Best Practices für Network Time Protocol

Inhalt

Einleitung

In diesem Dokument werden die Best Practices für das Design des Network Time Protocol beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Network Time Protocol
- Uhrentechnologie und Public Time Server

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 verstehen.

Hintergrundinformationen

IP-basierte Netzwerke (Internet Protocol) haben sich schnell vom *traditionell besten* Bereitstellungsmodell entwickelt und sind nun einem Modell zuzuordnen, bei dem Leistung und Zuverlässigkeit quantifiziert und in vielen Fällen durch Service Level Agreements (SLAs) garantiert werden müssen. Der Bedarf an besseren Einblicken in Netzwerkmerkmale hat zu umfangreichen Forschungsanstrengungen geführt, die sich auf wichtige Metriken und Messfunktionen zur Charakterisierung des Netzwerkverhaltens konzentrieren. Die Grundlage vieler metrischer Methoden ist die Messung der Zeit.

Die Synchronisierung der Netzwerkzeiten ist im Rahmen einer modernen Leistungsanalyse unerlässlich. Basierend auf den Geschäftsmodellen und den bereitgestellten Services wird die Charakterisierung der Netzwerkleistung als wichtiges Differenzierungsmerkmal im Wettbewerb betrachtet. In diesen Fällen entstehen hohe Kosten, wenn Sie Netzwerkmanagementsysteme und technische Direktresourcen bereitstellen, um die erfassten Leistungsdaten zu analysieren. Wenn

jedoch dem oft übersehenen Prinzip der Zeitsynchronisierung keine angemessene Beachtung geschenkt wird, sind diese Bemühungen unwirksam.

In diesem Dokument wird eine hypothetische Prozessdefinition für das Netzwerkmanagement-Funktionsmanagement für das Network Time Protocol (NTP) beschrieben. Sie können diesen Artikel als hypothetisches Verfahren und als Informationsbeispiel verwenden. Dies kann von einer Organisation angepasst werden, um interne Ziele zu erreichen.

Die in diesem Dokument enthaltenen Informationen sind in mehrere Abschnitte gegliedert:

- Der Terminologieabschnitt enthält allgemeine Definitionen von Begriffen rund um die Zeitsynchronisierung.
- Der Abschnitt "Übersicht" enthält Hintergrundinformationen zur Hardware der Netzwerkelemente in Bezug auf die Systemzeit, einen technologischen Überblick über NTP und wichtige Designaspekte für die NTP-Architektur.
- Im Abschnitt "NTP-Bereitstellungsbeispiel" werden Beispiele für NTP-Bereitstellungen mit Beispielkonfigurationen für WAN-, Campus-Netzwerke mit hoher und Campus-Zeit mit niedriger Schicht aufgeführt.
- Der Abschnitt "Prozessdefinitionen" bietet eine Übersicht über die Prozessdefinitionen für die NTP-Verwaltung. Die Prozessdetails werden anhand von Zielen, Leistungsindikatoren, Inputs, Outputs und einzelnen Aufgaben beschrieben.
- Der Abschnitt Aufgabendefinitionen enthält detaillierte Definitionen von Prozessaufgaben. Jede Aufgabe wird in Form von Zielen, Aufgabeneingaben, Aufgabenausgaben, erforderlichen Ressourcen zur Ausführung der Aufgabe und erforderlichen Fertigkeiten für die Aufgabenimplementierung beschrieben.
- Im Abschnitt zur Datenidentifizierung wird die Datenidentifizierung für NTP beschrieben. Bei der Datenidentifizierung wird die Quelle der Informationen berücksichtigt. Informationen können beispielsweise in der Simple Network Management Protocol (SNMP) Management Information Base (MIB), in von Syslog generierten Protokolldateien oder in internen Datenstrukturen enthalten sein, auf die nur über die Befehlszeilenschnittstelle (CLI) zugegriffen werden kann.
- Der Abschnitt "Datensammlung" beschreibt die Erfassung der NTP-Daten. Die Erhebung der Daten steht in engem Zusammenhang mit dem Ort der Daten. SNMP MIB-Daten werden beispielsweise durch verschiedene Mechanismen wie Traps, Remote Monitoring (RMON)-Alarme und -Ereignisse oder Polling erfasst. Daten, die von internen Datenstrukturen verwaltet werden, werden durch automatische Skripte erfasst oder wenn sich ein Benutzer manuell beim System anmeldet, um den CLI-Befehl auszugeben und die Ausgabe aufzuzeichnen.
- Der Abschnitt "Datenpräsentation" enthält Beispiele im Berichtsformat für die Darstellung der Daten.

Terminologie

- **Genauigkeit** - Die Nähe des absoluten Werts des Takts zum Offset von Null.
- **Accurate (Genauigkeit)** - Wenn ein Uhren-Offset zu einem bestimmten Zeitpunkt Null ist.
- **Drift (Drift)** - Die Messung in der Variation von Skew oder die zweite Ableitung des Taktversatzes in Bezug auf die Zeit.
- **Gemeinsame Auflösung** - Wenn Uhren verglichen werden, ist dies die Summe der

Auflösungen von C1 und C2. Die gemeinsame Auflösung gibt dann eine konservative Untergrenze der Genauigkeit von Zeitintervallen an, die durch Zeitstempel berechnet werden, die von einer Uhr erzeugt werden, die von den Zeitstempeln der anderen Uhr subtrahiert wird.
- **Node (Knoten**): Bezeichnet eine Instanziierung des NTP-Protokolls auf einem lokalen Prozessor. Ein Knoten kann auch als Gerät bezeichnet werden.
- **Offset (Offset**) - Die Differenz zwischen der von einer Uhr gemeldeten Zeit und der wahren Zeit, die von der Universellen koordinierten Zeit (UTC, Coordinated Universal Time) definiert wird. Wenn die Uhr eine Zeit Tc meldet und die wahre Zeit Tt ist, dann ist der Taktversatz Tc - Tt.
- **Peer** - Bezieht sich auf eine Instanziierung des NTP-Protokolls auf einem Remote-Prozessor, der über einen Netzwerkpfad vom lokalen Knoten verbunden ist.
- **Relativer Offset** - Der Begriff "wahre Zeit" wird durch die Zeit ersetzt, die durch den Takt C1 gemeldet wird, wenn zwei Uhren, C1 und C2, verglichen werden. Beispielsweise ist der Versatz des Taktes C2 relativ zu C1 zu einem bestimmten Zeitpunkt Tc2 - Tc1, die momentane Zeitdifferenz, die von C2 und C1 gemeldet wird.
- **Resolution (Auflösung**): Die kleinste Einheit, um die eine Uhrzeit aktualisiert wird. Die Auflösung wird in Sekunden angegeben. Die Auflösung ist jedoch relativ zur gemeldeten Uhrzeit und nicht zur wahren Zeit. Eine Auflösung von 10 Millisekunden bedeutet beispielsweise, dass die Uhr ihren Zeitbegriff in Schritten von 0,01 Sekunden aktualisiert, und nicht, dass dies der tatsächliche Zeitraum zwischen den Updates ist.**Hinweis**: Uhren können sehr feine Auflösungen haben und immer noch ungenau sein.
- **Skew (**Verzerrung) - Eine Taktfrequenzdifferenz oder die erste Ableitung ihres Offsets in Bezug auf die Zeit.
- **Synchronisieren (Synchronize**) - Wenn zwei Uhren genau zueinander sind (der relative Offset ist Null), werden sie synchronisiert. Uhren können synchronisiert werden und immer noch ungenau in Bezug darauf, wie gut sie wahre Zeit erzählen.

Überblick

Geräteübersicht

Das Herzstück des Zeitdienstes ist die Systemuhr. Die Systemuhr läuft ab dem Zeitpunkt, an dem das System gestartet wird, und verfolgt das aktuelle Datum und die aktuelle Uhrzeit. Die Systemuhr kann aus einer Vielzahl von Quellen eingestellt werden und kann wiederum dazu verwendet werden, die aktuelle Zeit über verschiedene Mechanismen auf andere Systeme zu verteilen. Einige Router enthalten ein batteriebetriebenes Kalendersystem, das Datum und Uhrzeit bei Systemneustarts und Stromausfällen verfolgt. Dieses Kalendersystem wird immer verwendet, um die Systemuhr zu initialisieren, wenn das System neu gestartet wird. Sie kann auch als maßgebliche Zeitquelle angesehen und über NTP umverteilt werden, wenn keine andere Quelle verfügbar ist. Wenn NTP aktiviert ist, wird der Kalender darüber hinaus regelmäßig vom NTP aktualisiert. Dadurch wird die inhärente Verschiebung der Kalenderzeit ausgeglichen. Wenn ein Router mit einem Systemkalender initialisiert wird, wird die Systemuhr anhand der Zeit im internen batteriebetriebenen Kalender eingestellt. Bei Modellen ohne Kalender wird die Systemuhr auf eine vorgegebene Zeitkonstante eingestellt. Die Systemuhr kann aus den als Nächstes aufgeführten Quellen eingestellt werden.

- NTP
- Simple Network Time Protocol (SNTP)

- Virtual Integrated Network Service (VINES) Time Service
- Manuelle Konfiguration

Einige einfache Cisco Geräte unterstützen nur SNTP. SNTP ist eine vereinfachte, nur auf Clients beschränkte Version von NTP. SNTP kann nur die Zeit von NTP-Servern empfangen und nicht verwendet werden, um Zeitdienste für andere Systeme bereitzustellen. SNTP liefert normalerweise eine Zeit innerhalb von 100 Millisekunden nach der genauen Zeit. Darüber hinaus authentifiziert SNTP keinen Datenverkehr. Sie können jedoch erweiterte Zugriffslisten konfigurieren, um einen gewissen Schutz zu gewährleisten. Ein SNTP-Client ist anfälliger für nicht konforme Server als ein NTP-Client und darf nur in Situationen verwendet werden, in denen keine starke Authentifizierung erforderlich ist.

Die Systemuhr zeigt die Zeit für die als Nächstes aufgeführten Dienste an.

- NTP
- VINES-Zeitdienst
- BenutzershowBefehle
- Protokollieren und Debuggen von Meldungen

Die Systemuhr verfolgt intern die Zeit basierend auf UTC, auch bekannt als Greenwich Mean Time (GMT). Sie können Informationen zur lokalen Zeitzone und zur Sommerzeit konfigurieren, sodass die Zeit im Verhältnis zur lokalen Zeitzone richtig angezeigt wird. Die Systemuhr verfolgt, ob die Zeit maßgebend ist oder nicht. Ist sie nicht autoritär, kann die Zeit nur für Anzeigezwecke zur Verfügung stehen und kann nicht umverteilt werden.

