Fehlerbehebung und Fehlerbehebung bei NTP-Problemen (Network Time Protocol)

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei NTP-Problemen (Network Time Protocol) mit debug Befehlen und dem show ntp Befehl beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

NTP-Befehle anzeigen

Bevor Sie sich die Ursache von NTP-Problemen ansehen, müssen Sie mit der Verwendung und Ausgabe der folgenden Befehle vertraut sein:

- NTP-Zuordnung anzeigen
- NTP-Zuordnungsdetail anzeigen
- NTP-Status anzeigen

Hinweis: Verwenden Sie das Tool zur Befehlssuche, um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen zugreifen.

Hinweis: Das Tool "Output Interpreter" unterstützt bestimmte Befehle zum Anzeigen. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der show-Befehlsausgabe anzuzeigen. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen zugreifen.

NTP-Zuordnung anzeigen

Eine NTP-Zuordnung kann eine Peer-Zuordnung (ein System ist bereit, eine Synchronisierung mit dem anderen System durchzuführen oder eine Synchronisierung mit dem anderen System zuzulassen) oder eine Server-Zuordnung (nur ein System führt eine Synchronisierung mit dem anderen System durch, nicht umgekehrt) sein.

Dies ist ein Beispiel für die Ausgabe des Befehls 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
```

Begriff	Erläuterung
	Zeichen vor der Adresse haben folgende Definitionen: * Mit diesem Peer synchronisiert # Fast mit diesem Peer synchronisiert + Peer für mögliche Synchronisierung ausgewählt - Peer ist ein Kandidat für die Auswahl ~ Peer ist statisch konfiguriert
adresse	Dies ist die IP-Adresse des Peers. Im Beispiel wird im ersten Eintrag 127.127.7.1 angezeigt. Dies zeigt an, dass der lokale Computer mit sich selbst synchronisiert hat. Im Allgemeinen wird nur ein primäres NTP mit sich selbst synchronisiert.
Referenzuhr	Dies ist die Adresse der Referenzuhr für den Peer. Im Beispiel haben die ersten sechs Peers/Server eine private IP als Referenzuhr, sodass ihre primären Geräte wahrscheinlich Router, Switches oder Server im lokalen Netzwerk sind. Bei den letzten vier Einträgen ist die Referenzuhr eine öffentliche IP-Adresse, daher sind ihre Primardaten wahrscheinlich eine öffentliche Zeitquelle.
st	Das NTP nutzt das Schichtenkonzept, um zu beschreiben, wie weit (in NTP-Hops) ein Rechner von einer maßgeblichen Zeitquelle entfernt ist. Beispielsweise ist ein Schicht-1-Zeitserver direkt mit einer Funk- oder Atomuhr verbunden. Es sendet seine Zeit über NTP an einen Schicht-2-Zeitserver usw. bis Schicht 16. Ein Computer, der NTP ausführt, wählt automatisch den Computer mit der niedrigsten Schicht-Nummer aus, mit dem er kommunizieren kann, und verwendet NTP als Zeitquelle.
Wann	Die Zeit seit dem Empfang des letzten NTP-Pakets von einem Peer wird in Sekunden gemeldet. Dieser Wert muss kleiner als das Abfrageintervall sein.
Umfrage	Das Abfrageintervall wird in Sekunden gemeldet. Das Intervall beginnt in der Regel mit einem Abfrageintervall von mindestens 64 Sekunden. Die RFC gibt an, dass maximal eine NTP-Transaktion pro Minute erforderlich ist, um zwei Computer zu synchronisieren. Wenn das NTP zwischen einem Client und einem Server stabil wird, kann sich das Abfrageintervall in kleinen Schritten von 64 Sekunden auf 1024 Sekunden erhöhen und stabilisiert sich im Allgemeinen irgendwo dazwischen. Dieser Wert ändert sich jedoch dynamisch, basierend auf den Netzwerkbedingungen zwischen Client und Server und dem Verlust von NTP-

