

Network Time Protocolのベストプラクティスの使用

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[用語](#)

[概要](#)

[デバイスの概要](#)

[NTP の概要](#)

[NTP 設計基準](#)

[アソシエーション モード](#)

[クライアント/サーバ モード](#)

[対称アクティブ/パッシブ モード](#)

[ブロードキャストまたはマルチキャスト モード](#)

[NTPうるう秒の設定](#)

[NTP アーキテクチャ](#)

[クロック テクノロジーとパブリック タイム サーバ](#)

[NTP 配置例](#)

[WAN 時間配信ネットワーク](#)

[上位ストラタム キャンパス時間配信ネットワーク](#)

[低層キャンパス時間配信ネットワーク](#)

[プロセス定義](#)

[プロセス オーナー](#)

[プロセスの目的](#)

[プロセス パフォーマンス インジケータ](#)

[プロセスの入力](#)

[プロセス出力](#)

[タスク定義](#)

[初期化タスク](#)

[NTP 設計の作成](#)

[シード ファイルの作成](#)

[NTP パフォーマンス パラメータのベースライン設定](#)

[反復タスク](#)

[シード ファイルを管理する](#)

[NTP ノード スキャンの実行](#)

[NTP ノード レポートの確認](#)

[データの識別](#)

[一般的なデータの特徴](#)

[SNMP データの識別](#)

[Cisco NTP MIB システム グループ](#)

[Cisco NTP MIB ピア グループ : ピア変数の表](#)

[データ収集](#)

[SNMP データ収集](#)

[データ表示](#)

[NTP 重要ノード レポート](#)

[NTPの対象ノードのレポート](#)

[NTPの設定レポート](#)

[関連情報](#)

概要

このドキュメントでは、ネットワークタイムプロトコル(NTP)を設計するためのベストプラクティスについて説明します。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- Network Time Protocol (NTP; ネットワーク タイム プロトコル)
- クロック テクノロジーとパブリック タイム サーバ

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

インターネットプロトコル(IP)ベースのネットワークは、従来の最良のeffortdeliveryモデルから、パフォーマンスと信頼性を定量化する必要があり、多くの場合、サービスレベル契約(SLA)で保証されるモデルへと急速に進化しました。ネットワークの特性に対する深い洞察の必要性から、ネットワークの動作を特徴付ける重要なメトリックと測定機能を対象とした重要な研究が行われています。中でも、時刻の測定は、多くのメトリック方式の基礎となっています。

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。ビジネスモデルと提供されるサービスに基づいて、ネットワークパフォーマンスの特性を評価することは、競争力のあるサービスの重要な差別化要因であると考えられま

す。このような場合、ネットワーク管理システムを導入し、収集したパフォーマンスデータを分析するためにエンジニアリングリソースを直接割り当てると、多大なコストが発生します。しかし、しばしば見過ごされがちな時間同期の原則に適切な注意を払わなければ、それらの取り組みは効果がありません。

このドキュメントでは、ネットワークタイムプロトコル(NTP)のネットワーク管理機能の管理に関する仮想プロセス定義について説明します。この記事は、仮想的な手順および情報の例として使用できます。これは、組織が内部目標を満たすようにカスタマイズできます。

このドキュメントで提供される情報は、次のいくつかの主要なセクションに分かれています。

- Terminology sectionは、時刻同期に関する用語の一般的な定義を提供します。
- 「概要」セクションでは、システム時刻に関連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、および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](#)」セクションでは、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設定例を使用して、NTPの展開例を示しています。
- 「[プロセス定義](#)」セクションでは、NTP管理を実現するために使用されるプロセス定義の概要を説明しています。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。
- 「[タスクの定義](#)」セクションでは、プロセスタスクの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](#)」セクションでは、NTPの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; 簡易ネットワーク管理プロトコル)のManagement Information Base (MIB; 管理情報ベース)、Syslogによって生成されたログファイル、または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などに格納できます。
- 「[データ収集](#)」セクションでは、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。内部データ構造によって維持されるデータは、自動スクリプトによって、またはユーザがシステムに手動でログインしてCLIコマンドを発行し、出力を記録することによって収集されます。
- 「[データの表示](#)」セクションでは、データの表示方法を示すレポート形式の例を示しています。

用語

- **Accuracy** : クロックの絶対値がオフセットのゼロに近いこと。
- **Accurate** : 特定の時点でクロックオフセットがゼロの場合。
- **Drift** : スキューの変動の測定値、または時間に対するクロックオフセットの2番目の導出値。
- **Joint resolution** : クロックを比較すると、C1とC2の分解能の合計になります。次に、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から他方のクロックによって生成されたタイムスタンプを差し引いて計算された時間間隔の精度に関する控えめな下限値を示します。
- **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。クロックが時間 T_c を報告し、真の時間が T_t である場合、クロックオフセットは $T_c - T_t$ です。
- **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 C_1 と C_2 を比較する際に、真の時間という概念がクロック C_1 によって報告される時間に置き換えられます。たとえば、特定時点でのクロック C_1 に対する C_2 の相対オフセットは $T_{c2} - T_{c1}$ (C_2 と C_1 によって報告される時間の瞬時的差異) になる。
- **Resolution** : クロック時間が更新される最小の単位。分解能は秒単位で定義される。ただし、分解能は報告されたクロック時間に関連し、真の時間には関連しません。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 : クロックの解像度は非常に高くても不正確な場合があります。
- **Skew** : クロックの周波数差、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、システムが起動した瞬間から作動し、現在の日付と時刻を維持します。システム クロックは、複数の時刻源から設定でき、さまざまなメカニズムを介して現在の時刻を他のシステムに配信するために使用できます。一部のルータには、バッテリー駆動式のカレンダー 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。システムを再起動するときには、常にこのカレンダー システムを使用してシステム クロックが初期化されます。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。さらに、NTPが有効な場合、カレンダーはNTPから定期的に更新され、カレンダー時間に固有のドリフトが補正されます。システム カレンダーを備えたルータを初期化すると、内部バッテリー駆動式カレンダーの時刻に基づいてシステム クロックが設定されます。なお、カレンダーのないモデルでは、システム クロックは、あらかじめ決められた特定の時刻に設定されます。システムクロックは、次に示すソースから設定できます。