NTP - Übersicht

Das NTP wurde zur Synchronisierung der Uhrzeit in einem Netzwerk von Systemen entwickelt. Das NTP wird über das User Datagram Protocol (UDP) ausgeführt, wobei Port 123 sowohl als Quelle als auch als Ziel fungiert, das wiederum über IP ausgeführt wird. Die NTP-Version 3RFC 1305 dient zum Synchronisieren der Zeiterfassung für eine Reihe von verteilten Zeitservern und Clients. Eine Gruppe von Knoten in einem Netzwerk wird mit NTP identifiziert und konfiguriert, und die Knoten bilden ein Synchronisierungs-Subnetz, das manchmal als Overlay-Netzwerk bezeichnet wird. Es können zwar mehrere primäre Server vorhanden sein, ein Auswahlprotokoll ist jedoch nicht erforderlich.

Ein NTP-Netzwerk erhält seine Uhrzeit normalerweise von einer zuverlässigen Zeitquelle, z. B. einer mit einem Zeitserver verbundenen Funkuhr oder Atomuhr. NTP verteilt diese Zeit dann über das Netzwerk. Ein NTP-Client führt über sein Abfrageintervall (von 64 auf 1024 Sekunden) eine Transaktion mit seinem Server durch, die sich im Laufe der Zeit dynamisch in Abhängigkeit von den Netzwerkbedingungen zwischen dem NTP-Server und dem Client ändert. Die andere Situation tritt auf, wenn der Router mit einem fehlerhaften NTP-Server kommuniziert (z. B. einem NTP-Server mit großer Dispersion). Der Router erhöht auch das Abfrageintervall. Es ist nicht mehr als eine NTP-Transaktion pro Minute erforderlich, um zwei Systeme zu synchronisieren. Es ist nicht möglich, das NTP-Abfrageintervall auf einem Router anzupassen.

Das NTP nutzt das Schichtenkonzept, um zu beschreiben, wie viele NTP-Hops ein Rechner von einer maßgeblichen Zeitquelle entfernt ist. Beispielsweise ist ein Schicht-1-Zeitserver direkt mit einer Funk- oder Atomuhr verbunden. Anschließend wird die Uhrzeit über NTP an einen Schicht-2-Zeitserver gesendet usw. Ein Computer, der das NTP ausführt, wählt automatisch den Computer mit der niedrigsten Schicht-Nummer aus, für die die Kommunikation mit dem NTP als Zeitquelle konfiguriert ist. Mit dieser Strategie wird auf effektive Weise ein sich selbst organisierender Tree aus NTP-Routern erstellt. NTP schneidet bei den nicht deterministischen

Pfadlängen von paketvermittelten Netzwerken gut ab, da es robuste Schätzungen der nächsten drei Schlüsselvariablen in der Beziehung zwischen einem Client und einem Zeitserver erstellt.

- Netzwerkverzögerung
- Zeitliche Verteilung des Paketaustauschs - Ein Maß für den maximalen Uhrfehler zwischen den beiden Hosts.
- Uhren-Offset - Die Korrektur, die auf eine Client-Uhr angewendet wird, um diese zu synchronisieren.

Die Uhrensynchronisierung erfolgt auf der Ebene von 10 Millisekunden über WANs (2000 km) für große Entfernungen und auf der Ebene von 1 Millisekunde für LANs.

Es gibt zwei Möglichkeiten, wie das NTP nicht mit einem Computer synchronisiert werden kann, dessen Uhrzeit nicht genau ist. Erstens führt das NTP keine Synchronisierung mit einem System durch, das nicht selbst synchronisiert wurde. Zweitens vergleicht das NTP 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.

Die Kommunikation zwischen Computern, auf denen NTP ausgeführt wird (Verknüpfungen), wird in der Regel statisch konfiguriert. Jeder Rechner erhält die IP-Adresse aller Rechner, mit denen er Zuordnungen bilden muss. Eine genaue Zeiterfassung wird durch NTP-Nachrichten ermöglicht, die zwischen zwei Rechnern mit einer Zuordnung ausgetauscht werden. In einer LAN-Umgebung kann das NTP jedoch so konfiguriert werden, dass es stattdessen IP-Broadcast-Nachrichten verwendet. Diese Alternative verringert den Konfigurationsaufwand, da jeder Computer so konfiguriert werden kann, dass er Broadcast-Nachrichten sendet oder empfängt. Die Genauigkeit der Zeiterfassung wird jedoch geringfügig reduziert, da der Informationsfluss nur in eine Richtung erfolgt.

Die auf einem Computer gespeicherte Zeit ist eine wichtige Ressource, und es wird dringend empfohlen, die Sicherheitsfunktionen von NTP zu verwenden, um versehentliche oder böswillige Einstellungen falscher Zeit zu vermeiden. Die beiden verfügbaren Sicherheitsfunktionen sind ein Zugriffslisten-basiertes Beschränkungsschema und ein verschlüsselter Authentifizierungsmechanismus.

Die NTP-Implementierung von Cisco unterstützt den Schicht-1-Service bestimmter Cisco IOS®-Softwareversionen. Wenn eine Freigabe den Befehl **thentp** refclock unterstützt, ist es möglich, eine Funk- oder Atomuhr anzuschließen. Bestimmte Versionen von Cisco IOS unterstützen entweder das Trimble Palisade NTP Synchronization Kit (nur Cisco Router der Serie 7200) oder das Telecom Solutions Global Positioning System (GPS). Wenn das Netzwerk die öffentlichen Zeitserver im Internet verwendet und das Netzwerk vom Internet isoliert ist, ermöglicht die Implementierung von NTP durch Cisco die Konfiguration eines Systems, sodass es wie über NTP synchronisiert agiert, obwohl es die Zeit tatsächlich auf andere Weise bestimmt hat. Andere Systeme werden dann über NTP mit diesem System synchronisiert.

NTP-Designkriterien

Jeder Client im Synchronisierungs-Subnetz, der auch ein Server für Clients höherer Schichten sein kann, wählt einen der verfügbaren Server für die Synchronisierung aus. Dieser Server gehört in der Regel zu den Servern der untersten Schicht, auf die er Zugriff hat. Dies ist jedoch nicht immer eine optimale Konfiguration, da das NTP ebenfalls unter der Prämisse betrieben wird, dass jede Serverzeit mit einem gewissen Maß an Misstrauen betrachtet werden muss. NTP bevorzugt den Zugriff auf mehrere Quellen einer kürzeren Schicht (mindestens drei), da es dann einen

Vereinbarungsalgorithmus anwenden kann, um Wahnsinn von einer dieser Quellen zu erkennen. Wenn alle Server übereinstimmen, wählt das NTP in der Regel den besten Server in Bezug auf die niedrigste Schicht, die nächstgelegene Schicht (in Bezug auf die Netzwerkverzögerung) und die angegebene Genauigkeit aus. Dies bedeutet, dass zwar angestrebt werden muss, jedem Client drei oder mehr Quellen für kürzere Schichten zur Verfügung zu stellen, dass jedoch einige von ihnen nur Backup-Services bereitstellen können und in Bezug auf Netzwerkverzögerungen und Schichten von geringerer Qualität sein können. Beispielsweise kann ein Peer derselben Schicht, der Zeit von Quellen einer niedrigeren Schicht erhält, auf die der lokale Server nicht direkt zugreift, ebenfalls einen guten Backup-Service bieten.

Das NTP bevorzugt in der Regel Server mit niedrigeren Schichten gegenüber Servern mit höheren Schichten, es sei denn, die Serverzeit mit niedrigeren Schichten unterscheidet sich erheblich. Der Algorithmus ist in der Lage, zu erkennen, wenn eine Zeitquelle wahrscheinlich extrem ungenau oder irrsinnig ist, und um Synchronisation in diesen Fällen zu verhindern, auch wenn die ungenaue Uhr auf einer niedrigeren Schicht Ebene ist. Und es kann niemals ein Gerät mit einem anderen Server synchronisieren, der nicht selbst synchronisiert ist.

Um zu erklären, ob der Server zuverlässig ist, muss er viele Plausibilitätsprüfungen bestehen, z. B.:

- Die Implementierungen müssen Zeitüberschreitungen für die Vernunft enthalten, die Trap-Übertragungen verhindern, wenn das Überwachungsprogramm diese Informationen nach einem längeren Intervall nicht erneuert.
- Zusätzliche Plausibilitätsprüfungen sind für die Authentifizierung, Bereichsgrenzen und zur Vermeidung der Verwendung sehr alter Daten enthalten.
- Es wurden Prüfungen hinzugefügt, um zu warnen, dass der Oszillator zu lange gegangen ist, ohne dass er von einer Referenzquelle aktualisiert wurde.
- Die Variablen peer.valid und sys.hold wurden hinzugefügt, um Instabilitäten zu vermeiden, wenn sich die Referenzquelle aufgrund großer dispersiver Verzögerungen bei starken Netzwerküberlastungen schnell ändert. Die Bits "peer.config", "peer.authenable" und "peer.authentic" wurden hinzugefügt, um spezielle Funktionen zu steuern und die Konfiguration zu vereinfachen.

Wenn mindestens eine dieser Prüfungen fehlschlägt, erklärt der Router dies für unzutreffend.

Zuordnungsmodi

In den nächsten Abschnitten werden die Zuordnungsmodi beschrieben, die die NTP-Server für die Zuordnung untereinander verwenden.

- Client/Server
- Symmetrisch Aktiv/Passiv
- Senden

Client/Server-Modus

Abhängige Clients und Server arbeiten normalerweise im Client/Server-Modus, in dem ein Client oder ein abhängiger Server mit einem Gruppenmitglied synchronisiert werden kann, jedoch kein Gruppenmitglied mit dem Client oder dem abhängigen Server synchronisiert werden kann. Dies bietet Schutz vor Fehlfunktionen oder Protokollangriffen.

Der Client-Server-Modus ist die am häufigsten verwendete Internetkonfiguration. Es arbeitet im klassischen RPC-Paradigma (Remote Procedure Call) mit Stateless Servern. In diesem Modus sendet ein Client eine Anfrage an den Server und erwartet zu einem späteren Zeitpunkt eine Antwort. In einigen Kontexten wird dies als Abfragevorgang beschrieben, indem der Client die Zeit- und Authentifizierungsdaten vom Server abfragt. Ein Client wird im Clientmodus mit dem Serverbefehl und dem angegebenen DNS-Namen (Domain Name Server) oder der angegebenen Adresse konfiguriert. Für den Server ist keine vorherige Konfiguration erforderlich.

In einem allgemeinen Client/Server-Modell sendet ein Client eine NTP-Nachricht an einen oder mehrere Server und verarbeitet die Antworten, wie sie empfangen werden. Der Server tauscht Adressen und Ports aus, überschreibt bestimmte Felder in der Nachricht, berechnet die Prüfsumme neu und sendet die Nachricht sofort zurück. Mithilfe der in der NTP-Nachricht enthaltenen Informationen kann der Client die Serverzeit in Bezug auf die lokale Zeit bestimmen und dann die lokale Uhr nach Bedarf anpassen. Darüber hinaus enthält die Nachricht Informationen zur Berechnung der erwarteten Genauigkeit und Zuverlässigkeit der Zeiterfassung sowie zur Auswahl des besten Servers.

