Network Time Protocol： ベスト プラクティスのホワイト ペーパー

目次

概要

Internet Protocol（IP）ベースのネットワークは、従来の「**ベスト エフォート**」配信モデルから、パフォーマンスおよび信頼性の定量化を必要とするモデルへと急速に進化しつつあり、多くの場合、それらは Service Level Agreements（SLA; サービス レベル契約）によって保証されています。 その結果、ネットワークの各種指標をより詳細に把握することが必要になり、ネットワーク動作の特性を表すメトリックや測定機能の定義を目的とした研究活動が盛んに行われています。中でも、時間の測定は、さまざまな測定方式の基礎になっています。

背景説明

現在のパフォーマンス分析で必要とされる水準までネットワーク タイムを同期させることは、必要不可欠の作業です。 ビジネス モデルや提供するサービスによっては、ネットワーク パフォーマンスの特性が競合サービスとの差別化を図る上で重要なポイントになると考えられます。 そのようなケースでは、ネットワーク管理システムを導入し、技術部門のリソースをパフォーマンス データの収集に充てるのに、多額の費用が必要になる場合があります。 ただし、しばしば見過ごされがちである時間の同期の原則に十分な注意を払わなければ、そのような努力も無駄になる可能性があります。

このドキュメントでは、Network Time Protocol（NTP）のネットワーク管理機能を実行するための仮定的なプロセスの定義について説明しています。 この仮定的手順は参考例であり、各組織の目的に合せてカスタマイズされることを想定しています。

このドキュメントの情報は、次のセクションに分けて記載されています。

「用語」の項では、時間の同期に関する用語の一般的な定義について説明しています。

「概要」の項では、システム タイムに関係するネットワーク要素ハードウェアの背景情報、NTP の技術的概要、NTP アーキテクチャの設計に関する主な側面について説明しています。

「NTP の展開例」の項では、WAN、上位ストラタム キャンパス、および下位ストラタム キャンパス時間配信ネットワークのサンプル構成を使用して、NTP の展開例を示しています。

「プロセス定義」の項では、NTP 管理を実現するために使用するプロセス定義の概要について説明しています。 プロセスの詳細は、目標、パフォーマンス インジケータ、入力、出力、および個々のタスクの観点から説明されています。

「タスク定義」の項では、プロセス タスク定義について詳しく説明しています。 タスクごとに、目的、タスクの入力、タスクの出力、タスクの実行に必要なリソース、およびタスクの実行に必要なジョブ スキルについて説明しています。

「データの識別」の項では、NTP データの識別について説明しています。 データの識別では、情報のソースが考慮されます。 情報は、Simple Network Management Protocol（SNMP）管理情報ベース（MIB）や、Syslog によって生成されるログ ファイルや、コマンド ライン インターフェイス（CLI）からのみアクセスできる内部データ構造内などに格納されています。

「データの収集」の項では、NTP データの収集について説明しています。 データ収集は、データの場所と密接な関係があります。 たとえば、SNMP MIB データは、トラップ、Remote Monitoring（RMON; リモート モニタリング）のアラームやイベント、またはポーリングなど、いくつかのメカニズムで収集されます。 内部データ構造内に格納されているデータは、自動スクリプトによって収集される場合と、ユーザが手動でシステムにログインして CLI コマンドを発行し、その出力を記録することによって収集される場合があります。

「データ表示」の項では、データの表示方法を示すために、レポート形式の例を示しています。

用語

- **Accuracy**：オフセット ゼロに対するクロックの絶対値の近接度。
- **Accurate**：特定の時点でクロックのオフセットがゼロである状態。
- **Drift**：歪みの変化量、またはクロックのオフセットを時間で 2 階微分した値。
- **Joint resolution**：2 つのクロックを比較する際の、C1 と C2 の精度の合計。 その場合、Joint resolution は、一方のクロックによって生成されたタイム スタンプを他方のクロックによって生成されたタイム スタンプから差し引くことによって計算された時間間隔の精度に対する安全を見込んだ下限を示す。
- **Node**：ローカル プロセッサにおける NTP プロトコルのインスタンスのこと。 ノードは、デバイスと呼ばれる場合もある。
- **Offset**：クロックによって報告される時間と、Coordinated Universal Time（UTC）で定義される真の時間との差異。 クロックによって報告された時間が Tc で、真の時間が Tt である場合、そのクロックのオフセットは Tc - Tt で求めることができる。
- **Peer**：ローカル ノードからのネットワーク パスによって接続されているリモート プロセッサにおける NTP プロトコルのインスタンスのこと。
- **Relative offset**：2 つのクロック C1 と C2 を比較する際に、真の時間をクロック C1 によって報告された時間と置き換えること。 たとえば、特定時点でのクロック C1 に対する C2 の相対オフセットは Tc2 - Tc1（C2 と C1 によって報告される時間の瞬時的差異）になる。
- **Resolution**：クロックの時間を更新する最小の単位。 分解能は秒単位で定義される。 ただし、分解能は、真の時間ではなく、クロックによって報告された時間を基準とする。 たとえば、分解能 10 ms は、そのクロックが 0.01 秒単位で更新されることを意味するが、その値は更新間隔の真の時間量を示していない。**注:** 非常に高い分解能を持つクロックでも、正確ではない場合があります。
- **Skew**：クロックの周波数の差異、またはオフセットを時間で 1 階微分した値。
- **Synchronize**：2 つのクロックが相互の関係において正確である場合（相対オフセットがゼロの場合）、それらのクロックは同期している。 クロックが同期されていても、真の時間との関係において正確でない場合がある。

概要

デバイスの概要

タイム サービスの中心となるのは、システム クロックです。 システム クロックは、システムが起動された瞬間から稼働し、現在の日時を追跡し続けます。 システム クロックは、さまざなまソースによって設定され、さまざまなメカニズムを通じて他のシステムに現在の時間を配信するために使用されます。 一部のルータには、バッテリ駆動式のカレンダ システムが内蔵されており、システムの再起動時や停電時にも日時が追跡されます。 システムの再起動時には、システム クロックを初期化するために、このカレンダ システムが必ず使用されます。 また、このシステムは、信頼できるタイム ソースの 1 つと見なされ、他のソースを使用できない場合は、NTP を通じて再配信されます。 NTP が稼働している場合は、このカレンダを NTP に基づいて定期的に更新できるため、カレンダ時間のドリフトを補正することができます。 システム カレンダ内蔵のルータを初期化すると、バッテリ駆動式の内部カレンダの時間に基づいてシステム クロックが設定されます。 カレンダが内蔵されていないモデルの場合は、事前に定義された時定数にシステム クロックが設定されます。 システム クロックは、次のソースから設定できます。

- NTP
- Simple Network Time Protocol（SNTP）

- Virtual Integrated Network Service（VINES）タイム サービス
- 手動設定

Cisco のローエンド デバイスの中には SNTP しかサポートしていないものがあります。 SNTP は、NTP をクライアントのみに限定して簡略化したバージョンです。 SNTP では、NTP サーバからの時間の受信のみを実行でき、他のシステムにタイム サービスを提供することはできません。一般的に、SNTP によって配信される時間の正確度は 100 ms 以内です。 また、SNTP では、拡張アクセス リストの設定である程度の安全性を確保することはできますが、トラフィックの認証は行われません。 SNTP クライアントは NTP クライアントよりも不正なサーバに対して脆弱であるため、強力な認証が必要でない場合にのみ使用することを推奨いたします。

システム クロックは、次のサービスに対して時間を配信します。

- NTP
- VINES タイム サービス
- ユーザの **show コマンド**
- メッセージのロギングおよびデバッグ

システム クロックは、UTC を基準として内部的に時間を追跡します。UTC はグリニッジ標準時（GMT）とも呼ばれます。 ローカル タイム ゾーンと夏時間に関する情報を設定すると、ローカル タイム ゾーンとの関係において正しく時間を表示させることができます。 システム クロックは、信頼できるかどうかにかかわらず、時間を追跡します。 信頼できない時間は表示の目的のみに使用され、再配信は行われません。

NTP の概要

NTP は、マシンのネットワーク上で時間を同期することを目的としたプロトコルです。 NTP は、User Datagram Protocol（UDP）上で動作し（ポート 123 を送信元および送信先として使用）、そして UDP は IP 上で動作します。 NTP バージョン 3 RFC 1305 は、分散されたタイム サーバおよびクライアント間の計時の同期に使用されます。 ネットワーク上のノードの識別および設定は NTP によって行われ、これらのノードは同期サブネット（オーバーレイ ネットワークと呼ばれることもあります）を形成します。 複数のマスター（プライマリ サーバ）を存在させることも可能で、選択プロトコルに関する要件は特にありません。