- NTP
- Simple Network Time Protocol (SNTP; シンプル ネットワーク タイム プロトコル)
- 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 を簡素化したクライアント専用バージョンです。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非準拠のサーバに対して脆弱であり、強力な認証が必要ない状況でのみ使用する必要があります。

システムクロックは、次に示すサービスに時間を提供します。

- NTP
- VINES タイム サービス
- Usershowcommands
- 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) と呼ばれます。現地のタイム ゾーンを基準として時刻が正確に表示されるように、現地のタイム ゾーンと夏時間に関する情報を設定できます。システム クロックは、時刻が正規のものか非正規のものを把握しています。権限がない場合、時刻は表示目的でのみ使用でき、再配布することはできません。

NTP の概要

NTP は、ネットワーク上の多くのマシンが時刻を同期することを目的としています。NTP はユーザデータグラムプロトコル (UDP) 上で動作し、ポート 123 は送信元と宛先の両方として機能し、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とクライアントの間でタイムキーピングを同期するために使用されます。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。複数のプライマリサーバが存在する可能性がありますが、選択プロトコルは必要ありません。

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。その後、NTP はこの時刻をネットワーク全体に配信します。NTP クライアントは、ポーリング間隔 (64 ~ 1024 秒) でサーバと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間のネットワーク状態に応じて動的に変化します。ルータが不良 NTP サーバ (たとえば、大きな dispersion 値をもった NTP サーバ) と通信して、これとは異なった状況が発生する場合にも、ルータではポーリングの間隔が増加します。2 台のマシンを同期するために必要な NTP トランザクションは 1 分あたり 1 つだけです。ルータで NTP ポーリング間隔を調整することはできません。

NTP では、正規の時刻源から各マシンが何段階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。このタイムサーバからストラタム 2 のタイムサーバに NTP によって時刻が送信され、同様に番号順に時刻が送信されます。NTP を実行しているマシンは、NTP と通信するように設定されているストラタム番号が最も小さいマシンを自動的に選択し、そのマシンを時刻源として使用します。この手法により、NTP スピーカーの自動形成型ツリーが効率的に構築されます。NTP は、クライアントとタイムサーバ間の関係における次の 3 つの主要な変数を確実に推定するため、パケット交換ネットワークのパス長が不確定な場合でも優れた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。
- Clock offset : クライアントのクロックを同期するために適用される補正。

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 to 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 to 実現されます。

時刻が正確でないマシンと NTP が同期しない方法は 2 つあります。まず、それ自身が同期できていないマシンとは同期しません。次に、NTP は複数のマシンから報告された時間を比較し、そのストラタムが低くても、他のマシンと時間が大幅に異なるマシンと同期しません。

通常、NTP を実行するマシン間の通信 (アソシエーション) は静的に設定されます。各マシンに

は、関連付けを形成する必要があるすべてのマシンのIPアドレスが与えられます。アソシエーションを持つマシンの各ペア間で交換されるNTPメッセージによって、正確な計時が可能になります。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。この代替の方法では、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、情報フローが一方向のみになるため、正確な時刻を保持する精度が若干低下します。

マシン上に保持される時間は重要なリソースです。誤った時間が偶発的または悪意のある方法で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お勧めします。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。

シスコのNTP実装では、特定のCisco IOS®ソフトウェアリリースでストラタム1サービスがサポートされています。リリースで`thentp refclockcommand`がサポートされている場合は、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。ネットワークがインターネット上のパブリックタイムサーバを使用し、ネットワークがインターネットから分離されている場合、シスコのNTP実装を使用すると、実際には他の手段で時間が決定されていても、NTPを介して同期されているかのように動作するようにマシンを設定できます。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

同期サブネット内の各クライアント (上位ストラタムクライアントのサーバにすることも可能) は、同期先として使用可能なサーバの1つを選択します。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は各サーバの時刻が一定の不信感を持って表示される必要があるという前提の下で動作するため、これは常に最適な設定とは限りません。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、すべてのサーバが一致すると、NTPは最も低いストラタム、最も近いストラタム (ネットワーク遅延)、および主張された精度の点で最適なサーバを選択します。つまり、各クライアントに3つ以上の低ストラタム時間のソースを提供する必要がありますが、そのうちのいくつかはバックアップサービスのみを提供し、ネットワーク遅延とストラタムの点で品質が劣る可能性があります。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ソースから時間を受信する同じストラタムピアは、優れたバックアップサービスも提供できます。

NTPは一般に、下位ストラタムサーバの時刻が大幅に異なる場合を除き、上位ストラタムサーバよりも下位ストラタ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トラタ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、それ自体が同期されていない別のサーバにデバイスを同期させることはできません。

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。

- 実装には、監視プログラムが長時間の間隔の後にこの情報を更新しない場合にトラップ送信を防止するサニティタイムアウトを含める必要があります。
- 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

次のセクションでは、NTPサーバが相互に関連付けるために使用する関連付け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。