Server, die eine Synchronisierung mit einer großen Anzahl von Clients ermöglichen, arbeiten normalerweise als Gruppe von drei oder mehr gegenseitig redundanten Servern und arbeiten jeweils mit drei oder mehr Schicht-1- oder Schicht-2-Servern im Client/Server-Modus sowie mit allen anderen Mitgliedern der Gruppe im symmetrischen Modus. Dies bietet Schutz vor Fehlfunktionen, bei denen ein oder mehrere Server ausfallen oder eine falsche Zeit liefern. Die NTP-Algorithmen sind so konzipiert, dass sie vor Angriffen schützen, wenn ein Bruchteil der konfigurierten Synchronisierungsquellen versehentlich oder vorsätzlich eine falsche Zeit liefert. In diesen Fällen wird ein spezielles Abstimmungsverfahren angewandt, um falsche Quellen zu identifizieren und ihre Daten zu verwerfen. Aus Gründen der Zuverlässigkeit können ausgewählte Hosts mit externen Uhren ausgestattet und für Backups bei Ausfall des primären und/oder sekundären Servers bzw. der Kommunikationswege zwischen diesen verwendet werden.

Die Konfiguration einer Zuordnung im Clientmodus wird normalerweise durch eine Serverdeklaration in der Konfigurationsdatei angegeben und gibt an, dass Sie Zeit vom Remoteserver abrufen möchten, dass Sie jedoch keine Zeit für den Remoteserver angeben möchten.

Symmetrischer Aktiv/Passiv-Modus

Der symmetrische Aktiv/Passiv-Modus ist für Konfigurationen vorgesehen, bei denen eine Gruppe von Peers auf einer niedrigen Schicht als gegenseitige Backups fungiert. Jeder Peer arbeitet mit einer oder mehreren primären Referenzquellen, z. B. einer Funkuhr oder einer Untergruppe zuverlässiger sekundärer Server. Wenn einer der Peers alle Referenzquellen verliert oder einfach den Betrieb beendet, werden die anderen Peers automatisch neu konfiguriert, sodass Zeitwerte von den aktuellen Peers zu allen anderen in der Warteschlange fließen können. In einigen Kontexten wird dies als *Aush*-Pulloperation beschrieben, indem der Peer die Zeit und die Werte entweder zieht oder verschiebt, basierend auf der jeweiligen Konfiguration.

Die Konfiguration einer Zuordnung im symmetrisch-aktiven Modus, die üblicherweise durch eine Peer-Deklaration in der Konfigurationsdatei angegeben wird, weist den Remote-Server darauf hin, dass man Zeit vom Remote-Server beziehen möchte und dass man auch bereit ist, dem Remote-Server bei Bedarf Zeit zuzuführen. Dieser Modus eignet sich für Konfigurationen mit mehreren redundanten Zeitservern, die über verschiedene Netzwerkpfade miteinander verbunden sind. Dies ist derzeit bei den meisten Schicht-1- und Schicht-2-Servern im Internet der Fall.

Symmetrische Modi werden am häufigsten zwischen zwei oder mehr Servern verwendet, die als gegenseitig redundante Gruppe arbeiten. In diesen Modi legen die Server in den Gruppenmitgliedern die Synchronisierungspfade so fest, dass eine maximale Leistung erzielt wird, basierend auf dem Netzwerk-Jitter und der Weiterleitungsverzögerung. Wenn eines oder mehrere der Gruppenmitglieder ausfallen, werden die verbleibenden Mitglieder automatisch neu konfiguriert.

Ein Peer wird im symmetrischen Aktiv-Modus mit dem Befehl peerkonfiguriert, wenn der DNS-Name oder die DNS-Adresse des anderen Peers angegeben wird. Der andere Peer wird auf diese Weise ebenfalls im symmetrischen aktiven Modus konfiguriert.

> **Hinweis**: Wenn der andere Peer nicht speziell auf diese Weise konfiguriert ist, wird bei Eintreffen einer symmetrischen aktiven Nachricht eine symmetrische passive Zuordnung aktiviert. Da ein Eindringling einen symmetrischen aktiven Peer imitieren und falsche Zeitwerte einschleusen kann, muss der symmetrische Modus immer authentifiziert werden.

Broadcast- und/oder Multicast-Modus

Wenn die Anforderungen an die Genauigkeit und Zuverlässigkeit eher gering sind, können die Clients für die Verwendung des Broadcast- und/oder Multicast-Modus konfiguriert werden. Normalerweise werden diese Modi nicht von Servern mit abhängigen Clients verwendet. Der Vorteil besteht darin, dass die Clients nicht für einen bestimmten Server konfiguriert werden müssen. Dies ermöglicht es allen Clients, dieselbe Konfigurationsdatei zu verwenden. Für den Broadcast-Modus ist ein Broadcast-Server im gleichen Subnetz erforderlich. Da Broadcast-Nachrichten nicht von Routern weitergeleitet werden, werden nur Broadcast-Server im gleichen Subnetz verwendet.

Der Broadcast-Modus ist für Konfigurationen vorgesehen, die einen oder mehrere Server und eine potenziell große Client-Population betreffen. Ein Broadcast-Server wird mit dem Befehl "ebroadcast" und einer lokalen Subnetzadresse konfiguriert. Ein Broadcast-Client wird mit dem BefehlBroadcastClient konfiguriert, der es dem Broadcast-Client ermöglicht, auf über eine beliebige Schnittstelle empfangene Broadcast-Nachrichten zu reagieren. Da ein Eindringling einen Broadcast-Server imitieren und falsche Zeitwerte einschleusen kann, muss dieser Modus immer authentifiziert werden.

NTP-Leap-Sekunde festlegen

Sie können den Befehl **thentp jump {add|delete}** verwenden, um eine Schaltsekunde einzufügen. Es gibt Optionen zum Hinzufügen oder Löschen von Schaltsekunden. Es gibt zwei Einschränkungen für diesen Vorgang:

- Die Uhr muss im Synchronisierungsstatus sein.
- Der Befehl wird nur innerhalb des Monats akzeptiert, bevor der Sprung erfolgen soll. Es kann keinen Sprung setzen, wenn die aktuelle Zeit vor 1 Monat nach dem Auftreten des Sprungs liegt.

Nachdem Sie sie gesetzt haben, wird die Schaltsekunde zur letzten Sekunde hinzugefügt oder gelöscht, wie hier gezeigt:

```
NTP leap second added :
```

```
Show clock given continuously
vl-7500-6#show clock
23:59:58.123 UTC Sun Dec 31 2006
vl-7500-6#show clock
23:59:58.619 UTC Sun Dec 31 2006
vl-7500-6#show clock
23:59:59.123 UTC Sun Dec 31 2006
vl-7500-6#show clock
23:59:59.627 UTC Sun Dec 31 2006
<< 59th second occurring twice
vl-7500-6#show clock
23:59:59.131 UTC Sun Dec 31 2006
vl-7500-6#show clock
23:59:59.627 UTC Sun Dec 31 2006
vl-7500-6#show clock
00:00:00.127 UTC Mon Jan 1 2007
vl-7500-6#show clock
00:00:00.623 UTC Mon Jan 1 2007
```

NTP-Architektur

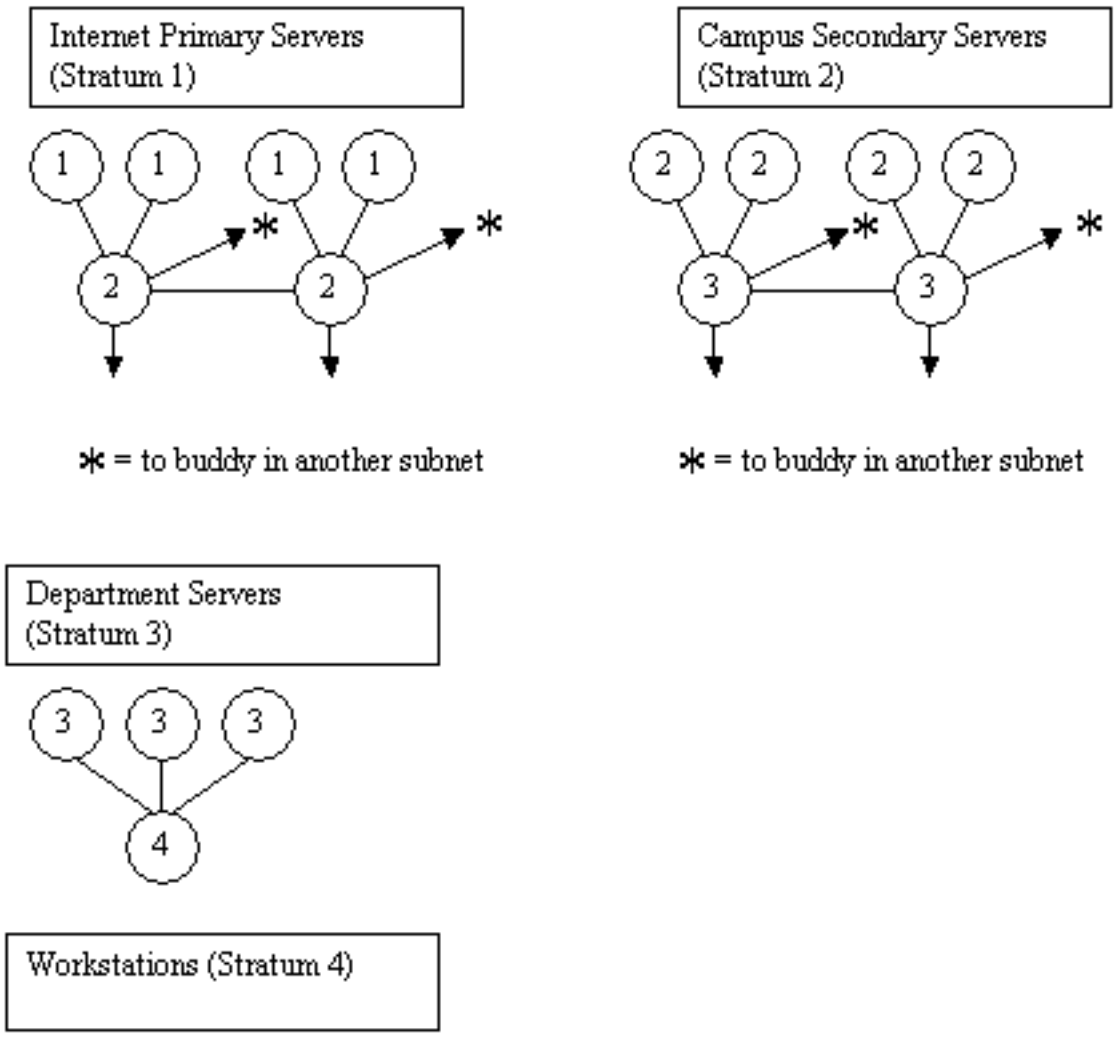
Diese drei Strukturen stehen für die NTP-Architektur zur Verfügung:

- Flache Peer-Struktur
- Hierarchische Struktur
- Sternstruktur

In einer flachen Peer-Struktur bilden alle Router eine Peer-Beziehung zueinander, wobei einige geografisch unabhängige Router so konfiguriert sind, dass sie auf externe Systeme verweisen. Die Konvergenzzeit verlängert sich mit jedem neuen Mitglied des NTP-Netzes.