NTP ネットワークは通常、タイム サーバに接続された電波時計や原子時計などの正規の時刻源から時刻を取得します。 NTP は、この時間をネットワーク全体に配信します。 NTP クライアントは、それぞれのポーリング間隔（64 ~ 1024 秒）でサーバとのトランザクションを行います。この間隔は、NTP サーバとクライアントの間のネットワーク状態によって動的に変化します。 不適切な NTP サーバ（ばらつきが大きい NTP サーバなど）とルータが通信するときは、別の状況となります。 ルータはポーリング間隔を上げます。 2 台のマシンを同期させるために、1 分あたり 2 回以上の NTP トランザクションを実行する必要はありません。 ルータでの NTP ポーリング間隔の調整はできません。

NTP では、信頼できるタイム ソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。 たとえば、ストラタム 1 のタイム サーバに電波時計または原子時計が直接接続されているとします。 このタイム サーバはストラタム 2 のタイム サーバに NTP で時間を配信します。このサーバはさらに別のマシンへ時間を再配信します。 NTP を実行しているマシンは、NTP を使用して通信するように設定されたマシンの内、ストラタム番号が最も低いマシンを自動的に選択し、自身のタイム ソースとして使用します。 この手法により、NTP スピーカの自動編成型ツリーが適切に構築されます。 NTP では、クライアントとタイム サーバの関係において次の 3 つの主要な変数が確実に評価されるため、パケット交換網のパスの長さが不定であっても、十分なパフォーマンスを発揮します。

- ネットワーク遅延
- 時間パケット交換のばらつき：2 つのホストの間の最大クロック誤差の測定値。
- クロック オフセット：クライアントのクロックを同期させるために適用される補正値。

長距離（2000 km）の Wide Area Network（WAN）では 10 ms レベルのクロック同期が定期的に実現され、Local Area Network（LAN）では 1 ms レベルのクロック同期が定期的に実現されます。

NTP は、時間が正確でない可能性があるマシンとの同期を、次の 2 つの方法で回避します。 1 つ目は、それ自身で同期を行わないマシンとの同期を避ける方法です。 2 つ目は、複数のマシンから報告された時間と大幅に時間が異なっているマシンとの同期を避ける方法です。

多くの場合、NTP を実行しているマシン（アソシエーション）の間の通信は、静的に設定されます。 各マシンには、すべてのマシンの IP アドレスが与えられ、それによってアソシエーションが形成されます。 正確な時間は、アソシエーションを持つ 2 台のマシンの間で NTP メッセージを交換することによって可能になりますが、 LAN 環境では、IP ブロードキャスト メッセージを使用するように NTP を設定することもできます。 その場合は、ブロードキャスト メッセージを送受信するように各マシンを設定できるので、設定の複雑さが軽減されます。 ただし、情報のフローが単一方向になるため、時間の精度が若干低くなります。

マシン上で維持される時間は重要なリソースなので、偶然または故意に不正確な時間が設定されることを防ぐために、NTP のセキュリティ機能を使用することを強く推奨いたします。 アクセスリストによる制約と、暗号化認証メカニズムという 2 種類のセキュリティ機能を使用できます。

一部の Cisco IOS ソフトウェア リリースでは、Cisco が提供する NTP 実装によって、ストラタム 1 サービスがサポートされます。 **ntp refclock** コマンドがサポートされているリリースでは、電波時計または原子時計を接続できます。 Cisco IOS の一部のリリースでは、Trimble Palisade NTP Synchronization Kit（Cisco 7200 シリーズのみ）または Telecom Solutions Global Positioning System（GPS）デバイスがサポートされています。 インターネットから分離されたネットワークでインターネット上のパブリック タイム サーバを利用する場合は、Cisco の NTP 実装を使用することで、実際には別の方法で時間が決定されていても、あたかも NTP を通じて同期が行われるかのように特定のマシンを設定することができます。 その後、他のマシンは、NTP によってそのマシンと同期されます。

NTP 設計基準

同期サブネットの各クライアント（上位ストラタム クライアントのサーバも含む）は、同期の対象として使用できるサーバを 1 台選択します。 通常、このサーバは、アクセス可能なサーバの中で最も低いストラタムのサーバから選択されます。 ただし、NTP の動作は、各サーバの時間に一定の誤差があるという前提に基づいているため、この設定は必ずしも最適とは限りません。 NTP は、より低いストラタムにある複数（少なくとも 3 つ）のタイム ソースにアクセスし、一致アルゴリズムを適用していずれかのソースの誤差を検出します。 通常、すべてのサーバの時間が一致した場合は、最も低いストラタムにあり、（ネットワーク遅延の観点で）最も近くに存在し、および報告された精度という観点から、最適なサーバが選択されます。 つまり、各クライアントには、より低いストラタムにある 3 つ以上のタイム ソースを提供する必要があり、その中のいくつはバックアップ サービスのみを提供することになります（それらのソースは、ネットワーク遅延とストラタムの観点から、品質が劣る場合があります）。 たとえば、ローカル サーバが直接アクセスしない下位ストラタムのソースから時間を受信している同じストラタムのピアも、品質の高いバックアップ サービスを提供することができます。

通常、NTP は、下位スタトラム サーバの時間が大幅にずれていなければ、上位スタトラム サーバよりも下位スタトラム サーバを優先します。 このアルゴリズムでは、不正確なクロックが下位

スタトラムのレベルであっても、時刻ソースに大きな誤差があるか狂っていると見なされる場合を検出して、このような状況での同期を防止できます。 また、それ自身で同期されていない他のサーバに対してデバイスが同期されることもありません。

サーバが信頼できるかどうかを宣言するには、次のような健全性チェックをパスする必要があります。

- 監視プログラムがこの情報を長期間更新していない場合にトラップ送信を防止するための健全性タイムアウトが、実装に含まれている。
- 認証、レンジ バウンド、および古いデータの使用防止を目的とした、その他の健全性チェックが含まれている。
- 発振器が参照ソースからの更新を長期間受信していないことを警告するためのチェックが追加されている。
- 深刻なネットワーク輻輳が発生している状態で分散的に発生する大きな遅延によって参照ソースが急速に変更した場合の不安定さを回避するために、peer.valid 変数と sys.hold 変数が追加されている。 特別な機能を制御し、設定を容易にするために、peer.config ビット、peer.authenable ビット、および peer.authentic ビットが追加されています。

これらのチェックを 1 つでもパスできなければ、ルータは不正確であると宣言されます。

アソシエーション モード

以後のセクションでは、NTP サーバを相互に関連付けるために使用するアソシエーション モードについて説明します。

- クライアント/サーバ
- 対称アクティブ/パッシブ
- ブロードキャスト

クライアント/サーバ モード

通常、依存型クライアントとサーバは、クライアント/サーバ モードで動作します。このモードでは、クライアントまたは依存型サーバをグループ メンバに同期させることができますが、グループ メンバをクライアントまたは依存型サーバに同期させることはできません。 これにより、障害やプロトコル攻撃からの保護が実現されます。

クライアント/サーバ モードは、最も一般的なインターネット設定です。 このモードは、ステートレス サーバに対するリモート プロシージャ コール（RPC）という典型的な枠組みの中で動作します。 このモードでは、クライアントがサーバに要求を送信し、将来のある時点で応答が返されることが想定されています。 時には、この動作はポーリング動作として説明されることがあります。この動作では、クライアントがサーバに時間と認証情報を収集します。 クライアントをクライアント モードで設定するには、サーバ コマンドを使用して、ドメイン ネーム サーバ（DNS）の名前またはアドレスを指定します。 サーバ側での事前の設定は必要ありません。

一般的なクライアント/サーバ モデルでは、クライアントが 1 台または複数台のサーバに NTP メッセージを送信し、受信した応答を処理します。 サーバは、アドレスとポートを交換し、メッセージ内の特定のフィールドを上書きし、チェックサムを再計算して、ただちにメッセージを返します。 クライアントは、NTP メッセージに含まれる情報を使用して、サーバの時間とローカルの時間の誤差を確認し、必要に応じてローカル クロックを調整します。 また、このメッセージには、最適なサーバを選択するための情報だけでなく、時間の精度と信頼度を計算するための情報も含まれています。

通常、多数のクライアントに同期を提供するサーバは、相互に冗長の関係を持つ 3 台以上のサーバのグループとして動作します。各サーバは、クライアント/サーバ モードのストラタム 1 または 2 にある 3 台以上のサーバ および対称モードのすべての他のグループメンバと動作します。これにより、1 台またそれ以上のサーバが動作しなくなった場合や、不正確な時間が配信された場合の障害からの保護が実現されます。 偶然または悪意によって不正確な時間が同期ソースの一部から配信された場合の攻撃を避けるために、NTP アルゴリズムは設計されています。 このようなケースでは、不適切なソースを特定して、それらのデータを破棄するために、特別な取捨手順が使用されます。 信頼性を確保するために、特定のホストに外部クロックを搭載して、プライマリ サーバ、セカンダリ サーバ、またはそれらの間のパスに障害が発生した場合のバックアップとして使用することもできます。