最も一般的なインターネット設定は、クライアント/サーバモードです。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。クライアントは、serverコマンドと、指定されたドメインネームサーバ(DNS)名またはアドレスを使用して、クライアントモードで設定されます。サーバにはこれ以外に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、クライアントは、NTPメッセージを1台以上のサーバに送信し、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。NTPメッセージに含まれる情報を使用すると、クライアントはサーバの時刻をローカル時刻と比較して決定し、必要に応じてローカルクロックを調整できます。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、クライアントの大規模なグループに同期を提供するサーバは、相互に冗長な3つ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/サーバモードでは3つ以上のストラタム1またはストラタム2サーバで動作し、対称モードではグループの他のすべてのメンバで動作します。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のアソシエーションの設定は、通常は設定ファイル内のサーバ宣言によっ

て示され、リモートサーバから時間を取得するが、リモートサーバには時間を提供しないことを示します。

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。一方のピアがすべてのリファレンスソースを失った場合、または動作を停止した場合、他方のピアは自動的に再設定を行い、現在のピアからキュー内の他のすべてのピアに時間値が流れるようにします。状況によっては、ピアが特定の設定に基づいて時間と値をプルまたはプッシュする *apush-pulloperation* と呼ばれることもあります。

対称アクティブモードでのアソシエーションの設定は、通常は設定ファイル内のピア宣言によって示され、リモートサーバに対して、リモートサーバから時間を取得すること、および必要に応じてリモートサーバに時間を提供することを示します。このモードは、多様なネットワークパスを介して相互接続された多数の冗長タイムサーバを含む構成に適しています。現在のインターネット上の大部分のストラタム1およびストラタム2サーバがこれに該当します。

対称モードは、相互に冗長なグループとして動作する2台以上のサーバ間で最もよく使用されます。これらのモードでは、グループメンバー内のサーバが、ネットワークジッターと伝搬遅延に基づいて、最大のパフォーマンスを得るために同期パスを配置します。1つ以上のグループメンバーに障害が発生すると、残りのメンバーは必要に応じて自動的に再設定されます。

peerコマンドを使用し、他のピアのDNS名またはアドレスを指定すると、対称アクティブモードでピアが設定されます。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、対称アクティブメッセージの到着時に対称パッシブアソシエーションがアクティブになります。侵入者が対称アクティブピアになりすまして誤った時間値を注入する可能性があるため、対称モードは常に認証される必要があります。

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、サーバと依存型クライアントでは利用されません。この利点は、特定のサーバに対してクライアントを設定する必要がないことです。これにより、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ます。ブロードキャスト モードを使用するには、同じサブネット上にブロードキャスト サーバがある必要があります。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を含む構成を対象としています。ブロードキャストサーバは、broadcastコマンドとローカルサブネットアドレスを使用して設定します。ブロードキャストクライアントはbroadcastclientcommandで設定されます。このコマンドを使用すると、ブロードキャストクライアントは、任意の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回答できます。侵入者がブロードキャストサーバになりすまして誤った時間値を挿入する可能性があるため、このモードは常に認証される必要があります。

NTPうるう秒の設定

うるう秒を挿入するには、`leap {add|delete}`コマンドを使用できます。うるう秒を追加または削除するオプションがあります。これには次の2つの制約があります。

- クロックは同期状態である必要があります。
- 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。現在の時刻がうるう秒の発生から1か月前である場合は、うるう秒を設定できません。