In einer hierarchischen Struktur wird die Routing-Hierarchie für die NTP-Hierarchie kopiert. Core-Router haben eine Client/Server-Beziehung zu externen Zeitquellen, die internen Zeitserver haben eine Client/Server-Beziehung zu den Core-Routern, die internen Benutzer- (Nicht-Zeitserver)-Router haben eine Client/Server-Beziehung zu den internen Zeitservern und so weiter in der Struktur. Diese Beziehungen werden als Hierarchieebenen bezeichnet. Eine hierarchische Struktur ist das bevorzugte Verfahren, da sie Konsistenz, Stabilität und Skalierbarkeit bietet.

Eine skalierbare NTP-Architektur weist eine hierarchische Struktur auf, wie im nächsten Diagramm dargestellt.



Skalierbare NTP-Architektur

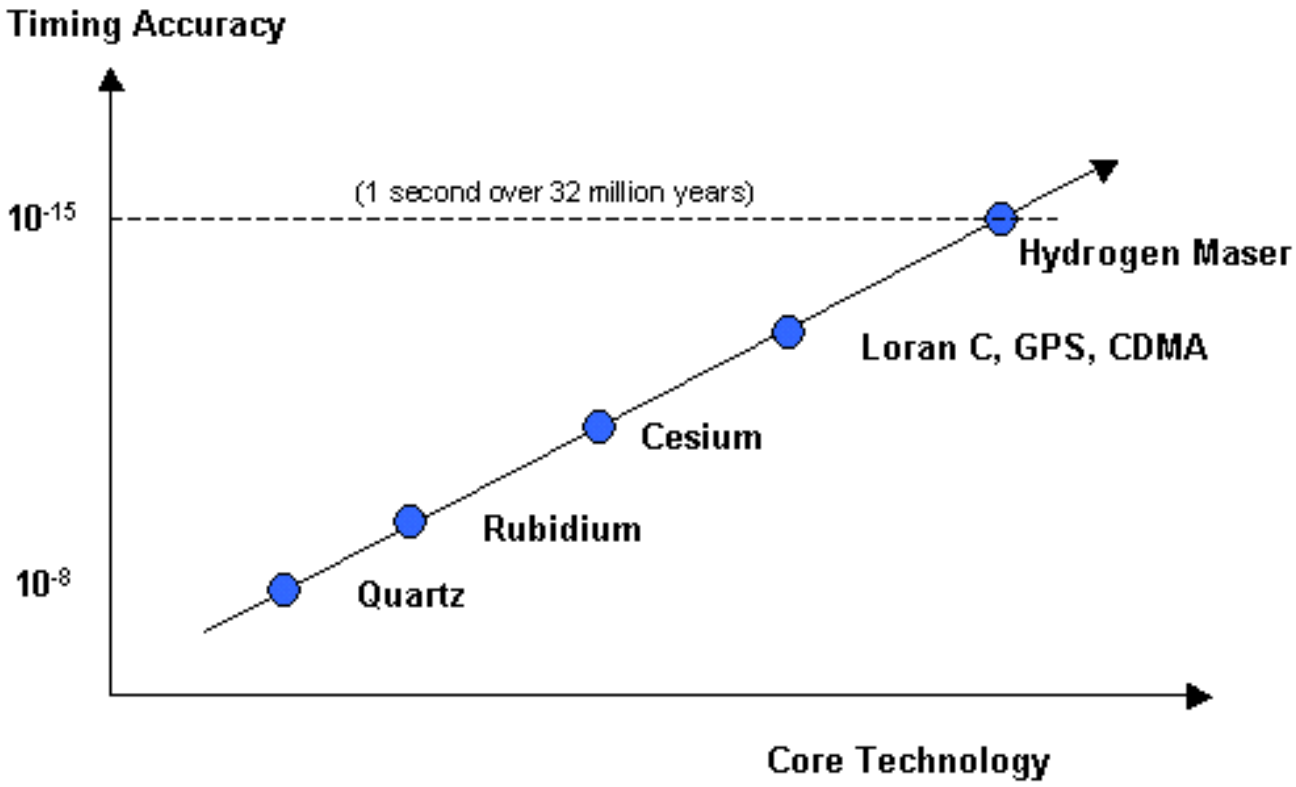
In einer Sternstruktur haben alle Router eine Client/Server-Beziehung zu einigen wenigen Zeitservern im Kern. Die dedizierten Zeitserver sind das Zentrum des Sterns und sind in der Regel mit externen Zeitquellen oder einem eigenen GPS-Empfänger synchronisierte UNIX-Systeme.

Uhrentechnologie und Public Time Server

Das Internet-NTP-Subnetz umfasst derzeit über 50 öffentliche primäre Server, die über Funk, Satellit oder Modem direkt mit UTC synchronisiert werden. Normalerweise werden Client-Workstations und Server mit einer relativ kleinen Anzahl von Clients nicht mit primären Servern synchronisiert. Etwa 100 öffentliche sekundäre Server werden mit den primären Servern synchronisiert und ermöglichen die Synchronisierung von insgesamt mehr als 100.000 Clients und Servern im Internet. DieListen der öffentlichen NTP-Zeitserver werden regelmäßig aktualisiert. Darüber hinaus gibt es zahlreiche private primäre und sekundäre Server, die normalerweise nicht öffentlich zugänglich sind.

> **Hinweis**: PIX und ASA können nicht als NTP-Server, sondern als NTP-Client konfiguriert werden.

In bestimmten Fällen, in denen im privaten Unternehmen hochgenaue Zeitdienste erforderlich sind, z. B. unidirektionale Metriken für VoIP-Messungen, können Netzwerkdesigner private externe Zeitquellen bereitstellen. Das nächste Diagramm zeigt eine vergleichende Grafik der relativen Genauigkeit der aktuellen Technologien.



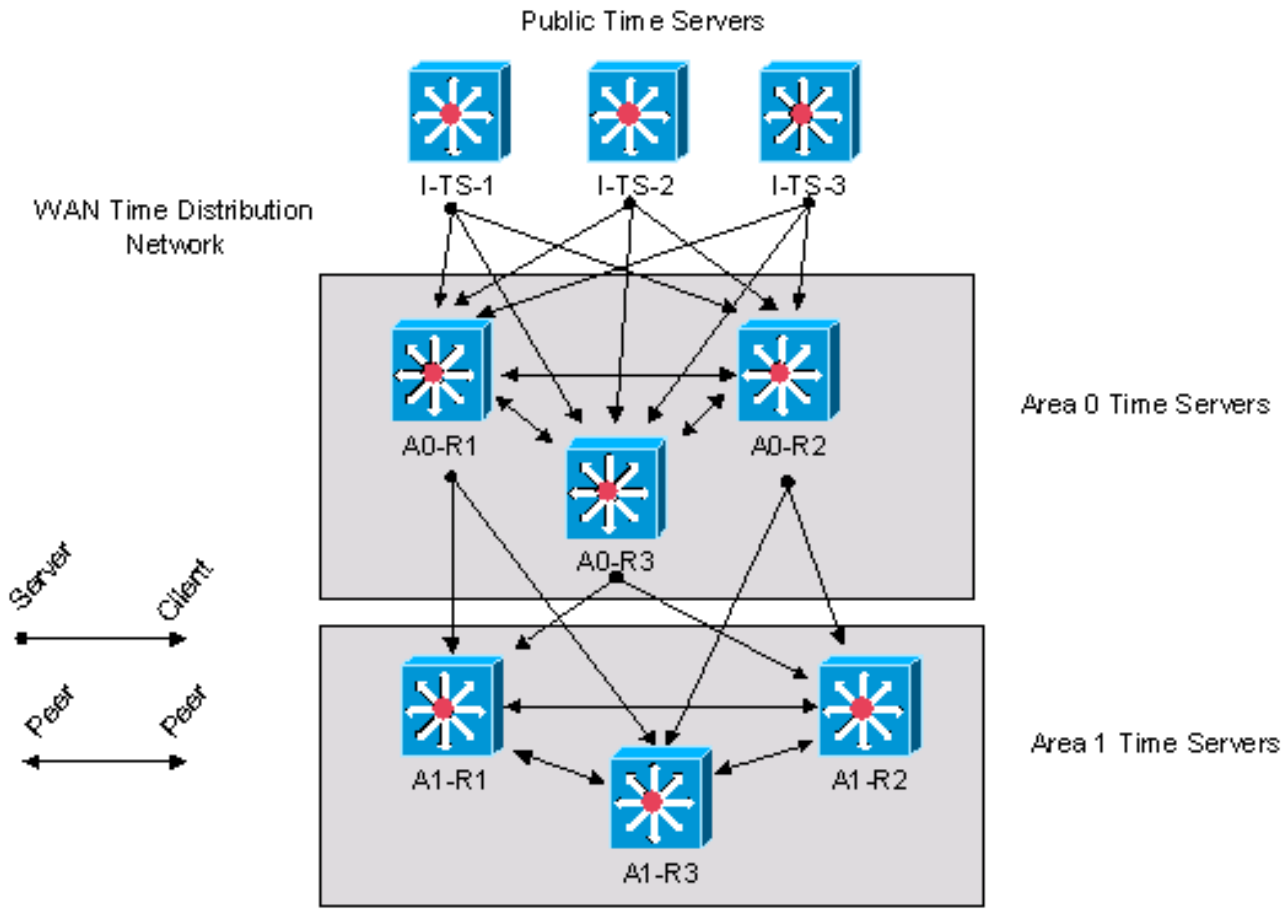
Vergleichsdiagramm

Bis vor kurzem wurde die Verwendung externer Zeitquellen in Unternehmensnetzwerken aufgrund der hohen Kosten für hochwertige externe Zeitquellen nicht weit verbreitet. Da jedoch die QoS-Anforderungen (Quality of Service) steigen und die Kosten für die Zeittechnologie weiter sinken, sind externe Zeitquellen für Unternehmensnetzwerke eine gangbare Option.