クライアント モードでアソシエーションを設定した場合は (通常は設定ファイル内のサーバ宣言で指定されます)、リモート サーバに時間を配信するのではなく、リモート サーバから時間を取得することになります。

対称アクティブ/パッシブ モード

対称アクティブ/パッシブ モードは、低いストラタムにあるピアのグループが相互にバックアップとして機能する構成を目的としています。 各ピアは、1 つ以上のプライマリ リファレンス ソース (電波時計など) または信頼性の高いセカンダリ サーバのサブネットを利用して動作します。いずれかのピアがすべてのリファレンス ソースを失った場合や動作を停止した場合は、まだ機能しているピアから他のすべてのピアに時間値が流れるように、残りのピアが自動的に再設定されます。 場合によっては、この動作は「*プッシュ/プル*」動作として説明されることがあります。この動作では、各ピアがそれぞれの設定に応じて時間および値をプルまたはプッシュします。

対称アクティブ モードでアソシエーションを設定した場合は (通常は設定ファイル内のサーバ宣言で指定されます)、リモート サーバから時間を取得するだけでなく、必要な場合はリモート サーバに時間を配信することになります。 このモードは、さまざまなネットワーク パスを通じて相互接続されている冗長構成のタイム サーバが多数含まれる構成に適しています。現在のインターネットでは、ストラタム 1 およびストラタム 2 にある大半のサーバがこれに該当します。

対称モードは、相互に冗長グループとして機能する 2 台以上のサーバの間で使用されるのが最も一般的です。 これらのモードでは、最大限のパフォーマンスを確保するために、ネットワーク ジッタや伝搬遅延などに応じて、グループ メンバのサーバが同期パスを取り決めます。 1 つまたは複数のグループ メンバに障害が発生した場合は、残りのメンバが必要に応じて自動的に再設定されます。

対称アクティブ モードでピアを設定するには、**peer** コマンドを使用して、他方のピアの DNS 名またはアドレスを指定します。 他方のピアを対称モードで設定する場合も同じ方法になります。

注: 他方のピアがこの方法で明示的に設定されていない場合は、対称アクティブ メッセージが到着すると対称パッシブ アソシエーションが有効になります。 侵入者が対称アクティブ ピアになりすまして虚偽の時間値を送信できないようにするために、対称モードを使用する場合は必ず認証を行ってください。

ブロードキャストまたはマルチキャスト モード

それほど厳密な精度や信頼性を必要としない場合は、ブロードキャスト モードまたはマルチキャスト モードを使用するようにクライアントを設定することができます。 通常、これらのモードは、依存型クライアントに対してサービスを提供するサーバによって使用されます。 このモードの利点は、特定のサーバを使用するようにクライアントを設定する必要がないため、動作中のすべてのクライアントが同じ設定ファイルを使用できる点です。 ブロードキャスト モードを使用する

場合は、同じサブネット上にブロードキャスト サーバが存在している必要があります。 ブロードキャスト メッセージはルータによって伝搬されないため、同じサブネット上のブロードキャスト サーバのみが使用されます。

ブロードキャスト モードは、1 台または数台のサーバと、多数のクライアントが含まれる構成に適しています。 ブロードキャスト サーバを設定するには、**broadcast** コマンドとローカル サブネット アドレスを使用します。 ブロードキャスト クライアントを設定するには、**broadcastclient** コマンドを使用します。これにより、そのブロードキャスト クライアントは、あらゆるインターフェイスで受信したブロードキャスト メッセージに対して応答することが可能になります。 侵入者がブロードキャスト サーバになりすまして虚偽の時間値を送信できないようにするために、このモードを使用する場合は必ず認証を行ってください。

NTP うるう秒（閏秒）の設定

うるう秒を挿入するには、**ntp leap {add | delete}** コマンドを使用できます。 うるう秒の追加と削除はオプションになっています。 これには次の 2 つの制約があります。

- クロックが同期（sync）ステートになっている必要があります。
- このコマンドが受け付けられるのは、うるう秒が発生する前の 1 か月間だけです。 現在の日時が、うるう秒の発生 1 か月前よりもさらに前の場合は、このコマンドではうるう秒は設定されません。