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
v1-7500-6#show clock
23:59:58.123 UTC Sun Dec 31 2006
v1-7500-6#show clock
23:59:58.619 UTC Sun Dec 31 2006
v1-7500-6#show clock
23:59:59.123 UTC Sun Dec 31 2006
v1-7500-6#show clock
23:59:59.627 UTC Sun Dec 31 2006
<< 59th second occurring twice
v1-7500-6#show clock
23:59:59.131 UTC Sun Dec 31 2006
v1-7500-6#show clock
23:59:59.627 UTC Sun Dec 31 2006
v1-7500-6#show clock
00:00:00.127 UTC Mon Jan 1 2007
v1-7500-6#show clock
00:00:00.623 UTC Mon Jan 1 2007
```

NTP アーキテクチャ

NTPアーキテクチャでは、次の3つの構造を使用できます。

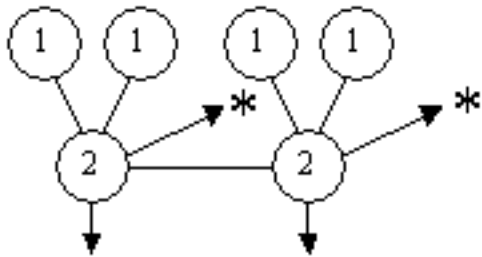
- フラットピア構造
- 階層型構造
- 星型構造

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。コアルータは外部タイムソースとのクライアント/サーバ関係を持ち、内部タイムサーバはコアルータとのクライアント/サーバ関係を持ち、内部ユーザ（非タイムサーバ）ルータは内部タイムサーバとのクライアント/サーバ関係を持ち、などといった具合にツリーを下っていきます。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。

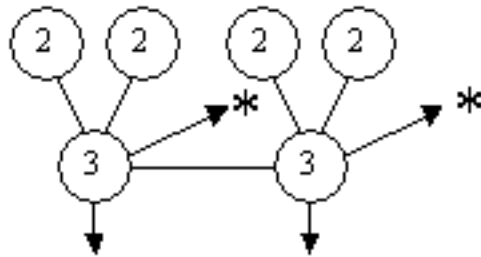
スケーラブルなNTPアーキテクチャには、次の図に示すように階層構造があります。

Internet Primary Servers
(Stratum 1)



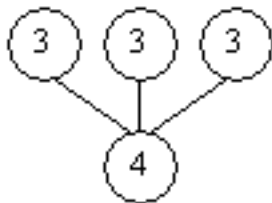
* = to buddy in another subnet

Campus Secondary Servers
(Stratum 2)



* = to buddy in another subnet

Department Servers
(Stratum 3)



Workstations (Stratum 4)

スケラブル

なNTPアーキテクチャ

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。

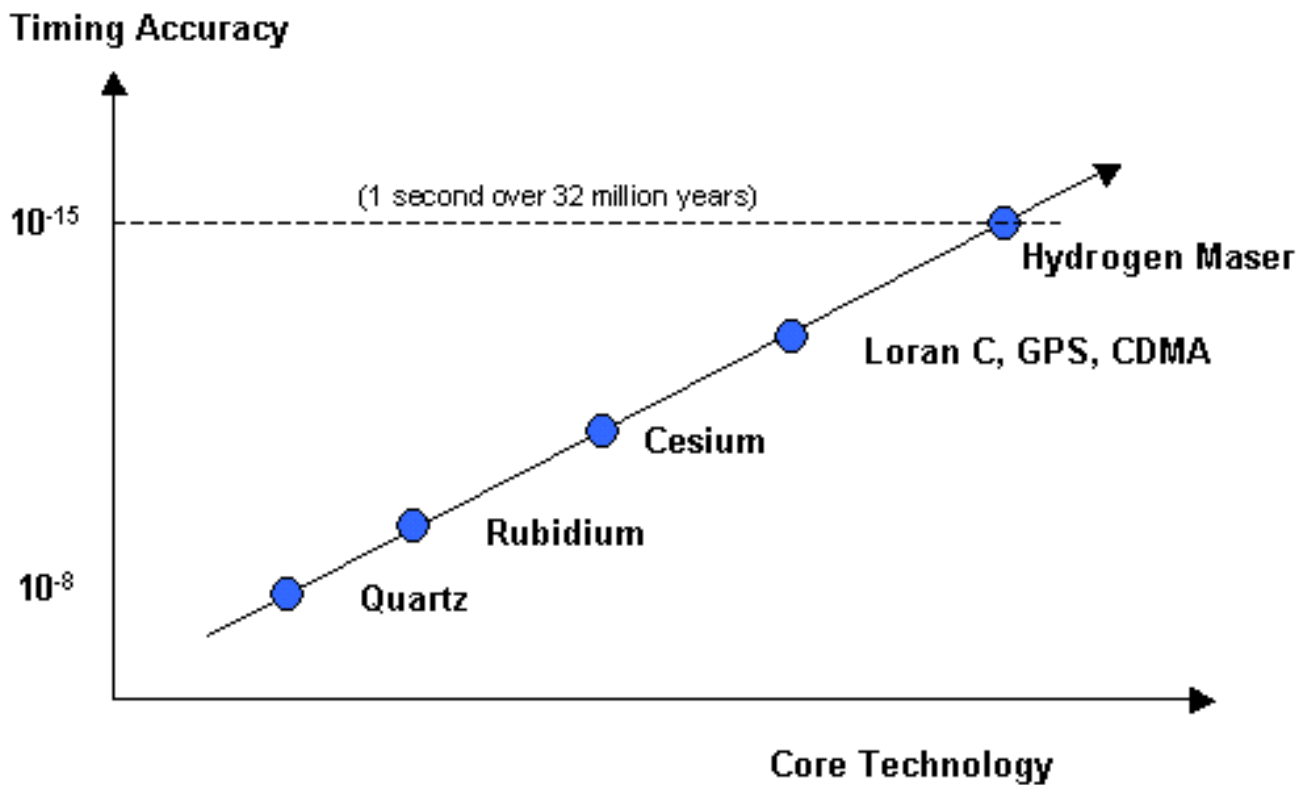
クロックテクノロジーとパブリックタイムサーバ