Beispiele für NTP-Bereitstellungen

WAN-Zeitverteilungsnetzwerk

Im nächsten Diagramm bezieht ein autonomes System (AS) eines Unternehmens Zeitinformationen von drei öffentlichen Zeitservern. Das Unternehmens-AS wird als Zeitserver für Area 0 und Area 1 angezeigt. In diesem Beispiel folgt die NTP-Hierarchie der OSPF-Hierarchie (Open Shortest Path First). OSPF ist jedoch keine Voraussetzung für NTP. Es wird nur als anschauliches Beispiel verwendet. NTP kann entlang anderer logischer, hierarchischer Grenzen bereitgestellt werden, z. B. einer EIGRP-Hierarchie (Enhanced Interior Gateway Routing Protocol) oder der standardmäßigen Core-/Distribution-/Access-Hierarchie.



WAN-Zeitverteilungsnetzwerk

Dieses Beispiel ist die Cisco IOS-Konfiguration für Gerät A0-R1, wie im vorherigen Diagramm gezeigt.

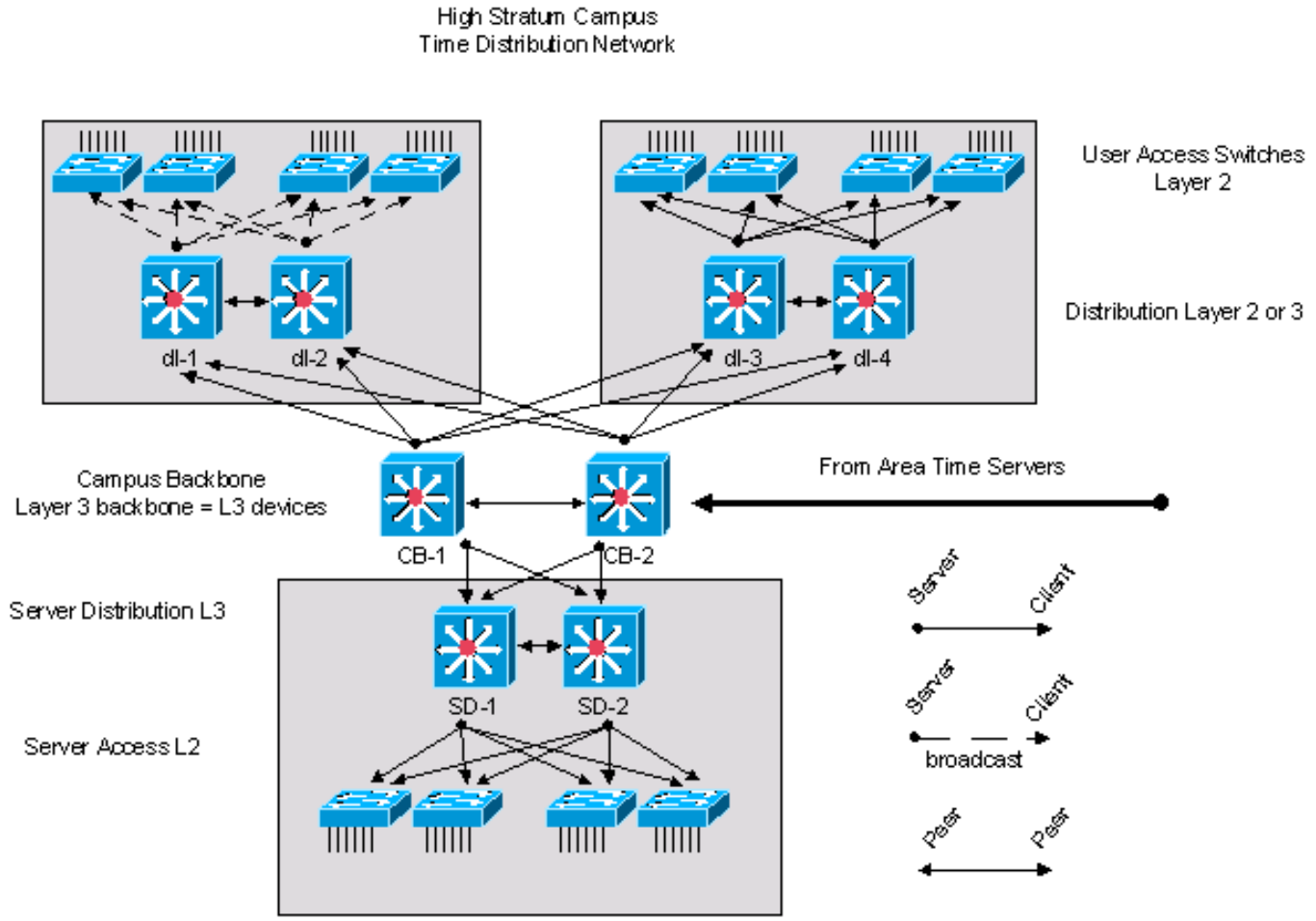
```
clock timezone CST -5
clock summer-time CDT recurring


!--- This router has a hardware calendar.
!--- To configure a system as an
!--- authoritative time source for a network
!--- based on its hardware clock (calendar),
!--- use the clock calendar-valid global
!--- configuration command. Notice later that
!--- NTP can be allowed to update the calendar
!--- and Cisco IOS can be configured to be an
!--- NTP master clock source.
!--- Cisco IOS can then obtain its clock from
!--- the hardware calendar. clock calendar-valid !--- This allows NTP to update the hardware
!--- calendar chip. ntp update-calendar !--- Configures the Cisco IOS software as an
!--- NTP master clock to which peers synchronize
!--- themselves when an external NTP source is
!--- not available. Cisco IOS can obtain the
!--- clock from the hardware calendar based on
!--- the previous line. This line can keep the
!--- whole network in Sync even if Router1 loses
!--- its signal from the Internet. Assume, for
!--- this example, that the Internet time servers
!--- are stratum 2. ntp master 3 !--- When the system sends an NTP packet, the
```

```
!--- source IP address is normally set to the
!--- address of the interface through which the
!--- NTP packet is sent.
!--- Change this to use loopback0. ntp source Loopback0 !--- Enables NTP authentication. ntp
authenticate ntp authentication-key 1234 md5 104D000A0618 7 ntp trusted-key 1234 !--- Configures
the access control groups for
!--- the public servers and peers for additional
!--- security. access-list 5 permit <I-TS-1> access-list 5 permit <I-TS-2> access-list 5 permit
<I-TS-3> access-list 5 permit <A0-R2> access-list 5 permit <A0-R3> access-list 5 deny any !---
Configures the access control groups for the
!--- clients to this node for additional security. access-list 6 permit <A1-R1> access-list 6
permit <A1-R2> access-list 6 permit <A1-R3> access-list 6 deny any !--- Restricts the IP
addresses for the peers
!--- and clients. ntp access-group peer 5 ntp access-group serve-only 6 !--- Fault tolerant
configuration polling for 3 NTP
!--- public servers, peering with 2 local servers. ntp server <I-TS-1> ntp server <I-TS-2> ntp
server <I-TS-3> ntp peer <A0-R2> ntp peer <A0-R3>
```

Campus-Zeitverteilungsnetzwerk mit hoher Schicht

Im vorherigen Abschnitt wurde ein WAN-Zeitverteilungsnetzwerk beschrieben. In diesem Abschnitt wird die Zeitverteilung auf einem Campus-Netzwerk mit hoher Schicht in der Hierarchie einen Schritt nach unten verschoben.

Der Hauptunterschied bei der Zeitverteilung in einem Campus-Netzwerk mit hoher Schicht besteht in der möglichen Verwendung des Broadcast-Zuordnungsmodus. Wie bereits beschrieben, vereinfacht der Broadcast-Zuordnungsmodus die Konfigurationen für die LANs, verringert jedoch die Genauigkeit der Zeitberechnungen. Daher ist der Ausgleich der Wartungskosten gegen die Genauigkeit der Leistungsmessungen zu berücksichtigen.



Das im obigen Diagramm dargestellte Hochschicht-Campus-Netzwerk basiert auf dem Cisco Campus-Standarddesign und umfasst drei Komponenten. Der Campus-Core besteht aus zwei Layer-3-Geräten mit der Bezeichnung CB-1 und CB-2. Die Serverkomponente befindet sich im unteren Bereich der Abbildung und verfügt über zwei Layer-3-Router mit der Bezeichnung SD-1 und SD-2. Die anderen Geräte im Serverblock sind Layer-2-Geräte. Oben links befindet sich ein Standardzugriffsblock mit zwei Layer-3-Verteilungsgeräten mit der Bezeichnung dl-1 und dl-2. Die übrigen Geräte sind Layer-2-Switches. In diesem Client-Zugriffsblock wird die Zeit mit der Broadcast-Option verteilt. Oben rechts befindet sich ein weiterer Standardzugriffsblock, der eine Client/Server-Zeitverteilungskonfiguration verwendet.

Die Campus-Backbone-Geräte werden in einem Client/Server-Modell mit den Area-Time-Servern synchronisiert.