	Paketen. Wenn ein Server für einige Zeit nicht erreichbar ist, wird das Abfrageintervall schrittweise auf 1024 Sekunden erhöht, um den Netzwerk-Overhead zu reduzieren. Es ist nicht möglich, das NTP-Abfrageintervall auf einem Router anzupassen, da das interne Intervall von heuristischen Algorithmen bestimmt wird.
erreichen	Die Peer-Erreichbarkeit ist eine Bitzeichenfolge, die als Oktalwert gemeldet wird. Dieses Feld gibt an, ob die letzten acht Pakete vom NTP-Prozess der Cisco IOS®-Software empfangen wurden. Die Pakete müssen vom NTP-Prozess und nicht nur vom Router oder Switch, der die NTP-IP-Pakete empfängt, empfangen, verarbeitet und als gültig akzeptiert werden. Reach verwendet das Abfrageintervall für eine Zeitüberschreitung, um zu entscheiden, ob ein Paket empfangen wurde oder nicht. Das Abfrageintervall ist die Zeit, die das NTP wartet, bevor es den Verlust eines Pakets feststellt. Die Abfragezeit kann für verschiedene Peers unterschiedlich sein. Daher kann die Zeit vor der Reichweite, die entscheidet, dass ein Paket verloren geht, auch für verschiedene Peers unterschiedlich sein. Im Beispiel gibt es vier verschiedene Reichweitenwerte: • 377 octal = 11111111 binary; gibt an, dass der NTP-Prozess die letzten acht Pakete empfangen hat. • 0 octal = 00000000, was bedeutet, dass der NTP-Prozess kein Paket empfangen hat. • 1 Oktal = 00000001, was bedeutet, dass der NTP-Prozess nur das letzte Paket empfangen hat. • 357 Oktal = 11101111, was bedeutet, dass das Paket vor dem Verlust der letzten vier Pakete gesendet wurde. "Reach" ist ein guter Indikator dafür, ob NTP-Pakete aufgrund einer schlechten Verbindung, CPU-Problemen und anderen zeitweiligen Problemen verworfen werden. Unit Converter ist ein Online-Konverter für diese und viele andere Konvertierungen.
verzögerung	Die Round-Trip-Verzögerung zum Peer wird in Millisekunden gemeldet. Um den Takt genauer einzustellen, wird diese Verzögerung bei der Einstellung der Taktzeit berücksichtigt.
Offset	Offset ist die Zeitdifferenz zwischen den Peers oder zwischen dem primären und dem Client. Dieser Wert ist die Korrektur, die auf eine Client-Uhr angewendet wird, um diese zu synchronisieren. Ein positiver Wert zeigt an, dass die Serveruhr höher ist. Ein negativer Wert zeigt an, dass die Client-Uhr höher ist.

verderben	Die Dispersion (in Sekunden) ist die maximale Zeitdifferenz, die je zwischen der lokalen Uhr und der Serveruhr gemessen wurde. Im Beispiel beträgt die Dispersion 0,3 für den Server 10.50.36.42, sodass die maximale Zeitdifferenz, die je lokal zwischen der lokalen Uhr und der Serveruhr beobachtet wurde, 0,3 Sekunden beträgt. Sie können davon ausgehen, dass ein hoher Wert angezeigt wird, wenn die Uhren zu Beginn synchronisiert werden. Wenn die Dispersion jedoch zu anderen Zeiten zu hoch ist, akzeptiert der NTP-Prozess auf dem Client keine NTP-Nachrichten vom Server. Die maximale Dispersion beträgt 16000; im Beispiel ist dies die Dispersion für die Server 10.50.44.69 und 10.50.44.133, sodass der lokale Client keine Zeit von diesen Servern akzeptiert. Wenn die Reichweite Null ist und die Dispersion sehr hoch ist, akzeptiert der Client wahrscheinlich keine Nachrichten von diesem Server. Weitere Informationen finden Sie in der zweiten Zeile des Beispiels: 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. Obwohl der Offset nur -4,26 ist, ist die Dispersion sehr hoch (vielleicht aufgrund eines vergangenen Ereignisses), und die Reichweite ist Null, sodass dieser Client keine Zeit von diesem Server akzeptiert.

NTP-Zuordnungsdetail anzeigen

Dies ist ein Beispiel für die Ausgabe des Befehls 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
```

Begriffe, die bereits im Abschnitt "Zuordnung anzeigen" definiert wurden, werden hier nicht wiederholt.