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ア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。約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に同期され、インターネット上の合計100,000を超えるクライアントとサーバに同期が提供されます。[Public NTP Time Serverのリスト](#)は頻繁に更新されます。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サーバとして設定できませんが、NTPクライアントとして設定することはできます。

Voice over IP(VoIP)測定の単方向メトリックなど、非常に正確なタイムサービスが民間企業で必

要とされる特定のケースでは、ネットワーク設計者はプライベート外部タイムソースの導入を選択できます。次の図は、現在の技術の相対精度の比較グラフを示しています。



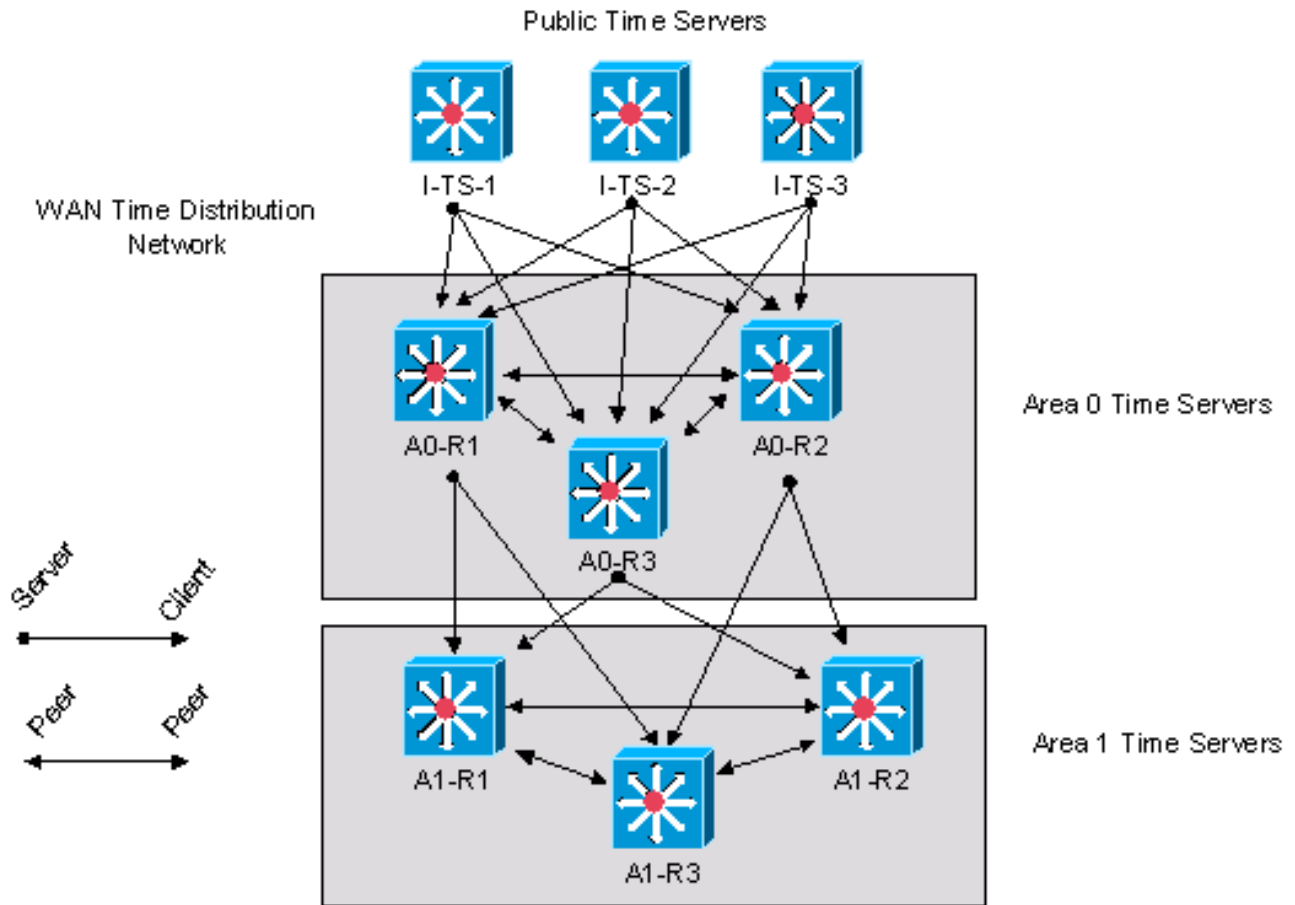
比較グラフ

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、ただし、Quality of Service(QoS)の要件が増加し、時間テクノロジーのコストが下がり続けるにつれて、エンタープライズネットワークの外部タイムソースが実行可能なオプションになります。

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刻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)階層や標準のコア/ディストリビューション/アクセス階層など、他の論理的な階層境界に沿って展開できます。



WAN 時間配信ネットワーク

次の例は、前の図に示したデバイスA0-R1のCisco IOS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 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
```

```

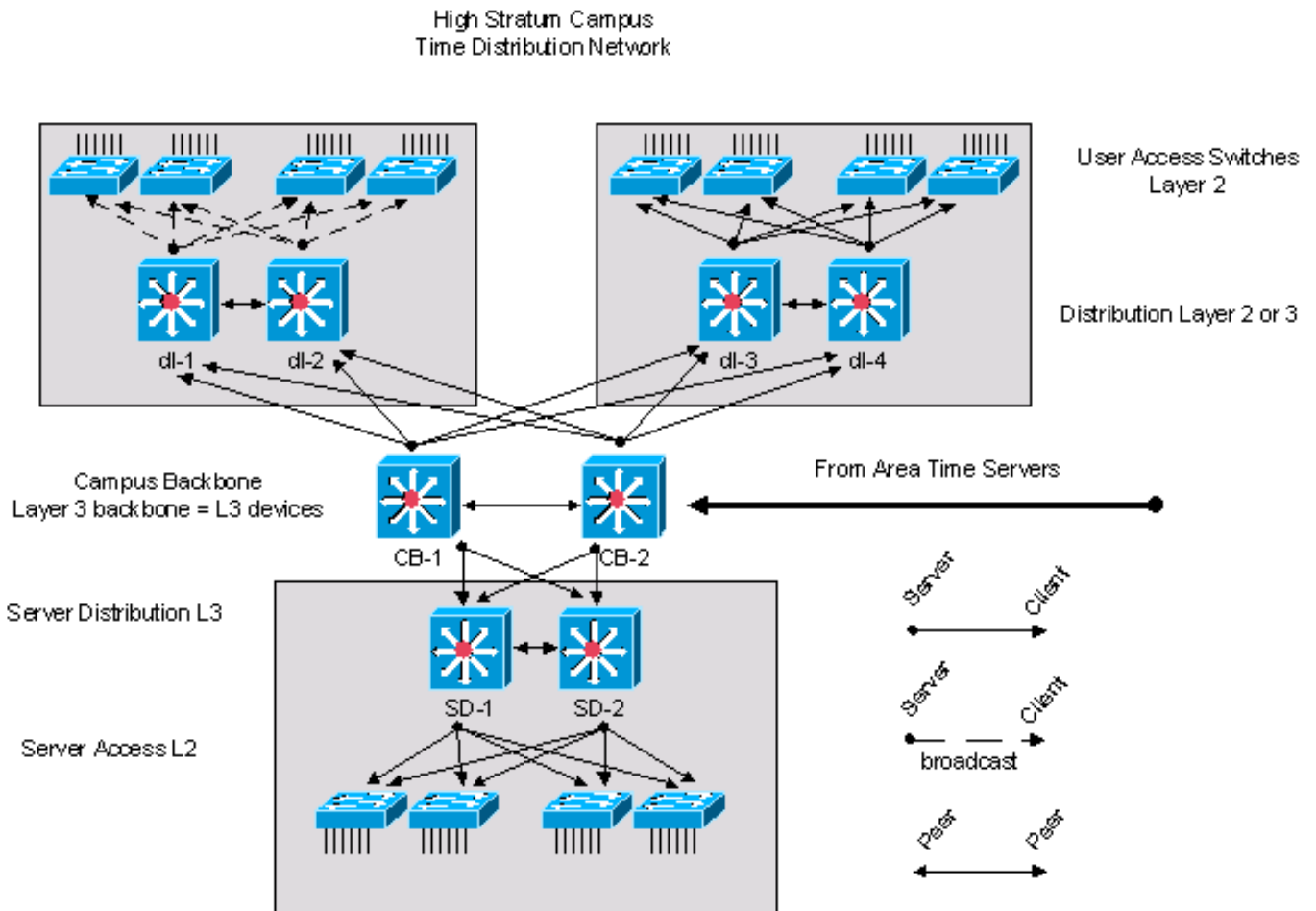
!--- address of the interface through which the
!--- NTP packet is sent.
!--- Change this to use loopback0. ntp source Loopback0 !--- Enables NTP authentication. ntp
authenticate ntp authentication-key 1234 md5 104D000A0618 7 ntp trusted-key 1234 !--- Configures
the access control groups for
!--- the 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>