このコマンドを設定すると、次に示すように、最後に設定された秒に対してうるう秒が追加または削除されます。

```
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 occuring 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 アーキテクチャ

NTP アーキテクチャには、次の 3 つの構造があります。

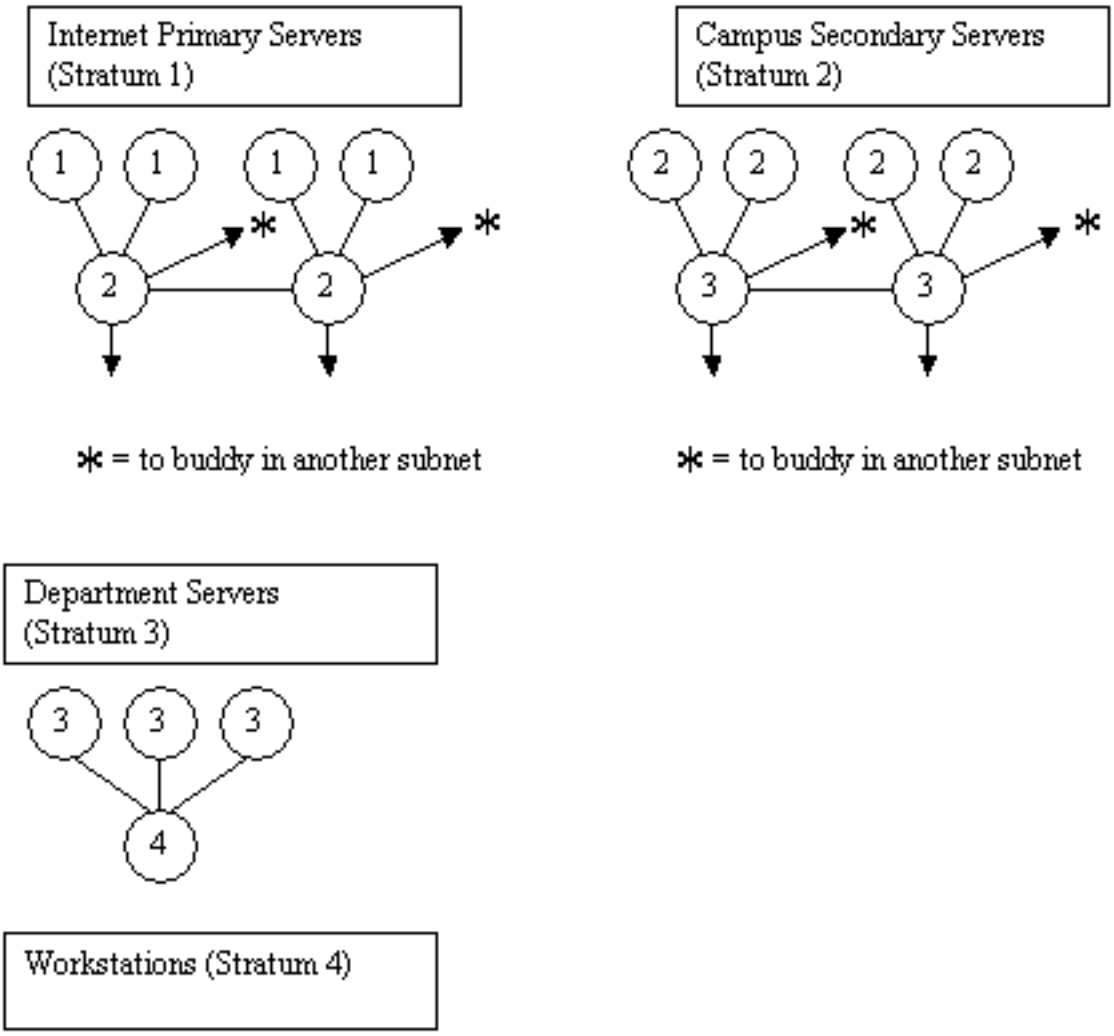
- フラット ピア構造
- 階層型構造
- 星型構造

フラット ピア構造では、すべてのルータが相互に対等な関係にあり、地理的に分離された少数のルータが外部のシステムを参照するように設定されます。 NTP メッシュのメンバが新たに追加されるたびに、コンバージェンス時間が長くなります。

階層型構造では、ルーティング階層が NTP 階層用に複製されます。 コア ルータが外部タイム ソースとクライアント/サーバの関係にあり、内部タイム サーバがコア ルータとクライアント/サーバの関係にあり、内部カスタマ ルータ（非タイム サーバ）が内部タイム サーバとクライアント/サーバの関係にあるという具合に、下へ向かってツリーが形成されます。 これらの関係は、階層スケールと呼ばれます。 階層型構造には、整合性、安定性、およびスケーラビリティがあるため

、望ましい手法と言えます。

下の図が示すように、スケーラブルな NTP アーキテクチャは、階層型構造を持っています。



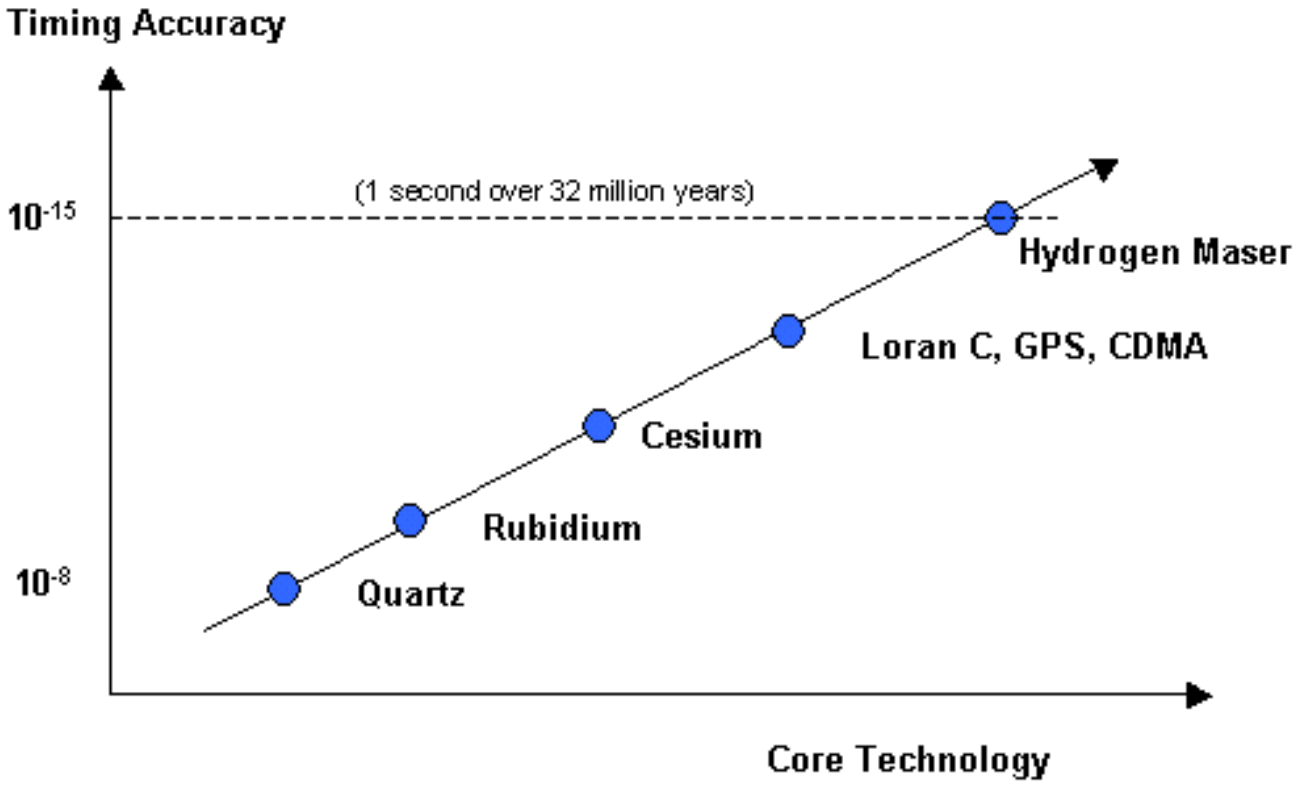
星型構造では、すべてのルータがコアにある少数のタイム サーバとクライアント/サーバの関係にあります。 専用のタイム サーバが星の中心になり、多くの場合は外部のタイム ソースまたはそれぞれぞれの GPS レシーバと同期された UNIX システムが使用されます。

クロック テクノロジーとパブリック タイム サーバ

現在、インターネットの NTP サブネットには、電波、衛星、またはモデムで UTC と直接同期されているパブリック プライマリ サーバが 50 以上存在しています。 通常、比較的少数のクライアントにサービスを提供するクライント ワークステーションやサーバは、プライマリ サーバに同期しません。 