (mais réduira la précision de l'horloge système au cours de ce délai prévu de recalcul).

Souvenez-vous que cette valeur est personne à charge de matériel, ainsi si vous copiez une configuration et l'utilisez sur des différents périphériques, vous pouvez poser des problèmes. Cisco prévoit de remplacer la version 3 de NTP par la version 4 afin de résoudre ce problème.

Si vous ne vous rendez pas compte de ces questions, vous pouvez décider de bricoler manuellement avec cette valeur. Afin de migrer d'un périphérique à l'autre, vous pouvez décider de copier la configuration ancienne et de la coller sur le nouveau périphérique. Malheureusement, parce que la commande de **ntp clock-period** apparaît dans le running-config et le startup-config, le ntp clock-period est collé sur le nouveau périphérique. Quand ceci se produit, le NTP sur le nouveau client sort toujours du sync avec le serveur avec une valeur élevée de dispersion de pair.

Au lieu de cela, effacez le ntp clock-period avec l'**aucune** commande de **ntp clock-period**, puis sauvegardez la configuration. Le routeur calcule par la suite une horloge-période appropriée pour elle-même.

La commande de **ntp clock-period** n'est plus disponible dans la version de logiciel 15.0 de Cisco IOS ou plus tard ; le programme d'analyse syntaxique rejette maintenant la commande avec l'erreur :

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

Ainsi, vous n'êtes pas permis pour configurer la horloge-période manuellement, et la horloge-période n'est pas donnée dans le running-config. Puisque le programme d'analyse syntaxique rejette la commande si elle était dans le config de démarrage (dans des versions plus tôt de Cisco IOS telles que 12.4), le programme d'analyse syntaxique rejette la commande quand il copie le config de démarrage sur le running-config sur l'amorce.

Le nouveau, commande de remplacement est **dérive de ntp clear**.

[Informations connexes](#)

- [Fil du forum de support : Ntp clock-period n'étant pas configuré](#)
- [Protocole d'Heure Réseau : Livre blanc sur les pratiques recommandées](#)
- [Dépannage du protocole NTP \(Network Time Protocol\)](#)
- [Support et documentation techniques - Cisco Systems](#)