```

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ネットワークでの時間配信の主な違いは、ブロードキャストアソシエーションモードを使用する可能性があることです。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はLANの設定を簡素化しますが、時間計算の精度を低下させます。したがって、パフォーマンス測定の精度に対するメンテナンス コストのトレードオフを考慮する必要があります。



上位ストラタム キャンパス時間配信ネットワーク

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。キャンパス コア は、CB-1 および CB-2 というラベルの付いた 2 台のレイヤ 3 デバイスで構成されています。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。サーバブロック内の他のデバイスは、レイヤ2デバイスです。左上には、dl-1 および dl-2 というラベルの付いた 2 台のレイヤ 3 ディストリビューション デバイスを含む標準アクセス 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ます。右上には、クライアント/サーバの時刻の配信設定を使用する別の標準アクセス ブロックがあります。

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ディストリビューションデバイスの設定を次に示します。

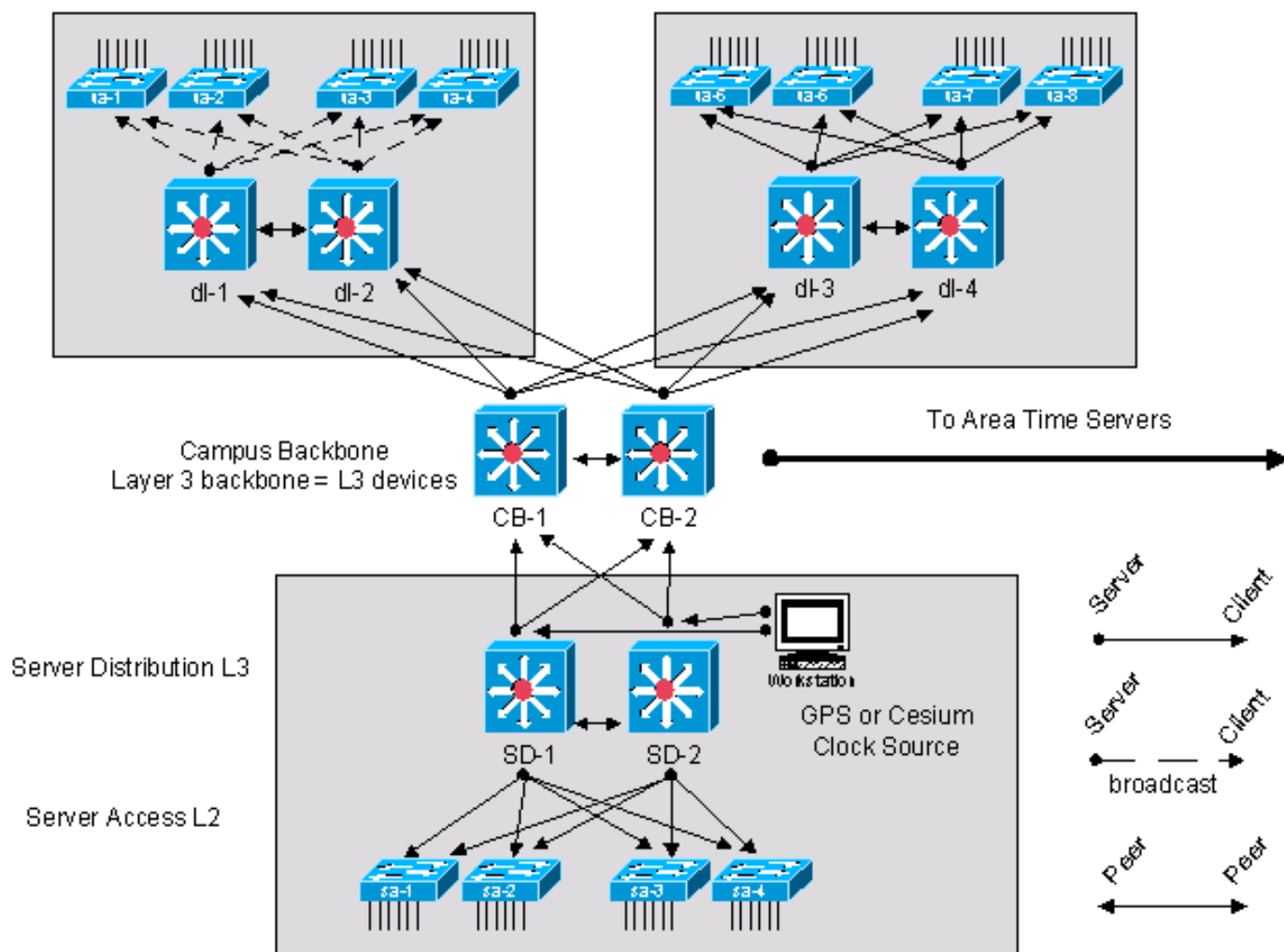
```
!--- In this case, dl-1 can be a broadcast server
!--- for the Layer 2 LAN. internet Ethernet0 ntp broadcast clock timezone CST -5 clock summer-
time CDT recurring !--- When the system sends an NTP packet, the
!--- source IP address is normally set to the
!--- address of the interface through which 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>
```