およそ 100 台のパブリック セカンダリ サーバがプライマリ サーバと同期しており、合計で 100,000 を越えるインターネット上のクライアントとサーバに同期を提供しています。 Public NTP Time Server のリストは頻繁に更新されています。 プライベートで使用されているプライマリ サーバやセカンダリ サーバも数多く存在しますが、通常は一般に公開されていません。

注: PIX と ASA は NTP サーバとしては設定できませんが、NTP クライアントとしては設定できます。

Voice over IP（VoIP）に関する単方向測定を行う場合など、きわめて正確なタイム サービスが私企業で必要とされるケースでは、プライベートの外部タイム ソースが展開されることがあります。 次の図は、現在のテクノロジーの精度を相対的に比較したグラフです。

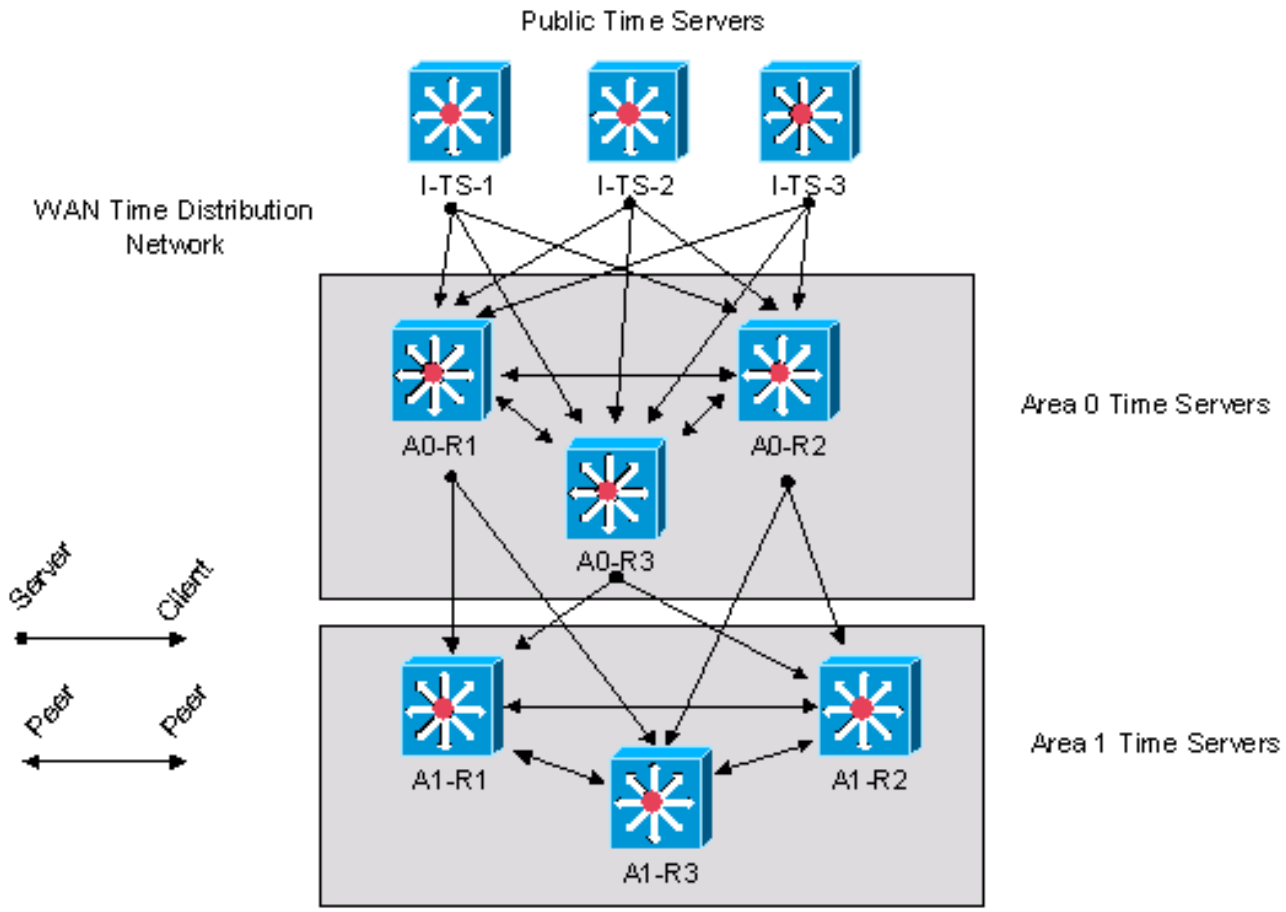


高品質な外部タイム ソースの利用には多大なコストがかかるため、最近までは企業ネットワークでそのようなソースが広範に展開されることはまれでしたが、 QoS（Quality of Service）の要件が高まり、時間関連テクノロジーのコストが低下するにつれて、企業向けの外部タイム ソースは選択可能なオプションとなりつつあります。

NTP 配置例

WAN 時間配信ネットワーク

次の図では、企業の自律システム（AS）が 3 つのパブリック タイム サーバから時間情報を取得しています。 企業 AS は、Area 0 および Area 1 のタイム サーバとして示されています。 この例の NTP 階層は、Open Shortest Path First（OSPF）階層に基づいています。 ただし、OSPF は NTP の必要条件ではありません。 これは単に説明のための例として使用されているにすぎません。 NTP は、Enhanced Interior Gateway Routing Protocol（EIGRP）階層や、標準的なコア/ディストリビューション/アクセス階層など、他の論理階層境界に沿って展開することもできます。



次の Cisco IOS 設定は、上の図のデバイス A0-R1 に関する設定です。

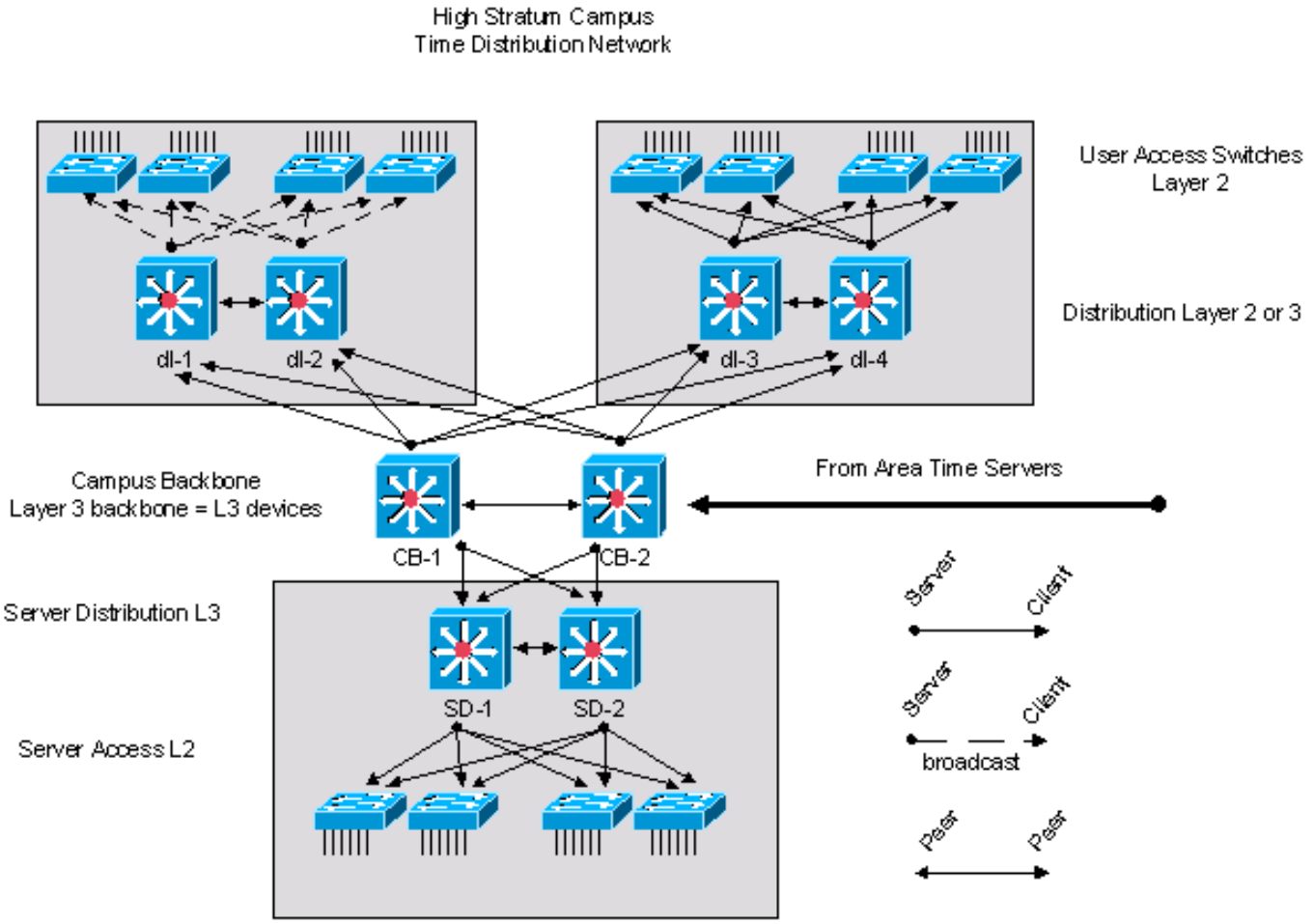
```
clock timezone CST -5
clock summer-time CDT recurring