Begriff	Erläuterung
konfiguriert	Diese NTP-Taktquelle wurde als Server konfiguriert. Dieser Wert kann auch dynamisch sein, wenn der Peer/Server dynamisch erkannt wurde.
unsere_primäre	Der lokale Client wird mit diesem Peer synchronisiert.
ausgewählt	Der Peer/Server wird für eine mögliche Synchronisierung ausgewählt, wenn 'our_primary' fehlschlägt oder der Client die Synchronisierung verliert.
gesund	Mit Integritätstests wird das von einem Server empfangene NTP-Paket getestet. Diese Tests sind in RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis spezifiziert. Die Tests sind:

Test	Maske	Erläuterung
1	0 x 01	Doppeltes Paket empfangen
2	0 x 02	Scheinpaket empfangen
3	0 x 04	Protokoll nicht synchronisiert
4	0 x 08	Überprüfung der Peer-Verzögerung/Dispersion fehlgeschlagen
5	0 x 10	Peer-Authentifizierung fehlgeschlagen
6	0 x 20	Peer-Uhr nicht synchronisiert (häufig für nicht synchronisierten Server)
7	0 x 40	Peerschicht außerhalb der Bindung
8	0 x 80	Überprüfung der Root-Verzögerung/Dispersion fehlgeschlagen

Die Paketdaten sind gültig, wenn die Tests 1 bis 4 bestanden wurden. Die Daten werden dann verwendet, um Offset, Verzögerung und Dispersion zu berechnen.

Der Paket-Header ist gültig, wenn die Tests 5 bis 8 bestanden wurden. Nur Pakete mit einem gültigen Header können verwendet werden, um zu bestimmen, ob ein Peer für die Synchronisierung ausgewählt werden kann.

geisteskrank	Die Plausibilitätsprüfungen sind fehlgeschlagen, daher wird keine Zeit vom Server akzeptiert. Der Server ist nicht synchronisiert.

gültig	Die Peer-/Serverzeit ist gültig. Der lokale Client akzeptiert diese Zeit, wenn dieser Peer zum primären Peer wird.
ungültig	Die Peer-/Serverzeit ist ungültig, und die Zeit kann nicht akzeptiert werden.
Referenz-ID	Jedem Peer/Server wird eine Referenz-ID (Label) zugewiesen.
Zeit	Zeit ist der letzte Zeitstempel, der von diesem Peer/Server empfangen wurde.
unser Modus/Peer-Modus	Dies ist der Status des lokalen Clients/Peers.
unsere Umfrage intvl/ peer poll intvl	Dies ist das Abfrageintervall von unserer Abfrage zu diesem Peer oder vom Peer zum lokalen Computer.
Wurzelverzögerung	Die Root-Verzögerung ist die Verzögerung in Millisekunden bis zum Root der NTP-Einrichtung. Stratum-1-Uhren gelten als die zugrunde liegenden Uhren bei einer NTP-Einrichtung/-Entwicklung. Im Beispiel können alle drei Server als Root fungieren, da sie sich in Schicht 1 befinden.
Wurzeldispersion	Die Root-Dispersion ist die maximale Zeitdifferenz zwischen der lokalen Uhr und der Root-Uhr, die je beobachtet wurde. Weitere Informationen finden Sie in der Erklärung von "disp" unter "show up association" (Zuordnung anzeigen).
Synchronisierungsdist.	Dies ist eine Schätzung der maximalen Differenz zwischen der Zeit auf der Schicht-0-Quelle und der vom Client gemessenen Zeit; sie besteht aus Komponenten für die Round-Trip-Zeit, die Systemgenauigkeit und die Uhrzeitdrift seit dem letzten tatsächlichen Auslesen der Schicht-Quelle. In einer großen NTP-Konfiguration (NTP-Server in Schicht 1 im Internet, mit Servern, die die Zeit auf verschiedenen Schichten beziehen) mit Servern/Clients in mehreren Schichten muss die NTP-Synchronisierungstopologie so organisiert sein, dass eine maximale Genauigkeit erreicht wird, es darf jedoch nie zugelassen werden, dass eine Zeitsynchronisierungsschleife gebildet wird. Ein weiterer Faktor ist, dass jedes Inkrement in der Schicht einen potenziell unzuverlässigen Zeitserver beinhaltet, was zusätzliche Messfehler mit sich bringt. Der im NTP verwendete Auswahlalgorithmus verwendet eine Variante des verteilten Routing-Algorithmus von Bellman-Ford, um die Spanning Trees mit der geringsten Gewichtung zu berechnen, die auf den primären Servern basieren. Die vom Algorithmus verwendete Entfernungsmetrik besteht aus der Schicht plus der Synchronisationsdistanz, die wiederum aus der Dispersion plus der Hälfte der absoluten Verzögerung besteht. Der Synchronisierungspfad führt also immer