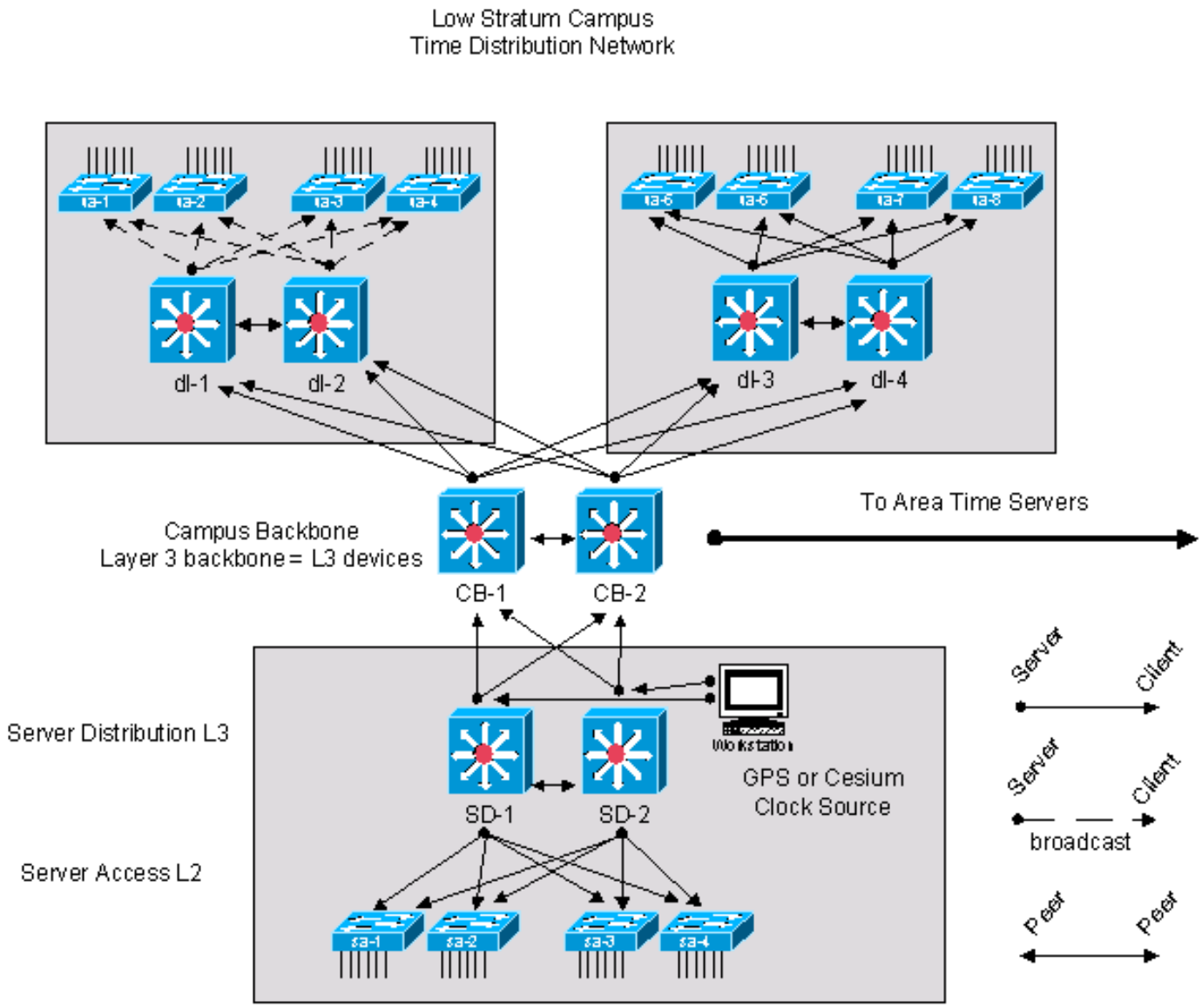
Dies ist die Konfiguration für die Layer-3-Verteilungsgeräte von dl-1:

```
!--- In this case, dl-1 can be a broadcast server
!--- for the Layer 2 LAN. internet Ethernet0 ntp broadcast clock timezone CST -5 clock summer-
time CDT recurring !--- When the system sends an NTP packet, the
!--- source IP address is normally set to the
!--- address of the interface through which the
!--- NTP packet is sent.
!--- Change this to use loopback0. ntp source Loopback0 !--- Enables NTP authentication. ntp
authenticate ntp authentication-key 1234 md5 104D000A0618 7 ntp trusted-key 1234 !--- Configures
the access control groups for
!--- the public servers and peers for
!--- additional security. access-list 5 permit <CB-1> access-list 5 permit <CB-2> access-list 5
permit <dl-2> access-list 5 deny any !--- Restricts the IP addresses for the peers
!--- and clients. ntp access-group peer 5 !--- Fault tolerant configuration polling 2
!--- local time servers and 1 local peer. ntp server <CB-1> ntp server <CB-2> ntp peer <dl-2>
```

Campus-Zeitverteilungsnetzwerk mit niedriger Schicht

Im folgenden Diagramm wird eine GPS- oder Cäsium-Zeitquelle im zentralen Rechenzentrum für das Campus-Netzwerk der unteren Schicht bereitgestellt. Dadurch wird eine Schicht-1-Zeitquelle im privaten Netzwerk bereitgestellt. Wenn sich im privaten Netzwerk mehrere GPS- oder Cäsium-Zeitquellen befinden, muss die Zeitverteilung im privaten Netzwerk geändert werden, um die verfügbaren Zeitquellen zu nutzen.

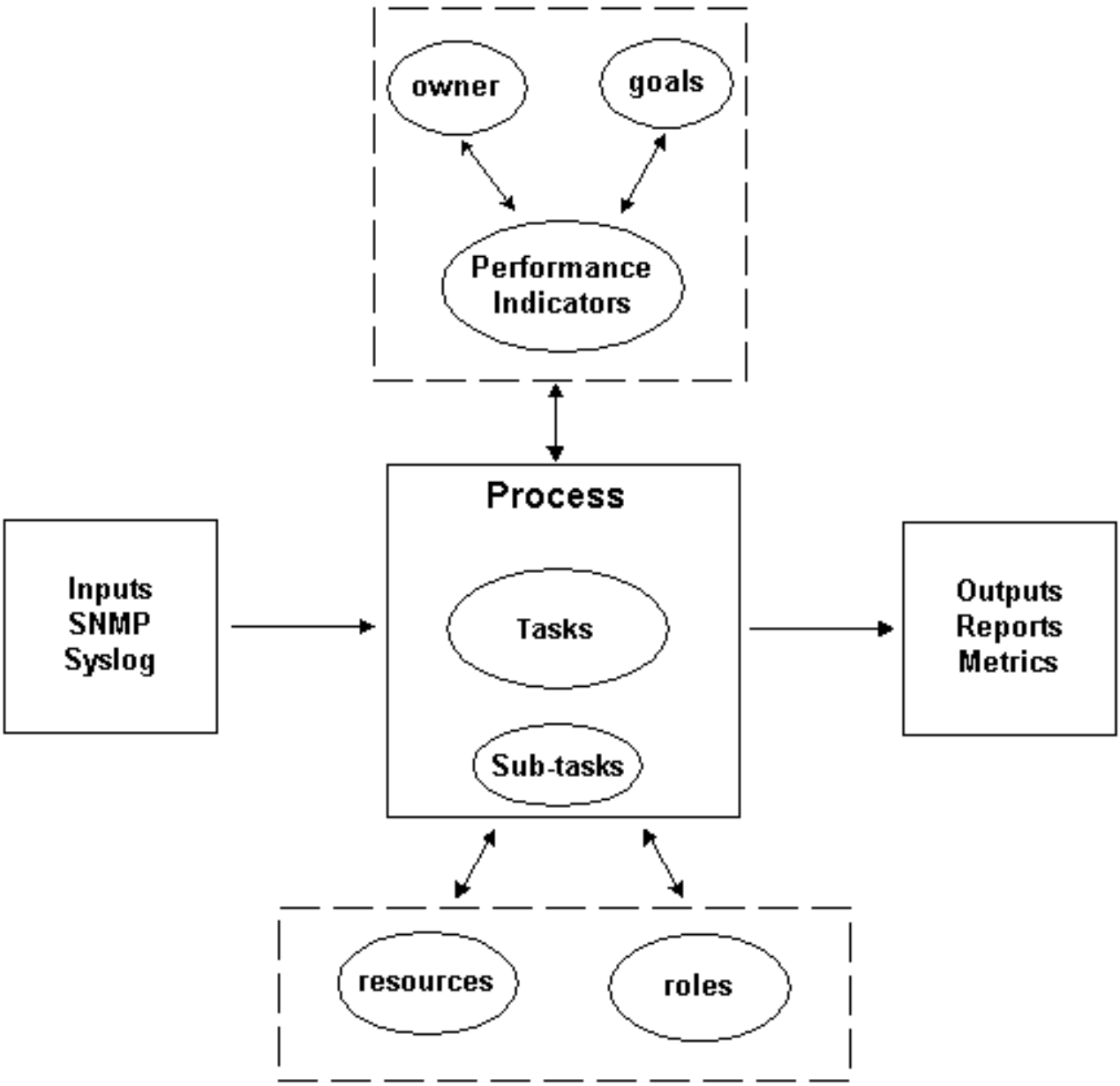
Im Allgemeinen gelten die gleichen Prinzipien und Konfigurationen wie in den vorherigen Beispielen. Der Hauptunterschied besteht in diesem Fall darin, dass der Stamm des Synchronisationsbaums eine private Zeitquelle und keine öffentliche Zeitquelle aus dem Internet ist. Dadurch wird das Design des Zeitverteilungsnetzwerks geändert, um die Vorteile der hochpräzisen privaten Zeitquelle zu nutzen. Die private Zeitquelle ist über das private Netzwerk verteilt, wobei die in den vorherigen Abschnitten beschriebenen Prinzipien der Hierarchie und Modularität beachtet werden.



Campus-Zeitverteilungsnetzwerk mit niedriger Schicht

Prozessdefinitionen

Eine Prozessdefinition ist eine verbundene Reihe von Aktionen, Aktivitäten und Änderungen, die von Agenten ausgeführt werden, die einen Zweck erfüllen oder ein Ziel erreichen möchten. Prozesssteuerung ist der Prozess der Planung und Regelung mit dem Ziel, einen Prozess effektiv und effizient durchzuführen. Dies wird im nächsten Diagramm veranschaulicht.



Reihe von Prozessen

Die Ergebnisse des Prozesses müssen den betrieblichen Normen entsprechen, die von einer Organisation definiert werden und auf den Geschäftszielen basieren. Wenn der Prozess den festgelegten Normen entspricht, wird er als effektiv betrachtet, da er wiederholt, gemessen und verwaltet werden kann und zur Erreichung der Geschäftsziele beiträgt. Wenn die Aktivitäten mit einem minimalen Aufwand durchgeführt werden, wird das Verfahren ebenfalls als effizient angesehen.

Prozesseigentümer

Prozesse umfassen verschiedene organisatorische Grenzen. Daher ist es wichtig, dass nur ein Prozesseigentümer für die Definition des Prozesses verantwortlich ist. Der Verantwortliche ist der zentrale Ansprechpartner, der feststellt und meldet, ob der Prozess effektiv und effizient ist. Wenn der Prozess nicht effektiv oder effizient ist, wird die Änderung des Prozesses vom Prozesseigner durchgeführt. Die Änderung des Prozesses wird durch Änderungskontroll- und Überprüfungsprozesse geregelt.

Ziele des Prozesses

Es werden Prozessziele festgelegt, um die Richtung und den Umfang für die Prozessdefinition festzulegen. Ziele werden auch verwendet, um Metriken zu definieren, mit denen die Effektivität eines Prozesses gemessen wird.

Ziel dieses Prozesses ist es, Kriterien bereitzustellen, die während der NTP-Entwurfsphase dokumentiert werden müssen, und eine Prüffunktion für eine bereitgestellte NTP-Architektur bereitzustellen, um die langfristige Konformität mit dem beabsichtigten Design sicherzustellen.

Leistungsindikatoren für Prozesse

Anhand von Prozessleistungsindikatoren wird die Effektivität der Prozessdefinition gemessen. Die Leistungsindikatoren müssen messbar und quantifizierbar sein. Die als Nächstes aufgeführten Leistungsindikatoren sind beispielsweise entweder numerisch oder werden nach Zeit gemessen.