!--- 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 will be allowed to
update the calendar !--- and Cisco IOS will be configured to be an !--- NTP master clock source.
!--- Cisco IOS will 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 will obtain the !---
clock from the hardware calendar based on !--- the previous line. This line will 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>
```

上位ストラタム キャンパス時間配信ネットワーク

前のセクションでは、WAN の時間配信ネットワークについて説明しました。 このセクションでは、階層を 1 段階下げて、上位ストラタム キャンパス ネットワークでの時間配信について説明します。

上位ストラタム キャンパスでの時間配信について考察する場合の最大の違いは、ブロードキャスト アソシエーション モードが使用される可能性があるという点です。 すでに説明したように、ブロードキャスト アソシエーション モードを使用すると、LAN の設定が簡単になりますが、時間計算の精度が低下します。 したがって、維持費用を重視するか、パフォーマンス測定の精度を重視するかを検討する必要があります。



上の図で示されている上位ストラタム キャンパス ネットワークは、標準的な Cisco キャンパス ネットワーク設計に基づいており、3 種類のコンポーネントが含まれています。 このキャンパス コアは、CB-1 および CB-2 とラベル付けされた 2 基のレイヤ 3 デバイスから構成されています。 この図の下部分にあるサーバ コンポーネントには、SD-1 および SD-2 とラベル付けされた 2 基のレイヤ 3 ルータがあります。 サーバ ブロックの残りのデバイスはレイヤ 2 デバイスです。 上部左には、dl-1 および dl-2 とラベル付けされた 2 基のレイヤ 3 配信デバイスが置かれた標準アクセス ブロックがあります。 残りのデバイスはレイヤ 2 スイッチです。 このクライアント アクセス ブロックでは、ブロードキャスト オプションを使用して時間が配信されています。 右上には、標準的なアクセス ブロックがもう 1 つあります。このアクセス ブロックでは、クライアント/サーバ時間配信構成が使用されています。

キャンパスのバックボーン デバイスは、クライアント/サーバ モデルで地域のタイム サーバと同期されています。

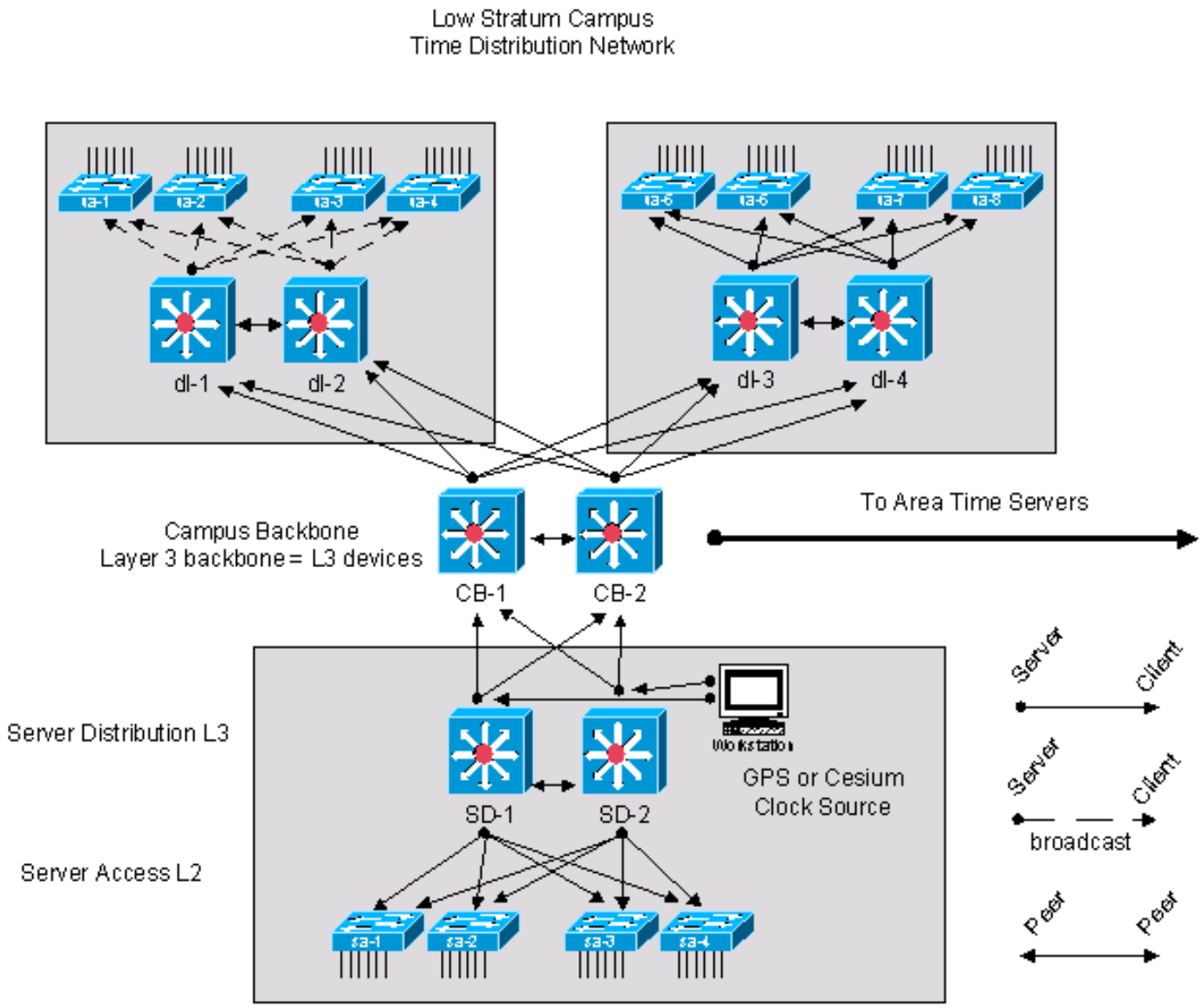
dl-1 レイヤ 3 配信デバイスの設定を以下に示します。