低層キャンパス時間配信ネットワーク

次の図では、下位ストラタムキャンパスネットワークの中央データセンターにGPSまたはセシウム時刻源が提供されています。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またはセシウム時刻源がある場合、使用可能な時刻源を利用するには、プライベートネットワーク内の時刻分布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とモジュール性の原則を使用して、プライベートネットワーク全体に分散されます。

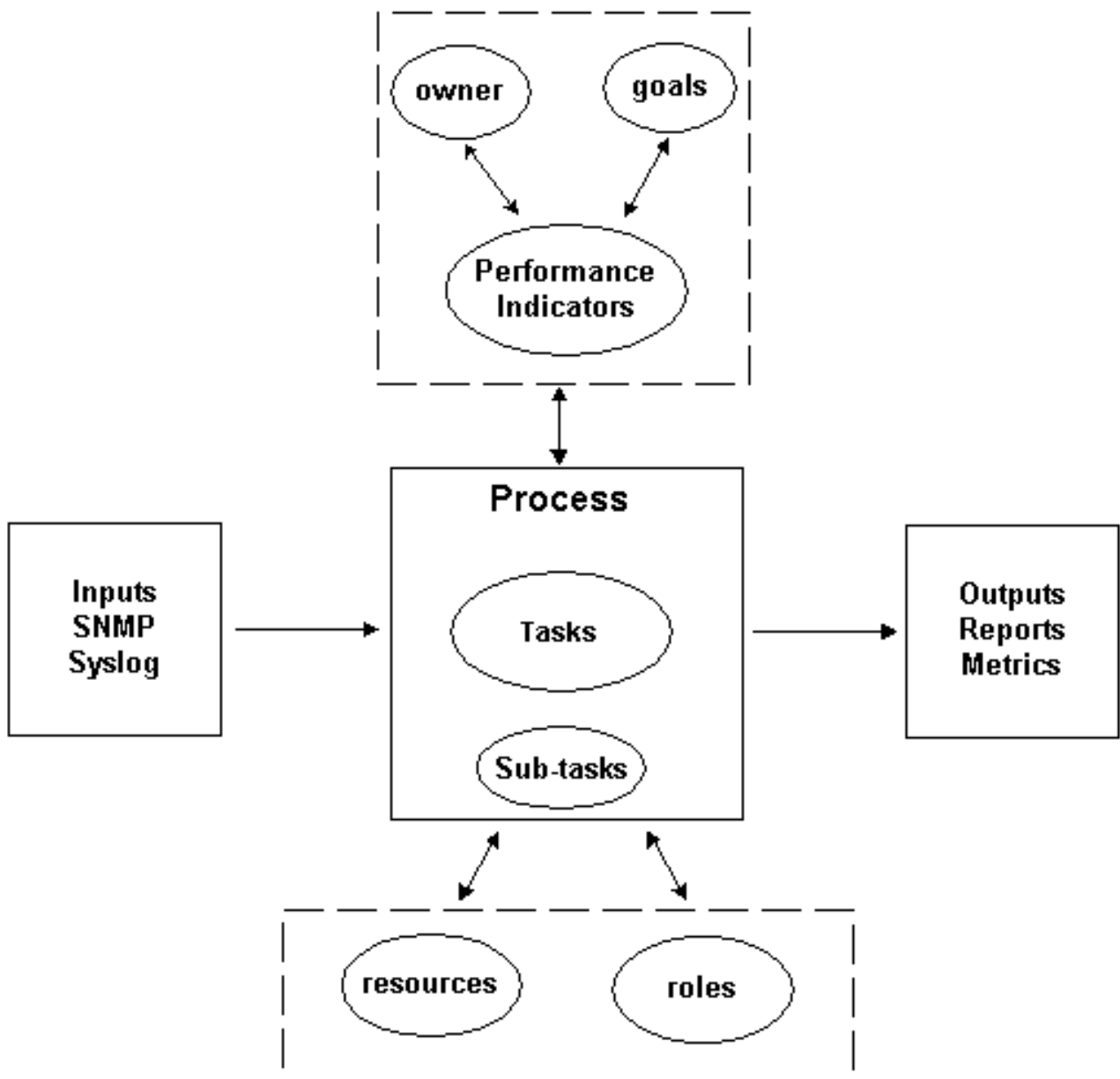
Low Stratum Campus Time Distribution Network



低層キャンパス時間配信ネットワーク

プロセス定義

プロセス定義は、目的を満たすため、または目標を達成するためにエージェントによって実行される、一連のアクション、アクティビティ、および変更を連結したものです。プロセス制御は、効果的かつ効率的な方法でプロセスを実行することを目的とした、計画および調整のプロセスです。これを次の図に示します。



一連のプロセス

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ぎます。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、プロセスが効果的かつ効率的であるかどうかを判断し、報告する中心です。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基準を文書化し、展開されたNTPアーキテクチャに監査機能を提供して、意図された設計に長期的に準拠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、測定可能かつ定量化可能である必要があります。たとえば、次に示すパフォーマンス指標は、数値または時間で測定されます。

- 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エラー数
- 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。次に、NTP管理に関連する入力のリストを示します。