- Die zum Durchlaufen des gesamten Prozesses erforderliche Zeitdauer.
- Die Häufigkeit der Ausführung, die erforderlich ist, um NTP-Probleme proaktiv zu erkennen, bevor sie sich auf die Benutzer auswirken.
- Die Netzwerkauslastung, die mit der Ausführung des Prozesses verbunden ist.
- Die Anzahl der vom Prozess empfohlenen Korrekturmaßnahmen
- Die Anzahl der Korrekturmaßnahmen, die als Ergebnis des Prozesses durchgeführt wurden.
- Der Zeitraum, der für die Durchführung von Korrekturmaßnahmen benötigt wird.
- Der Rückstand bei den Korrekturmaßnahmen.
- Die Fehler bei der Fehlerbehebung oder Problemdiagnose werden auf NTP-bezogene Probleme zurückgeführt.
- Die Anzahl der in der Seed-Datei hinzugefügten, entfernten oder geänderten Elemente. Dies ist ein Zeichen für Genauigkeit und Stabilität.

Eingaben verarbeiten

Prozesseingaben werden verwendet, um Kriterien und Voraussetzungen für einen Prozess zu definieren. Die Identifizierung von Prozesseingaben liefert häufig Informationen zu externen Abhängigkeiten. Als Nächstes wird eine Liste der Eingaben für das NTP-Management bereitgestellt.

- NTP-Designdokumentation
- Durch SNMP Polling erfasste NTP-MIB-Daten

Prozessausgaben

Die Prozessausgaben werden wie folgt definiert:

- NTP-Konfigurationsberichte, die im Abschnitt "Datenpräsentation" dieses Dokuments definiert sind
- NTP-Korrekturmaßnahmen

Aufgabendefinitionen

In den nächsten Abschnitten werden die Initialisierungs- und iterativen Aufgaben im Zusammenhang mit der NTP-Verwaltung definiert.

Initialisierungsaufgaben

Initialisierungsaufgaben werden während der Implementierung des Prozesses einmal ausgeführt und dürfen nicht während jeder Iteration des Prozesses ausgeführt werden.

Erstellen des NTP-Designs

Wenn Sie erforderliche Aufgaben überprüfen und feststellen, dass eine der Aufgaben nicht implementiert ist oder keine ausreichenden Informationen liefert, um die Anforderungen dieses Verfahrens effektiv zu erfüllen, muss diese Tatsache vom Prozesseigner dokumentiert und dem Management vorgelegt werden. In der nächsten Tabelle sind die erforderlichen Initialisierungsaufgaben aufgeführt.

Erforderliche Aufgabe	Beschreibung
Aufgabenziele	Erstellung eines detaillierten Designdokuments für die NTP-Architektur, das den Designanforderungen und Kostenzielen entspricht
Task-Eingaben	• Technische und wirtschaftliche Anforderungen entwerfen • Derzeitige Netzwerkdesign-Dokumentation • Kriterien, die die im Design aufzuzeichnenden Aspekte definieren, um Managementfunktionen zu ermöglichen • Informationen zur Bereitstellung von IT-Anwendungen • Anforderungen an die Leistungsüberwachung
Aufgabenausgabe	NTP-Designdokumentation.
Aufgabenressourcen	Netzwerktechniker, Architekt für den Netzwerkbetrieb.
Aufgabenrollen	Technische Genehmigung des Netzwerkdesigns durch Prüfer für Technologie und Betrieb; Genehmigung der Netzwerkdesignkosten durch den zuständigen Budgetmanager

Seed-Datei erstellen

Für den NTP-Managementprozess muss eine Seed-Datei verwendet werden, damit keine Netzwerkerkennungsfunktion mehr erforderlich ist. Die Seed-Datei zeichnet die durch den NTP-Prozess gesteuerten Router auf und dient als zentrale Stelle für die Koordination mit den Change-Management-Prozessen in einer Organisation. Wenn beispielsweise neue Knoten in das Netzwerk eingegeben werden, müssen sie der NTP-Seed-Datei hinzugefügt werden. Wenn die SNMP-Community-Namen aufgrund von Sicherheitsanforderungen geändert werden, müssen diese Änderungen in der Seed-Datei übernommen werden. In der nächsten Tabelle wird beschrieben, wie Sie eine Seed-Datei erstellen.

Erforderliche Aufgabe	Beschreibung
Aufgabenziele	Erstellen Sie eine Seed-Datei, die drei Kategorien von Netzwerkgeräten identifiziert: 1. Kritische Geräte - Häufig gestellte Fragen zu Konfigurationsinformationen 2. Interessante Geräte - seltener Polling 3. Alle NTP-fähigen Geräte - Abruf der geringsten Menge
Task-Eingaben	NTP-Design-Dokumentation Netzwerktopologie-Dokumentation.

Aufgabenausgabe	Seed-Datei
Aufgabenressourcen	Designkriterien, anhand derer die an der NTP-Architektur beteiligten Knoten identifiz und priorisiert werden können

Grundlegende NTP-Leistungsparameter

Einige der für die Überwachung des NTP-Netzwerks verfügbaren Parameter weisen einige normale erwartete Schwankungen auf. Der Baselining-Prozess wird verwendet, um die normalen erwarteten Schwankungen zu charakterisieren und Schwellenwerte festzulegen, die unerwartete oder abnormale Bedingungen definieren. Mit dieser Aufgabe wird die Baseline für den variablen Parametersatz für die NTP-Architektur erstellt. Eine ausführlichere Erläuterung der Baselining-Techniken finden Sie im Whitepaper Baseline Process: Best Practice.

Prozess	Beschreibung
Aufgabenziele	Baseline-Variablenparameter
Task-Eingaben	Identifizieren variabler Parameter cntpSysRootDelay cntpSysRootDispersion cntpPeersRootDelay cntpPeersRootDispersion cntpPeersOffset cntpPeersDelay cntpPeersDispersion.
Task-Ausgaben	Basiswerte und Schwellenwerte.
Aufgabenressourcen	Tools, die SNMP-Daten erfassen und Basislinien berechnen.
Aufgabenrolle	Netzwerktechniker, NMS-Techniker.

Iterative Aufgaben

Iterative Tasks werden während jeder Iteration des Prozesses ausgeführt und deren Häufigkeit bestimmt und modifiziert, um die Leistungsindikatoren zu verbessern.

Seed-Datei verwalten

Die Seed-Datei ist für die effektive Implementierung des NTP-Managementprozesses von entscheidender Bedeutung. Daher muss der aktuelle Status der Seed-Datei aktiv verwaltet werden. Netzwerkänderungen, die sich auf den Inhalt der Seed-Datei auswirken, müssen vom NTP-Verwaltungsprozesseigentümer nachverfolgt werden.

Prozess	Beschreibung
Aufgabenziele	Beibehaltung der Genauigkeit der Seed-Datei
Task-Eingaben	Informationen zu Netzwerkänderungen
Task-Ausgaben	Startdatei
Aufgabenressourcen	Berichte, Benachrichtigungen, Meetings, die Änderungen betreffen
Aufgabenrolle	Netzwerktechniker - NMS-Techniker

NTP-Knotenscan durchführen

Sammeln Sie Informationen zu kritischen, interessanten und Konfigurations-Scans, die durch dieses Verfahren definiert werden. Führen Sie diese drei Scans mit unterschiedlichen Frequenzen aus.

Kritische Knoten sind Geräte, die als sehr wichtig für die Leistungs-Datensammlungspunkte angesehen werden. Der kritische Knotenscan wird häufig, z.B. stündlich oder bedarfsgesteuert vor und nach Änderungen durchgeführt. Interessante Knoten sind Geräte, die für die Gesamtintegrität der NTP-Architektur als wichtig erachtet werden, jedoch nicht in den Zeitsynchronisierungsbaum

für die Erfassung kritischer Leistungsdaten aufgenommen werden können. Dieser Bericht wird periodisch, z.B. täglich oder monatlich, ausgeführt. Der Konfigurationsbericht ist ein umfassender und ressourcenintensiver Bericht, mit dem die gesamte NTP-Bereitstellungskonfiguration anhand von Design-Datensätzen charakterisiert wird. Dieser Bericht wird seltener erstellt, z. B. monatlich oder vierteljährlich. Ein wichtiger Punkt ist, dass die Häufigkeit der Berichterstellung an die beobachtete Stabilität der NTP-Architektur und die geschäftlichen Anforderungen angepasst werden kann.

Prozess	Beschreibung
Aufgabenziel	Überwachen der NTP-Architektur
Task-Eingabe	Netzwerkgerätedaten
Aufgabenausgabe	Berichte
Aufgabenressourcen	Softwareanwendungen zur Datenerfassung und Berichterstellung
Aufgabenrolle	Netzwerktechniker

NTP-Knotenberichte überprüfen

Für diese Aufgabe müssen kritische, interessante und Konfigurationsberichte geprüft und analysiert werden. Wenn Probleme erkannt werden, müssen Korrekturmaßnahmen eingeleitet werden.

Prozess	Beschreibung
Task-Eingaben	Scannen von Berichten
Task-Ausgaben	Stabilitätsanalyse Korrekturmaßnahmen
Aufgabenressourcen	Zugriff auf Netzwerkgeräte für weitere Untersuchungen und Verifizierungen
Aufgabenrolle	Netzwerktechniker

Datenidentifizierung

Allgemeine Dateneigenschaften

In der nächsten Tabelle werden Daten beschrieben, die bei der Analyse der NTP-Architektur als wichtig erachtet werden.

Daten	Beschreibung
Knoten-ID	Ein Gerät mit konfiguriertem NTP
Peers	Die konfigurierten Peers für das Gerät
Synchronisierungsquelle	Der ausgewählte Peer für die Synchronisierung
NTP-Konfigurationsdaten	Parameter zur Beurteilung der Konsistenz des NTP-Designs
NTP-Qualitätsdaten	Parameter zur Charakterisierung der Qualität der NTP-Verbindungen

SNMP-Datenidentifizierung

Cisco NTP MIB-Systemgruppe

Die NTP-SNMP-Daten werden von Cisco-NTP-MIB definiert. Aktuelle Informationen zu den Versionen, die diese MIB unterstützen, finden Sie im CCO Feature Navigator. Wählen Sie dort die Option MIB Locator (MIB-Locator). Der Zugriff auf dieses Tool erfolgt über die Seite "TAC Tools for Voice, Telefony and Messaging Technologies" (TAC-Tools für Sprach-, Telefonie- und Messaging-Technologien).

Die Systemgruppe in der Cisco NTP MIB stellt Informationen für den Zielknoten bereit, auf dem NTP ausgeführt wird. Der Zielknoten ist das Ziel der SNMP-Abfragen.