```
!--- In this case, dl-1 will 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>
```

低層キャンパス時間配信ネットワーク

次の図では、中央のデータ センターに下位ストラタム キャンパス ネットワーク用の GPS またはセシウム タイム ソースがあります。 これにより、プライベート ネットワーク上のストラタム 1 タイム ソースが提供されます。 プライベート ネットワーク内に複数の GPS またはセシウム タイム ソースがある場合は、それらのタイム ソースを有効に活用できるようにプライベート ネットワーク内での時間配信を変更する必要があります。

適用される原理および構成は、これまでの例とほぼ同じです。 このケースにおける最大の違いは、同期ツリーの起点がインターネットのパブリック タイム ソースではなくプライベート タイム ソースになる点です。 したがって、精度の高いプライベート タイム ソースを利用するように時間配信ネットワークの設計を変更することになります。 プライベート タイム ソースは、前のセクションで説明した階層およびモジュール性の原理を使用して、プライベート ネットワーク全体に配信されます。

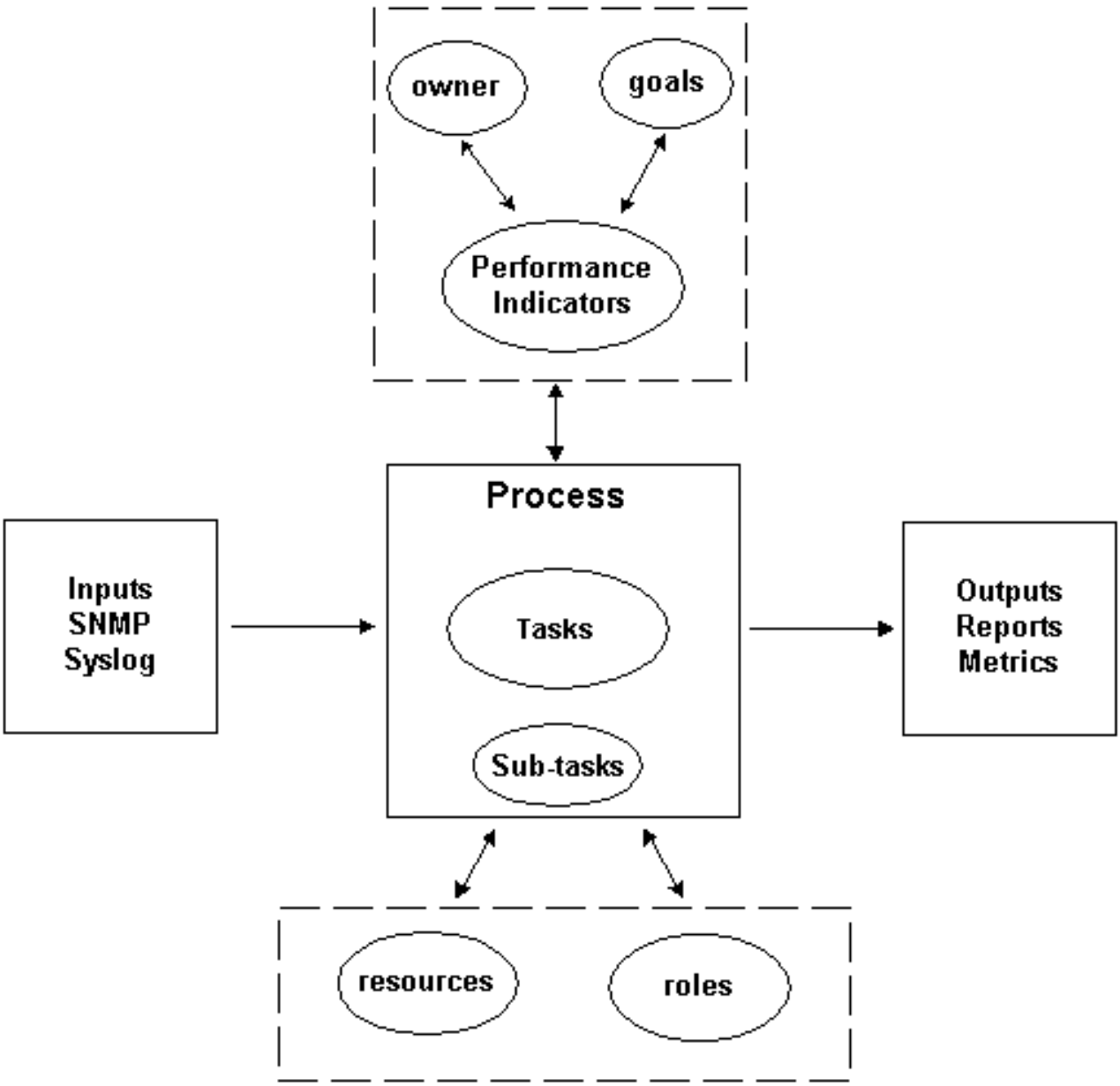


プロセス定義

プロセス定義とは、特定の目的を達成するためにエージェントによって実行される一連の動作、活動、および変更を意味します。

プロセス制御とは、プロセスを効果的かつ効率的に実行することを目的とした計画および調整の過程を意味します。

これを次の図で視覚的に示します。



プロセスの出力は、組織によって定義された運用基準と、ビジネス上の目的に準拠している必要があります。 一連の基準に準拠しているプロセスは、反復、測定、および管理が可能であり、ビジネス上の目的の達成に貢献するため、効果的であると考えられます。 また、最小限の労力で活動を実行できるプロセスは、効率的であると考えられます。

プロセス オーナー

プロセスは、さまざまな組織的境界をまたがります。 したがって、プロセス定義に責任を負うプロセス所有者は 1 人だけにする必要があります。 所有者は、そのプロセスが効果的および効率的であるかどうかを判断し、レポートする際の中心となります。 そのプロセスが効果的または効率的ではない場合、プロセス所有者はそのプロセスの修正を余儀なくされます。 プロセスを修正する際には、変更管理とチェックの手順が原則となります。

プロセスの目的

プロセスの目標は、プロセス定義の方向付けと範囲を設定するために定められます。 また、目標はプロセスの有効性を測定するためのメトリックを定義するためにも使用されます。

このプロセスの目的は、NTP 設計フェーズの間に各種の基準をドキュメント化し、展開された NTP アーキテクチャが意図されている設計に準拠しているかどうかを長期的に監査できるようにすることです。

プロセス パフォーマンス インジケータ

プロセス性能インジケータは、プロセス定義の有効性を測定するために使用されます。 パフォーマンス インジケータは、測定および定量化が可能な基準である必要があります。 たとえば、次のパフォーマンス インジケータは時間によって数値化または計測されます。

- プロセス全体を一巡するために必要な時間の長さ。
- ユーザに影響を与える前に NTP の問題を事前に発見するのに必要な実施頻度
- プロセスの実行に関連するネットワークの負荷。
- プロセスによって推奨される修正処理の回数。
- プロセスの結果として実施された修正操作の数。
- 修正処理を実行するために必要な時間の長さ。
- 修正操作の未処理件数
- NTP 関連の問題に起因するトラブルシューティングまたは問題診断での工ラー数
- シード ファイル内で追加、削除、または修正された項目の数。 これは正確性と安定性を示します。

プロセスの入力

プロセスの入力は、プロセスの基準と前提条件を定義するために使用されます。 プロセスの入力を確認することで、外的要因への依存性に関する情報がしばしば得られます。 NTP 管理に関係する入力のリストを以下に示します。

- NTP 設計ドキュメント
- SNMP ポーリングによって収集された NTP MIB データ

プロセスの出力

プロセスの出力は、次のように定義されます。

- このドキュメントの「データ表示」セクションで説明されている NTP 設定レポート
- NTP の修正操作

タスク定義

以後のセクションでは、NTP 管理に関係する初期化タスクおよび反復タスクについて説明します。

初期化タスク

初期化タスクは、プロセスの実施中に 1 度だけ実行し、そのプロセスを反復するたびに実行しないようにしてください。

NTP 設計の作成

必須タスクの確認中に、いずれかのタスクが実施されていないか、あるいはこの手順の要求に応えるだけの十分な情報が提供されていない場合は、この事実をプロセス所有者が文書化し、管理者に提出する必要があります 次の表では、必須の初期化タスクを概説しています。

必須タスク	説明
タスクの目的	設計上の要件およびコスト面での目標に合致したNTP アーキテクチャに関する詳細な設計ドキュメントを作成する
タスクの入力	• 技術面および経済面からの設計上の要件 • 既存のネットワーク設計ドキュメント • 管理機能を有効にするために設計に記録される要件定義の基準 • IT アプリケーション展開情報 • パフォーマンス監視の要件
タスクの出力	NTP 設計ドキュメント
タスクのリソース	ネットワーク エンジニア アーキテクト、ネットワーク運用アーキテクト
タスクに関係する役割	ネットワーク設計に関する技術面での承認は技術部門および運用部門のチェック担当者が行い、ネットワーク設計に関するコスト面での承認は担当の予算管理者が行う

シード ファイルの作成

NTP 管理プロセスでは、ネットワーク検出機能の必要性を排除するために、シード ファイルを使用する必要があります。 シード ファイルには、NTP プロセスによって管理されているルータのセットが記録されており、組織内の変更管理プロセスとの調整を行う際に中心的な役割を担います。 たとえば、ネットワークに新しいノードを追加した場合は、NTP シード ファイルにそれらのノードを追加する必要があります。 セキュリティ上の理由で SNMP コミュニティ名に変更を加えた場合は、それらの変更をシード ファイルに反映する必要があります。 次の表では、シード ファイルの作成手順を概説しています。

必須タスク	説明
タスクの目的	ネットワーク デバイスの 3 つのカテゴリを識別するシード ファイルを作成する 1. 重要デバイス：設定情報のポーリング頻度が高い 2. 対象（interesting）デバイス：ポーリング頻度が少ない 3. すべての NTP 対応デバイス：ポーリング頻度が最も少ない

タスクの入力	NTP 設計ドキュメント、ネットワーク トポロジ ドキュメント
タスクの出力	シード ファイル
タスクのリソース	NTP アーキテクチャに含まれるノードの識別および優先順位付けに使用される設計基準

NTP パフォーマンス パラメータのベースライン設定

NTP ネットワークの監視に使用できるパラメータの中には、予想範囲内の正常な変動を示すものがあります。 ベースライン設定のプロセスは、予想内の正常な変動を評価し、予想外または異常な状態を定義したしきい値を設定するために使用されます。 このタスクは、NTP アーキテクチャに関するパラメータの変数セットのベースラインを設定するために使用されます。 ベースライン化テクニックのさらに詳細な説明は、『ベースライン プロセス： ベスト プラクティス ホワイト ペーパー』を参照してください。

Process	説明
タスクの目的	変動するパラメータのベースラインを設定する
タスクの入力	変動するパラメータを識別する（ cntpSysRootDelay cntpSysRootDispersion cntpPeersRootDelay cntpPeersRootDispersion cntpPeersOffset cntpPeersDelay cntpPeersDispersion ）
タスクの出力	ベースライン値およびしきい値
タスクのリソース	SNMP データ収集およびベースライン計算用のツール
タスクの役割	ネットワーク エンジニア、NMS エンジニア

反復タスク

反復タスクは、プロセスを反復するたびに実行され、その頻度はパフォーマンス インジケータの改善を考慮して決定または変更されます。

シード ファイルを管理する

シード ファイルは、NTP 管理プロセスを効果的に実施する上で、きわめて重要になります。 したがって、シード ファイルの現在の状態を積極的に管理する必要があります。 シード ファイルの内容に影響する変更がネットワークに加えられた場合は、NTP 管理プロセスのオーナーがそれらの変更を記録する必要があります。

Process	説明
タスクの目的	シード ファイルの精度を維持する
タスクの入力	ネットワークの変更に関する情報
タスクの出力	シード ファイル

タスクのリソース	変更に関連する報告、通知、会議
タスクの役割	ネットワーク エンジニア、NMS エンジニア

NTP ノード スキャンの実行

この手順で定義された重要ノードのスキャン、対象ノード（interesting）のスキャン、および設定のスキャンに関する情報を収集します。 これら 3 つのスキャンを異なる頻度で実行します。

重要ノードとは、パフォーマンス データ収集 ポイントにとってきわめて重要と考えられるデバイスです。 重要ノード スキャンは頻繁に（例としては 1 時間ごとに）実行され、変更前および変更後にオンデマンドで実行されることもあります。 対象（interesting）ノードとは、NTP アーキテクチャの全体的な整合性にとって重要と考えられるデバイスです。ただし、これらのノードは、重要パフォーマンス データ収集の同期ツリーに属していなくてもかまいません。 このレポートは定期的に（例としては 1 日ごと、または 1 か月ごとに）実行されます。 設定レポートは、NTP 展開全体の設定を記録して設計記録と比較するために使用される総合的なレポートで、多くのリソースを消費します。 このレポートは低い頻度で（例としては 1 か月ごと、または四半期ごとに）実行されます。 確認された NTP アーキテクチャの安定性およびビジネス上のニーズに基づいてレポートの収集頻度を調整できるようにすることが重要なポイントとなります。

Process	説明
タスクの目的	NTP アーキテクチャを監視する
タスクの入力	ネットワーク デバイス データ
タスクの出力	レポート
タスクのリソース	データを収集してレポートを作成するためのソフトウェア アプリケーション
タスクの役割	ネットワーク エンジニア

NTP ノード レポートの確認

このタスクでは、重要レポート、対象（interesting）レポート、および設定レポートの確認と分析を行う必要があります。 問題が見つかった場合は、修正操作を開始する必要があります。

Process	説明
タスクの入力	スキャン レポート
タスクの出力	安定性の分析、修正操作
タスクのリソース	さらに詳細な調査と検証を行うためのネットワーク デバイスへのアクセス
タスクの役割	ネットワーク エンジニア

データの識別

一般的なデータの特徴

次の表では、NTP アーキテクチャの分析に役立つと考えられるデータについて説明しています。

データ	説明
ノード ID	NTP 設定済みのデバイス
Peers	そのデバイスに対して設定されているピア
同期ソース	同期のために選択されたピア
NTP 設定データ	NTP 設計の整合性を判断するために使用されるパラメータ
NTP 品質データ	NTP アソシエーションの品質を評価するために使用されるパラメータ

SNMP データの識別

Cisco NTP MIB システム グループ

NTP SNMP データは、Cisco-NTP-MIB によって定義されます。 この MIB をサポートするリリースについての最新情報を入手するには、Cisco,com の Feature Navigator ツールを使用して、MIB Locator オプションを選択してください。 このツールへは、『ボイス、テレフォニー、およびメッセージングテクノロジー用 TAC ツール』ページからアクセスできます。

Cisco NTP MIB のシステム グループは、NTP を実行しているターゲット ノードに関する情報を提供します。 ターゲット ノードとは、SNMP クエリの宛先になるノードです。

Object Name	オブジェクトの説明
cntpSysStratum	ローカル クロックのストラタム。 この値が 1（プライマリ リファレンス）に設定されている場合は、RFC-1305 のセクション 3.4.6 で説明されている Primary-Clock プロシージャが呼び出されます。 :::: = { cntpSystem 2 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.2