	die minimale Anzahl von Servern zum Root; die Bindungen werden auf Basis des maximalen Fehlers aufgelöst.
verzögerung	Dies ist die Round-Trip-Verzögerung zum Peer.
Präzision	Dies ist die Genauigkeit der Peer-Uhr in Hz.
version	Dies ist die vom Peer verwendete NTP-Versionsnummer.
Organisationszeit	Dies ist der Zeitstempel des NTP-Paketentwicklers, d. h. der Peer-Zeitstempel, wenn das NTP-Paket erstellt wurde, aber bevor es das Paket an den lokalen Client gesendet hat.

Empfangszeit	Dies ist der Zeitstempel, nach dem der lokale Client die Nachricht empfangen hat. Die Differenz zwischen der Organisationszeit und der Empfangszeit ist der Offset für diesen Peer. Im Beispiel hat Primary 10.4.2.254 die folgenden Zeiten:
	
	`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)`
	
	Die Differenz ist der Offset von 268,3044 msec.

xmt-Zeit	Dies ist der Übertragungszeitstempel für das NTP-Paket, das der lokale Client an diesen Peer/Server sendet.

Verzug
Filtoffset
Filter
	Dies ist die Round-Trip-Verzögerung in Millisekunden für jede Stichprobe.
	Dies ist der Uhrzeitoffset in Millisekunden für jede Probe.
	Dies ist der ungefähre Fehler jeder Stichprobe.
	
	Ein Beispiel ist das letzte empfangene NTP-Paket. Im Beispiel hat Primary 10.4.2.254 die folgenden Werte:
	
	`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`

	Diese acht Samples entsprechen dem Wert des Reach-Felds, das anzeigt, ob der lokale Client die letzten acht NTP-Pakete empfangen hat.

NTP-Status anzeigen

Dies ist ein Beispiel für die Ausgabe des Befehls 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
```

Begriffe, die bereits im Abschnitt zum Anzeigen von Zuordnungen oder im Abschnitt zum Anzeigen von NTP-Zuordnungsdetails definiert wurden, werden nicht wiederholt.

Begriff	Erläuterung
Präzision	Die Genauigkeit wird automatisch bestimmt und als Zweierpotenz gemessen. Im Beispiel bedeutet 2**18 2^(-18) oder 3,8 Mikrosekunden. Der Verlust der Synchronisierung zwischen NTP-Peers oder zwischen einem primären und einem Client kann auf verschiedene Ursachen zurückzuführen sein. Das NTP vermeidet die Synchronisierung mit einem System, dessen Uhrzeit auf folgende Weise mehrdeutig sein kann:

	1. NTP führt keine Synchronisierung mit einem System durch, das nicht selbst synchronisiert wurde. 1. Das NTP vergleicht die von mehreren Systemen gemeldete Zeit und führt keine Synchronisierung mit Systemen durch, deren Uhrzeit sich erheblich von der der anderen Systeme unterscheidet, selbst wenn deren Schicht geringer ist.

Fehlerbehebung bei NTP mit Debuggen

Zu den häufigsten Ursachen für NTP-Probleme gehören:

- NTP-Pakete werden nicht empfangen.
- NTP-Pakete werden empfangen, aber nicht vom NTP-Prozess auf dem Cisco IOS verarbeitet.
- NTP-Pakete werden verarbeitet. Fehlerhafte Faktoren oder Paketdaten verursachen jedoch den Verlust der Synchronisierung.
- Die NTP-Taktperiode wird manuell festgelegt.

Wichtige Debug-Befehle, mit denen Sie die Ursache dieser Probleme identifizieren können:

- debuggen von IP-Paketen <acl>

- debuggen von NTP-Paketen
- debug ntp gültigkeit
- debug ntp sync
- debugging ntp-Ereignisse

In den folgenden Abschnitten wird die Verwendung von Debugs zur Behebung dieser häufig auftretenden Probleme erläutert.

Hinweis: Verwenden Sie das Tool zur Befehlssuche, um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen zugreifen.

Hinweis: Lesen Sie den Artikel Important Information on Debug Commands (Wichtige Informationen zu Debug-Befehlen), bevor Sie debug-Befehle verwenden.

NTP-Pakete nicht empfangen

Verwenden Sie den Befehl debug ip packet, um zu überprüfen, ob NTP-Pakete empfangen und gesendet werden. Da die Debug-Ausgabe chattierbar sein kann, können Sie die Debug-Ausgabe mithilfe von Zugriffskontrolllisten (Access Control Lists, ACLs) einschränken. NTP verwendet den UDP-Port 123 (User Datagram Protocol).

1. ACL 101 erstellen:

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

NTP-Pakete haben in der Regel einen Quell- und einen Ziel-Port von 123. Dies hilft:

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

2. Verwenden Sie diese ACL, um die Ausgabe des Befehls debug ip packet einzuschränken:

```
debug ip packet 101
```

3. Wenn das Problem bei bestimmten Peers auftritt, grenzen Sie die ACL 101 auf diese Peers ein. Wenn der Peer 172.16.1.1 lautet, ändern Sie ACL 101 in:

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

Dieses Beispiel zeigt an, dass keine Pakete gesendet wurden:

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

Wenn Sie bestätigen, dass keine NTP-Pakete empfangen wurden, müssen Sie:

- Überprüfen Sie, ob das NTP richtig konfiguriert ist.
- Überprüfen Sie, ob eine ACL NTP-Pakete blockiert.
- Überprüfen Sie, ob Routing-Probleme zur Quell- oder Ziel-IP-Adresse vorliegen.

Nicht verarbeitete NTP-Pakete

Wenn sowohl die Befehle debug ip packet als auch debug ntp packages aktiviert sind, können Sie die empfangenen und übertragenen Pakete sehen, und Sie können sehen, dass das NTP auf diese Pakete einwirkt. Für jedes empfangene NTP-Paket (wie durch debug ip packet dargestellt) gibt es einen entsprechenden Eintrag, der durch debug ntp packages generiert wird.

Dies ist die Debug-Ausgabe, wenn der NTP-Prozess empfangene Pakete verarbeitet:

```
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)
```

Dies ist ein Beispiel, in dem NTP für empfangene Pakete nicht funktioniert. Obwohl NTP-Pakete empfangen werden (wie bei debug ip-Paketen gezeigt), werden sie vom NTP-Prozess nicht verarbeitet. Bei ausgesendeten NTP-Paketen wird ein entsprechendes Debug-NTP-Paket ausgegeben, da der NTP-Prozess das Paket generieren muss. Das Problem betrifft empfangene NTP-Pakete, die nicht verarbeitet werden.

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

Synchronisierungsverlust

Ein Verlust der Synchronisierung kann auftreten, wenn der Dispersions- und/oder Verzögerungswert für einen Server sehr hoch wird. Hohe Werte zeigen an, dass die Pakete zu lange dauern, bis sie vom Server/Peer in Bezug auf den Stamm der Uhr an den Client gesendet werden. Das lokale System kann daher der Genauigkeit der im Paket enthaltenen Zeit nicht vertrauen, da es nicht weiß, wie lange es gedauert hat, bis das Paket hier ankommt.

Das NTP verfolgt einen genauen Zeitrahmen und kann keine Synchronisierung mit einem anderen Gerät durchführen, dem es nicht vertraut oder das es nicht auf eine vertrauenswürdige Weise anpassen kann.

Wenn eine gesättigte Verbindung besteht und zwischengespeichert wird, werden die Pakete verzögert, sobald sie an den NTP-Client gesendet werden. Der Zeitstempel eines nachfolgenden NTP-Pakets kann sich also gelegentlich stark unterscheiden, und der lokale Client kann sich nicht wirklich auf diese Varianz einstellen.

Das NTP bietet nur dann eine Methode, um die Validierung dieser Pakete zu deaktivieren, wenn Sie SNTP (Simple Network Time Protocol) verwenden. SNTP ist keine große Alternative, da es von der Software nicht umfassend unterstützt wird.

Wenn der Synchronisierungsvorgang unterbrochen wird, müssen Sie die folgenden Links überprüfen:

- Sind sie gesättigt?
- Gibt es irgendeinen Ausfall von WAN-Verbindungen (Wide Area Network)?
- Erfolgt die Verschlüsselung?

Überwachen Sie den Reichweitenwert mit dem Befehl show ntp associations detail. Der höchste Wert ist 377. Wenn der Wert 0 oder ein niedriger ist, werden NTP-Pakete periodisch empfangen, und der lokale Client läuft nicht mehr synchron mit dem Server.

debug ntp gültigkeit

Der Befehl debug ntp validation gibt an, ob die Plausibilitäts- oder Validitätsprüfung des NTP-Pakets fehlgeschlagen ist, und gibt den Grund für den Fehler an. Vergleichen Sie diese Ausgabe mit den in RFC1305 angegebenen Integritätstests, mit denen das von einem Server empfangene NTP-Paket getestet wird. Acht Tests sind definiert:

Test Maske	Erläuterung

1	0 x 01	Doppeltes Paket empfangen
2	0 x 02	Scheinpaket empfangen
3	0 x 04	Protokoll nicht synchronisiert
4	0 x 08	Überprüfung der Peer-Verzögerung/Dispersion fehlgeschlagen
5	0 x 10	Peer-Authentifizierung fehlgeschlagen
6	0 x 20	Peer-Uhr nicht synchronisiert (häufig für nicht synchronisierten Server)
7	0 x 40	Peerschicht außerhalb der Bindung
8	0 x 80	Überprüfung der Root-Verzögerung/Dispersion fehlgeschlagen

Dies ist eine Beispielausgabe des Befehls debug ntp validation:

```
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
```

debuggen von NTP-Paketen

Sie können den Befehl debug ntp packages verwenden, um die Zeit anzuzeigen, die Ihnen der Peer/Server im empfangenen Paket zuweist. Die Zeit, die der lokale Rechner dem Peer/Server im übertragenen Paket mitteilt, wie lange er weiß.

Feld	RCV-Paket	xmit-Paket
Org	Zeitstempel des Originators, der die Serverzeit angibt.	Zeitstempel des Absenders (Clients) beim Senden des Pakets. (Der Client sendet ein Paket an den Server.)
rec	Zeitstempel auf dem Client beim Empfang des Pakets.	Aktuelle Client-Zeit.

In dieser Beispielausgabe sind die Zeitstempel des vom Server empfangenen Pakets und des an einen anderen Server gesendeten Pakets identisch. Dies zeigt an, dass das Client-NTP synchronisiert ist.

```
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)
```

Dies ist ein Beispiel für eine Ausgabe, wenn die Uhren nicht synchronisiert sind. Beachten Sie die Zeitdifferenz zwischen dem xmit-Paket und dem rcv-Paket. Die Peer-Dispersion kann den maximalen Wert von 16000 haben, und die Reichweite für den Peer kann 0 anzeigen.

```
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- und debug ntp-Ereignisse

Der Befehl debug ntp sync erzeugt einzeilige Ausgaben, die anzeigen, ob die Uhr synchronisiert oder die Synchronisation geändert wurde. Der Befehl wird im Allgemeinen mit debug ntp-Ereignissen aktiviert.

Der Befehl debug ntp events zeigt alle auftretenden NTP-Ereignisse an. Anhand dieser Informationen können Sie feststellen, ob eine Änderung des NTP ein Problem ausgelöst hat, z. B. dass die Uhren nicht mehr synchronisiert sind. (Mit anderen Worten, wenn deine glücklich synchronisierten Uhren plötzlich verrückt werden, weißt du, dass du nach einem Wechsel oder Auslöser suchen musst!)

Dies ist ein Beispiel für beide Debugs. Zunächst wurden die Client-Uhren synchronisiert. Der Befehl debug ntp events zeigt an, dass eine Änderung der NTP-Peer-Schicht aufgetreten ist und die Uhren nicht mehr synchronisiert sind.

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

NTP-Taktperiode manuell festlegen

Auf der Website Cisco.com wird gewarnt:

"Der Befehl ntp clock-period wird automatisch generiert, um den Korrekturfaktor widerzuspiegeln, der sich ständig ändert, wenn der Befehl copy running-configuration startup-configuration eingegeben wird, um die Konfiguration im NVRAM zu speichern. Versuchen Sie nicht, den Befehl ntp clock-period manuell zu verwenden. Stellen Sie sicher, dass Sie diese Befehlszeile entfernen, wenn Sie Konfigurationsdateien auf andere Geräte kopieren."