Objektname	Objektbeschreibung
cntpSysStratum	Schicht der lokalen Uhr. Wenn der Wert auf 1 (eine primäre Referenz) festgelegt wird die in Abschnitt 3.4.6 in RFC-1305 beschriebene Primary-Clock-Prozedur ausgeführt. wird aufgerufen. ::= { cntpSystem 2 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.1.
cntpSysPrecision	Vorzeichenbehaftete Ganzzahl, die die Genauigkeit der Systemuhr in Sekunden zur nächsten Potenz von zwei angibt. Der Wert muss auf die nächstgrößere Pote von zwei gerundet werden. Beispielsweise wird einem 50-Hz- (20 ms) oder 60-Hz (16,67 ms) Hochfrequenztakt der Wert -5 (31,25 ms), während einem 1000-Hz- (Kristalltakt der Wert -9 (1,95 ms) zugeordnet wird. ::= { cntpSystem 3 } Objektken = .1.3.6.1.4.1.9.9.168.1.1.3
cntpSysRootDelay	Eine mit Vorzeichen versehene Festpunktzahl, die die gesamte Round-Trip-Verzögerung in Sekunden an die primäre Referenzquelle im Stamm des Synchronisierungs-Subnetzes angibt. ::= { cntpSystem 4 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRootDispersion	Der maximale Fehler in Sekunden, relativ zur primären Referenzquelle im Stamm Synchronisierungs-Subnetzes. Es sind nur positive Werte größer Null möglich. ::= cntpSystem 5 } Objektkennung = .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysReferenzzeit	Die lokale Zeit, zu der die lokale Uhr zuletzt aktualisiert wurde. Wenn die lokale U noch nie synchronisiert wurde, ist der Wert Null. ::= { cntpSystem 7 } Objektkennu .1.3.6.1.4.1.9.9.168.1.1.7
cntpSysPeer	Die aktuelle Synchronisierungsquelle, die den eindeutigen Zuordnungsbezeichne cntpPeersAssocId des entsprechenden Peereintrags in der cntpPeersVarTable d Peers enthält, der als Synchronisierungsquelle fungiert. Wenn kein Peer vorhand ist der Wert 0. ::= { cntpSystem 9 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.1.9
cntpSystemuhr	Die aktuelle Ortszeit Die Ortszeit wird aus der Hardware-Uhr der jeweiligen Masc abgeleitet und erhöht sich in Intervallen, je nach verwendetem Design. ::= { cntpSystem 10 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.1.10

Cisco NTP MIB-Peer-Gruppe - Tabelle mit Peers-Variablen

Die Peer-Gruppe der Cisco NTP MIB stellt Informationen zu den Peers des Zielknotens bereit.

Objektname	Objektbeschreibung
cntpPeersVarTabelle	Diese Tabelle enthält Informationen zu den Peers, denen der lokale NTP-Serve zugeordnet ist. Die Peers sind auch NTP-Server, die auf verschiedenen Hosts ausgeführt werden. Dies ist eine Tabelle mit cntpPeersVarEntry ::= { cntpPeers Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1
cntpPeersVarEintrag	Jeder Peer-Eintrag enthält NTP-Informationen, die von einem bestimmten Peer NTP-Server abgerufen werden. Jeder Peer wird durch eine eindeutige Zuordnu ID identifiziert. Einträge werden automatisch erstellt, wenn der Benutzer den NT Server so konfiguriert, dass er Remote-Peers zugeordnet wird. Ebenso werden Einträge gelöscht, wenn der Benutzer die Peer-Zuordnung vom NTP-Server en Einträge können auch von der Verwaltungsstation erstellt werden, indem Werte cntpPeersPeerAddress, cntpPeersHostAddress, cntpPeersMode festgelegt we und cntpPeersEntryStatus als aktiv (1) festgelegt wird. Zumindest muss die Verwaltungsstation einen Wert für "cntpPeersPeerAddress" festlegen, um die Z zu aktivieren. INDEX { cntpPeersAssocId } ::= { cntpPeersVarTable 1 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1
cntpPeersAssocID	Eine Ganzzahl größer als Null, die einen Peer eindeutig identifiziert, dem der lo

	NTP-Server zugeordnet ist. ::= { cntpPeersVarEntry 1 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.1
cntpPeersKonfiguriert	Dies ist ein Hinweis darauf, dass die Verknüpfung aus Konfigurationsinformatio erstellt wurde und nicht getrennt werden darf, auch wenn der Peer nicht erreich ist. ::= { cntpPeersVarEntry 2 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.
cntpPeersPeerAdresse	Die IP-Adresse des Peers. Wenn eine neue Zuordnung erstellt wird, muss ein W für dieses Objekt festgelegt werden, bevor die Zeile aktiviert wird. ::= { cntpPeersVarEntry 3 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.3
cntpPeersModus	SYNTAX INTEGER { unspecified (0), symmetricActive (1), symmetricPassive (2 client (3), server (4), broadcast (5), reservedControl (6), reservedPrivate (7) } W eine neue Peer-Zuordnung erstellt wird und kein Wert für dieses Objekt angege wird, wird standardmäßig symmetricActive (1) verwendet. ::= { cntpPeers VarEn } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1.1.8
cntpPeersSchicht	Die Schicht der Peer-Uhr ::= { cntpPeersVarEntry 9 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.9
cntpPeersRootDelay	Eine mit Vorzeichen versehene Festpunktzahl, die die gesamte Round-Trip-Verzögerung in Sekunden angibt, vom Peer zur primären Referenzquelle im St des Synchronisierungs-Subnetzes. ::= { cntpPeersVarEntry 13 } Objektbezeichn .1.3.6.1.4.1.9.9.168.1.2.1.1.13
cntpPeersRootDispersion	Der maximale Fehler (in Sekunden) der Peer-Uhr relativ zur primären Referenzquelle im Root des Synchronisierungs-Subnetzes. Es sind nur positive Werte größer Null möglich. ::= { cntpPeersVarEntry 14 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.14
cntpPeersRefZeit	Die lokale Zeit am Peer, als die Uhr zuletzt aktualisiert wurde. Wenn die Peer-U noch nie synchronisiert wurde, ist der Wert Null. ::= { cntpPeersVarEntry 16 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.16
cntpPeersReichweite	Ein Schieberegister, das zur Bestimmung des Erreichbarkeitsstatus des Peers verwendet wird, mit Bits, die vom Ende mit der geringsten Bedeutung (ganz rec eingehen. Ein Peer gilt als erreichbar, wenn mindestens ein Bit in diesem Regis auf Eins gesetzt ist (Objekt ist ungleich null). Die Daten im Schieberegister wer von den NTP-Protokollprozeduren aufgefüllt. ::= { cntpPeersVarEntry 21 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersOffset	Der geschätzte Offset der Peer-Uhr relativ zur lokalen Uhr in Sekunden. Der Ho bestimmt den Wert dieses Objekts, das den NTP-Taktfilteralgorithmus verwend ::= { cntpPeersVarEntry 23 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersVerzögerung	Die geschätzte Round-Trip-Verzögerung der Peer-Uhr relativ zur lokalen Uhr ü den Netzwerkpfad zwischen den beiden Geräten in Sekunden. Der Host bestim den Wert dieses Objekts, das den NTP-Taktfilteralgorithmus verwendet. ::= { cntpPeersVarEntry 24 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.24
cntpPeersDispersion	Der geschätzte maximale Fehler der Peer-Uhr im Verhältnis zur lokalen Uhr üb den Netzwerkpfad zwischen den beiden Geräten in Sekunden. Der Host bestim den Wert dieses Objekts, das den NTP-Taktfilteralgorithmus verwendet. ::= { cntpPeersVarEntry 25 } Objektbezeichner = .1.3.6.1.4.1.9.9.168.1.2.1.1.25

Datensammlung

SNMP-Datensammlung

Alle für dieses Verfahren erforderlichen Informationen können über SNMP-Abfragen gesammelt werden. Um die Daten zu analysieren und die Reports zu erstellen, müssen angepasste Skripte oder Softwareprogramme entwickelt werden.

Datenpräsentation

Bericht zu kritischen NTP-Knoten

Kritische Knoten sind Geräte, die im Synchronisierungsbaum ausgewählter Leistungs-Datensammlungspunkte wichtig sind. Wenn ein umsatzstarker VoIP-Service überwacht wird und Kennzahlen für die unidirektionale Verzögerung und Variation erfasst werden, gelten die Quell- und Zielknoten, in denen die Zeitstempel aufgezeichnet werden, als kritische Knoten.

In diesem Beispiel wurde das NTP-Design als Nächstes einer OSPF-Beispielhierarchie festgelegt. Daher werden die nachfolgend beschriebenen Berichte formatiert, um die NTP-Geräte nach dem OSPF-Bereich des Geräts zu gruppieren. In Fällen, in denen ein Knoten Schnittstellen in mehreren Bereichen aufweist, muss von der Berichterstellungssoftware entschieden werden, in welchem Bereich der Knoten zu Berichtszwecken aufgeführt werden kann. Wie bereits erwähnt, ist OSPF keine Voraussetzung für NTP. Es wird in diesem Dokument nur als anschauliches Beispiel verwendet.

Bereich	"Slot0:"	Gerätedaten	Wert
AreaId #n	Geräte-ID #1	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysReferenzzeit	
		cntpSysPeer	
		cntpSystemuhr	
	Geräte-ID #n	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysReferenzzeit	
		cntpSysPeer	
		cntpSystemuhr	

NTP-Bericht zu interessanten Knoten

Das Format des interessanten Knotenberichts entspricht dem Format für den kritischen Knotenbericht. Interessante Knoten sind Knoten, die für die allgemeine NTP-Architektur wichtig sind, aber nicht direkt zur Zeitsynchronisierung wichtiger Performance-Überwachungspunkte beitragen können.

NTP-Konfigurationsbericht

Der Konfigurationsbericht ist ein umfassender Bericht, der Informationen über die gesamte NTP-Architektur erfasst. Dieser Bericht wird verwendet, um die NTP-Bereitstellung anhand der Design-Datensätze aufzuzeichnen und zu überprüfen.

Bereich	"Slot0:"	Peer	Peer-Daten	Wert
AreaId #n	Geräte-ID #n	Peer-ID #1	cntpPeersAssocID	
			cntpPeersKonfiguriert	
			cntpPeersPeerAdresse	
			cntpPeersModus	

Peer-ID #n	cntpPeersSchicht cntpPeersRootDelay cntpPeersRootDispersion cntpPeersRefZeit cntpPeersReichweite cntpPeersOffset cntpPeersVerzögerung cntpPeersDispersion cntpPeersAssocID cntpPeersKonfiguriert cntpPeersPeerAdresse cntpPeersModus cntpPeersSchicht cntpPeersRootDelay cntpPeersRootDispersion cntpPeersRefZeit cntpPeersReichweite cntpPeersOffset cntpPeersVerzögerung cntpPeersDispersion

Zugehörige Informationen

- RFC 1305 Network Time Protocol
- RFC 2330-Framework für IP-Leistungsmetriken
- Grundlegende Cisco IOS-Funktionen v2.84 für jeden ISP
- Technischer Support – Cisco Systems

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.