cntpSysPrecision	システム クロックの精度（秒単位）を最も近い 2 の累乗数に丸めた符号付き整数。 この値は、次に大きな 2 の累乗数に丸められます。 たとえば、周波数 50-Hz（20 ms）または 60-Hz（16.67 ms）のクロックには値 -5（31.25 ms）が割り当てられ、1000-Hz（1 ms）の水晶時計には値 -9（1.95 ms）が割り当てられます。 :: = { cntpSystem 3 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.3
cntpSysRootDelay	同期サブネットの起点にあるプライマリ リファレンス ソースへのラウンドトリップ遅延（秒単位）を示す符号付き固定小数点数。 :: = { cntpSystem 4 } オブジェクト識別子

	= .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRootDispersion	同期サブネットの起点にあるプライマリ リファレンス ソースとの最大誤差（秒単位）。 使用される値はゼロよりも大きい正の値のみです。 :: = { cntpSystem 5 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRefTime	ローカル クロックが最後に更新されたときのローカル時刻。 ローカル クロックがまだ 1 度も同期されていない場合は、この値がゼロになります。 :: = { cntpSystem 7 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.7
cntpSysPeer	現在の同期ソース。これには、同期ソースとして動作しているピアの cntpPeersVarTable 内にある対応するピア エントリの一意のアソシエーション ID cntpPeersAssocId が含まれます。 ピアがない場合は、この値がゼロになります。 :: = { cntpSystem 9 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.9
cntpSysClock	現在のローカル時間。 ローカル時間は、特定のマシンのハードウェア クロックから取得され、使用されている設計に応じた間隔で増加します。 :: = { cntpSystem 10 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.10

Cisco NTP MIB ピア グループ：ピア変数の表

Cisco NTP MIB のピア グループは、ターゲット ノードのピアに関する情報を提供します。

Object Name	オブジェクトの説明
cntpPeersVarTable	このテーブルには、ローカル NTP サーバとアソシエーションを持つピアについての情報が含まれます。 他のホスト上で実行されている NTP サーバもピアになります。 これは cntpPeersVarEntry のテーブルです :: = { cntpPeers 1 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1
cntpPeersVarEntry	各ピアのエントリには、特定のピア NTP サーバから取得された NTP 情報が含まれます。 各ピアは一意のアソシエーション ID によって識別されます。 ユーザが NTP サーバをリモート ピアに関連付けると、エントリが自動的に作成されます。 また、ユーザが NTP サーバからピアのアソシエーションを削除すると、エントリが削除されます。 管理端末から cntpPeersPeerAddress、cntpPeersHostAddress、cntpPeersMode の値を設定して、cntpPeersEntryStatus をアクティブ（1）にする方法でエントリを作成することもで

	きます。 管理端末では、少なくとも cntpPeersPeerAddress の値を設定して、その行をアクティブにする必要があります。 INDEX { cntpPeersAssocId } :: = { cntpPeersVarTable 1 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1
cntpPeersAssocId	ローカル NTP サーバに関連付けられたピアを一意に識別する 1 以上の整数値。 :: = { cntpPeersVarEntry 1 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.1
cntpPeersConfigured	そのアソシエーションが設定情報から作成されたものであり、該当するピアに到達できなくなった場合でも関連付けを解除してはならないことを示すビット。 :: = { cntpPeersVarEntry 2 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.2
cntpPeersPeerAddress	ピアの IP アドレス。 新しいアソシエーションを作成した場合、このオブジェクトの値を設定しないと、その行はアクティブになりません。 :: = { cntpPeersVarEntry 3 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.3
cntpPeersMode	SYNTAX INTEGER { unspecified (0), symmetricActive (1), symmetricPassive (2), client (3), server (4), broadcast (5), reservedControl (6), reservedPrivate (7) } When creating a new peer association, if no value is specified for this object, it defaults to symmetricActive (1). :: = { cntpPeersVarEntry 8 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.8
cntpPeersStratum	ピア クロックのストラタム :: = { cntpPeersVarEntry 9 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.9
cntpPeersRootDelay	ピアから同期サブネットの起点にあるプライマリ リファレンス ソースへのラウンドトリップ遅延（秒単位）を示す符号付き固定小数点数。 :: = { cntpPeersVarEntry 13 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.13
cntpPeersRootDispersion	同期サブネットの起点にあるプライマリ リファレンス ソースとピアとの最大誤差（秒単位）。使用される値はゼロよりも大きい正の値のみです。 :: = { cntpPeersVarEntry 14 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.14
cntpPeersRefTime	ピアのクロックが最後に更新されたときのピアのローカル時刻。 ピアのクロックがまだ 1 度も同期されていない場合は、この値がゼロになります。 :: = { cntpPeersVarEntry 16 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.16
cntpPeersReach	ピアに到達可能かどうかを確認するために使用されるシフト レジスタ。ビットは、最小位（右端）から挿入されます。 このレジスタの 1 つ以上のビットが 1 に設定されている場合（オブジ

	エクトがゼロでない場合）は、ピアに到達可能であると見なされます。 このシフト レジスタのデータは、NTP プロトコル プロシージャによって挿入されます。 :: = { cntpPeersVarEntry 21 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersOffset	ローカル クロックに対するピア クロックの推定オフセット（秒単位）。 ホストは、NTP クロック フィルタ アルゴリズムを使用してこのオブジェクトの値を決定します。 :: = { cntpPeersVarEntry 23 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersDelay	ローカル クロックとピア クロックの間のネットワーク パスを経由する際の、ローカル クロックに対するピア クロックの推定ラウンドトリップ遅延（秒単位）。 ホストは、NTP クロック フィルタ アルゴリズムを使用してこのオブジェクトの値を決定します。 :: = { cntpPeersVarEntry 24 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.24
cntpPeersDispersion	ローカル クロックとピア クロックの間のネットワーク パスを経由する際の、ローカル クロックに対するピア クロックの推定最大誤差（秒単位）。 ホストは、NTP クロック フィルタ アルゴリズムを使用してこのオブジェクトの値を決定します。 :: = { cntpPeersVarEntry 25 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.25

データ収集

SNMP データ収集

この手順で必要となる情報はすべて SNMP クエリによって収集されます。 これらのデータを解析してレポートを作成するには、カスタム スクリプトまたはソフトウェア プログラムを開発する必要があります。

データ表示

NTP 重要ノード レポート

重要ノードとは、特定のパフォーマンス データ収集ポイントの同期ツリーにおいて重要なデバイスです。 収益性の高い VoIP サービスを監視して単方向遅延変動メトリックを収集している場合は、タイム スタンプが記録される送信元ノードおよび宛先ノードは重要ノードと見なされます。

この例の NTP 設計は、Open Shortest Path First（OSPF）階層に基づいて作成されています。 したがって、以下で説明するレポートは、デバイスの OSPF 領域に従って NTP デバイスをグループ化するように書式設定されています。 複数の領域にインターフェイスを持つノードがある場合は、レポートの作成時にそのノードをどの領域にリストするかをレポート生成ソフトウェアで判断する必要があります。 すでに述べたように、OSPF は NTP の必要条件ではありません。 この

ドキュメントでは、単に説明のための例として使用しているにすぎません。

エリア	デバイス	デバイス データ	値
AreaId #n	DeviceId #1	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	
	DeviceId #n	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	

NTP の対象ノードのレポート

対象（interesting）ノード レポートの書式は、重要ノード レポートと同じです。 対象（interesting）ノードとは、NTP アーキテクチャ全体にとって重要と考えられるデバイスです。 ただし、これらのノードは、重要パフォーマンス監視ポイントの時間同期に直接関与しなくてもかまいません。

NTP の設定レポート

設定レポートは、NTP アーキテクチャ全体に関する情報を収集する総合的なレポートです。 このレポートは、NTP の展開を記録して、設計記録と比較するために使用されます。

エリア	デバイス	ピア	ピア データ	値
AreaId #n	DeviceId #n	PeerId #1	cntpPeersAssocId	
			cntpPeersConfigured	
			cntpPeersPeerAddress	
			cntpPeersMode	
			cntpPeersStratum	
			cntpPeersRootDelay	
			cntpPeersRootDispersion	
			cntpPeersRefTime	
			cntpPeersReach	
			cntpPeersOffset	
			cntpPeersDelay	
			cntpPeersDispersion	
		PeerId #n	cntpPeersAssocId	

			cntpPeersConfigured	
			cntpPeersPeerAddress	
			cntpPeersMode	
			cntpPeersStratum	
			cntpPeersRootDelay	
			cntpPeersRootDispersion	
			cntpPeersRefTime	
			cntpPeersReach	
			cntpPeersOffset	
			cntpPeersDelay	
			cntpPeersDispersion	

関連情報

- RFC 1305 Network Time Protocol
- RFC 2330 Framework for IP Performance Metrics
- Essential IOS Features Every ISP Should Consider v2.84
- テクニカルサポート - Cisco Systems