Der Wert für die Taktperiode hängt von der Hardware ab und unterscheidet sich daher von Gerät zu Gerät.

Der Befehl ntp clock-period wird automatisch in der Konfiguration angezeigt, wenn Sie NTP aktivieren. Der Befehl wird verwendet, um die Softwareuhr anzupassen. Der 'Anpassungswert' kompensiert das 4 ms Teilungsintervall, sodass Sie bei der geringfügigen Anpassung am Ende des Intervalls 1 Sekunde haben.

Wenn das Gerät berechnet hat, dass seine Systemuhr Zeit verliert (möglicherweise muss eine Frequenzkompensation von der Basisebene des Routers erfolgen), fügt es diesen Wert automatisch der Systemuhr hinzu, um seine Synchronizität aufrechtzuerhalten.

Hinweis: Dieser Befehl darf vom Benutzer nicht geändert werden.

Der Standard-NTP-Zeitraum für einen Router ist 17179869 und wird im Wesentlichen zum Starten des NTP-Prozesses verwendet.

Die Konvertierungsformel lautet 17179869 * 2^(-32) = 0,003999999957159161567687988281 25 oder ca. 4 Millisekunden.

Die Systemuhr für die Cisco 2611 Router (einer der Cisco Router der Serie 2600) war z. B. etwas nicht synchron und konnte mit dem folgenden Befehl re-synchronisiert werden:

```
ntp clock-period 17208078
```

Dies entspricht 17208078 * 2^(-32) = 0,004006567876785993576049804687 5 oder etwas mehr als 4 Millisekunden.

Cisco empfiehlt, den Router unter normalen Netzwerkbedingungen eine Woche lang laufen zu lassen und dann den Befehl wr mem zu verwenden, um den Wert zu speichern. Dadurch erhalten Sie eine genaue Zahl für den nächsten Neustart, und das NTP kann schneller synchronisiert werden.

Verwenden Sie den Befehl no ntp clock-period, wenn Sie die Konfiguration für die Verwendung auf einem anderen Gerät speichern, da dieser Befehl die Uhrzeit auf den Standardwert dieses bestimmten Geräts zurücksetzt. Sie können den wahren Wert neu berechnen (aber die Genauigkeit der Systemuhr während dieses Neuberechnungszeitraums reduzieren).

Denken Sie daran, dass dieser Wert von der Hardware abhängt. Wenn Sie also eine Konfiguration kopieren und auf verschiedenen Geräten verwenden, können Sie Probleme verursachen. Cisco plant, NTP-Version 3 durch Version 4 zu ersetzen, um dieses Problem zu beheben.

Wenn Sie diese Probleme nicht kennen, können Sie diesen Wert manuell anpassen. Um von einem Gerät auf ein anderes zu migrieren, können Sie die alte Konfiguration kopieren und auf dem neuen Gerät einfügen. Da der Befehl "ntp clock-period" in den Befehlen running-config und startup-config angezeigt wird, wird der Befehl "ntp clock-period" auf dem neuen Gerät eingefügt. In diesem Fall läuft das NTP auf dem neuen Client immer synchron mit dem Server mit einem hohen Peer-Dispersionswert.

Löschen Sie stattdessen die NTP-Taktperiode mit dem Befehl no ntp clock-period, und speichern Sie die Konfiguration. Der Router berechnet schließlich eine für sich geeignete Taktperiode.

Der Befehl ntp clock-period ist in Version 15.0 oder höher der Cisco IOS-Software nicht mehr verfügbar. Der Parser lehnt den Befehl jetzt mit der folgenden Fehlermeldung ab:

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

Sie sind nicht berechtigt, die Zeitperiode manuell zu konfigurieren, und die Zeitperiode ist in der Ausführungskonfiguration nicht zulässig. Da der Parser den Befehl zurückweist, wenn er sich in der Startkonfiguration befand (in früheren Cisco IOS-Versionen, z. B. 12.4), lehnt der Parser den Befehl ab, wenn er die Startkonfiguration beim Start in die aktuelle Konfiguration kopiert.

Der neue Befehl "replace" lautet ntp clear drift.

Zugehörige Informationen

- Support Forum Thread: NTP-Taktperiode nicht konfiguriert
- Network Time Protocol: Best Practices - Whitepaper
- Fehlerbehebung beim Network Time Protocol (NTP)
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.