- 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

プロセス出力

プロセス出力は次のように定義されます。

- このドキュメントの「[データの表示](#)」セクションで定義されているNTP設定レポート
- NTP の修正操作

タスク定義

次のセクションでは、NTP管理に関連する初期化タスクと反復タスクを定義します。

初期化タスク

初期化タスクは、プロセスの実装中に1回実行されます。プロセスの反復ごとに実行することはできません。

NTP 設計の作成

前提タスクを検証するときに、いずれかのタスクが実装されていないか、この手順のニーズを効果的に満たすのに十分な情報が提供されていないと判断された場合は、そ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。次の表に、前提条件となる初期化タスクの概要を示します。

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設計要件。 <ul style="list-style-type: none">技術面および経済面からの設計上の要件現在のネットワーク設計文書
タスクの入力	<ul style="list-style-type: none">管理機能を有効にするために設計に記録する必要のある側面を定義する基準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。

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。次の表に、シードファイルの作成方法の概要を示します。

必須タスク	説明
タスクの目的	次の3つのカテゴリのネットワークデバイスを識別するシードファイルを作成します。 <ol style="list-style-type: none">重要デバイス：設定情報のポーリング頻度が高い対象 (interesting) デバイス：ポーリング頻度が少ないすべての 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 アーキテクチャに関係するノードを特定し、優先順位を付けるために使用できる。

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詳細については、『[ベースラインプロセス：ベストプラクティスのホワイトペーパー](#)』を参照してください。

プロセス	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	可変パラメータ <code>cntpSysRootDelay</code> <code>cntpSysRootDispersion</code> <code>cntpPeersRootDelay</code> <code>cntpPeersRootDispersion</code> <code>cntpPeersOffset</code> <code>cntpPeersDelay</code> <code>cntpPeersDispersion</code> を特定します。
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 データを収集し、ベースラインを計算するツール。

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。

プロセス	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	変更に関するレポート、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が、重要なパフォーマンスデータを収集するための時刻同期ツリーには含まれません。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。

プロセス	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。問題が検出された場合は、是正措置を開始する必要があります。

プロセス	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

次の表に、NTPアーキテクチャを分析する際に重要と見なされるデータを示します。

Data	説明
ノード ID	NTP 設定済みのデバイス
ピア	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関する最新情報を入手するには、CCO Feature Navigatorツールを使用して、MIB Locatorオプションを選択します。このツールには、[TAC Tools for Voice, Telephony and Messaging Technologies](#)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を実行す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。値が1 (プライマリリファレンス) に設定され、呼び出されます。 ::= { cntpSystem 2 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.9
cntpSysPrecision	システムクロックの精度を秒単位で最も近い2のべき乗に示す符号付き整数。この値が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。
cntpSysRootDelay	同期サブネットのルート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
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)
cntpSysRefTime	ローカルクロックが最後に更新された時の現地時間。ローカル クロックがまだ更新されていません。
cntpSysPeer	同期ソースとして動作しているピアのcntpPeersVarTable内の対応するピアエンタリ
cntpSysClock	{ cntpSystem 9 } オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.1.9 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ます。

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、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 情報が含まれています。
cntpPeersVarEntry	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。エントリは、cntpPeersVarTable内の値を設定して、その行をアクティブにする必要があります。INDEX { cntpPeersVarEntry }
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

cntpPeersConfigured	このビットは、関連付けが設定情報から作成されたことを示し、ピアが到達不
cntpPeersPeerAddress	ピアの IP アドレス。新しい関連付けが作成されると、行をアクティブにする前
cntpPeersMode	SYNTAX INTEGER { unspecified (0), symmetricActive (1), symmetricPassive (1) } なります。 ::= { cntpPeersVarEntry 8 } オブジェクト識別子 = .1.3.6.1.4.1.9.1.8
cntpPeersStratum	ピア クロックのストラタム ::= { cntpPeersVarEntry 9 } オブジェクト識別子 = .1.3.6.1.4.1.9.1.9
cntpPeersRootDelay	ピアから同期サブネットのルートにあるプライマリリファレンスソースまでの
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計
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
cntpPeersReach	ピアの到達可能性ステータスを判別するために使用されるシフトレジスタ。ピ
cntpPeersOffset	タは、NTP プロトコル プロシージャによって挿入されます。 ::= { cntpPeersV
cntpPeersDelay	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
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、 オブジェクト識別子 = .1.3.6.1.4.1.9.9.168.1.2.1.1.24 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、 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。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。高収益のVoIPサービスが監視され、単方向遅延変動メトリックが収集される場合、タイムスタンプが記録される送信元ノードと宛先ノードは重要なノードと見なされます。

この例では、OSPF階層の例の次にNTP設計が確立されています。したがって、次に説明するレポートは、デバイスのOSPFエリアごとにNTPデバイスをグループ化するようにフォーマットされています。ノードが複数のエリアにインターフェイスを持つ場合、レポート作成ソフトウェアは、レポート用にノードをリストできるエリアを決定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、説明の例としてのみ使用されています。

領域	デバイス	デバイス データ	値
		cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
	Deviceld #1	cntpSysRootDispersion	
		cntpSysRefTime	
	Areald #n	cntpSysPeer	
		cntpSysClock	
		cntpSysStratum	
	Deviceld #n	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)ノードは、NTPアーキテクチャ全体にとって重要であると考えられますが、重要なパフォーマンスモニタリングポイントの時刻の同期には直接関与できないノードです。

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。

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

関連情報

- [RFC 1305 Network Time Protocol](#)
- [RFC 2330 Framework for IP Performance Metrics](#)
- [すべてのISPがv2.84を検討する必要がある基本的なCisco IOS機能](#)
- [テクニカルサポート - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。