使用網路時間協定的最佳實踐

目錄

簡介

本文檔介紹設計網路時間協定的最佳實踐。

必要條件

需求

思科建議您瞭解以下主題：

- 網路時間協定
- 時鐘技術和公共時間伺服器

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

基於網際網路協定(IP)的網路已迅速從傳統的盡力交付模式進步到需要量化效能和可靠性的模式，而且在許多情況下還需要透過服務級別協定(SLA)來保證效能和可靠性。對更深入地瞭解網路特徵的需求促使人們開展大量研究工作，以重要的指標和測量功能為目標來表徵網路行為。許多度量方法的基礎是時間的度量。

網路時間同步（達到現代效能分析所需的程度）是一項基本練習。根據業務模式和提供的服務，網路效能表徵被視為一項重要的競爭服務差異因素。在這種情況下，部署網路管理系統並指導工程資源分析收集的效能資料將產生巨大費用。然而，如果不適當注意常常被忽視的時間同步原則，這些努力就毫無效果。

本文描述網路時間協定(NTP)網路管理功能管理的假設過程定義。您可以將此文章用作假設過程和資訊示例。組織可以對此進行定製以滿足內部目標。

本檔案所提供的資訊分為以下幾個主要章節：

- 術語部分提供了時間同步相關術語的一般定義。
- 概述部分提供有關與系統時間相關的網元硬體的背景資訊、NTP的技術概述以及NTP體系結構的關鍵設計方面。
- NTP部署示例部分提供了NTP部署示例，其中包括WAN、高層園區和低層園區時間分配網路的示例配置。
- 進程定義部分概述了用於完成NTP管理的進程定義。該過程的詳細資訊按目標、績效指標、輸入、輸出和單個任務進行描述。
- 任務定義部分提供了詳細的進程任務定義。每個任務都按照目標、任務輸入、任務輸出、完成任務所需的資源以及任務實施者所需的工作技能進行描述。
- 資料標識部分介紹NTP的資料標識。資料標識考慮資訊的來源。例如，資訊可以包含在簡單網路管理協定(SNMP)管理資訊庫(MIB)中、系統日誌生成的日誌檔案中，也可以透過只能透過命令列介面(CLI)訪問的內部資料結構來獲得。
- 資料收集部分介紹了如何收集NTP資料。資料的收集與資料的位置密切相關。例如，SNMP MIB資料透過多種機制收集，例如陷阱、遠端監控(RMON)警報和事件或輪詢。內部資料結構維護的資料由自動指令碼收集，或在使用者手動登入到系統以發出CLI命令並記錄輸出時收集。
- 資料呈現部分提供了如何呈現資料的報告格式示例。

技術

- 精度- 時鐘絕對值到零偏移的接近程度。
- Accurate -時鐘偏移在特定時間為零時。
- 漂移 -歪斜變化的量度，或時鐘偏移相對於時間的第二次衍生。
- 連線解析度— 比較時鐘時，它是C1和C2解析度的總和。然後，聯合解析度指示由從另一個時鐘生成的時間戳減去一個時鐘生成的時間戳計算的任何時間間隔的精度的保守下界。
- Node -指在本地處理器上例項化NTP協定。節點也可以稱為裝置。
- Offset -時鐘報告的時間與協調世界時(UTC)定義的實際時間之間的差。如果時鐘報告時間Tc，並且真即時間是Tt，則時鐘偏移是Tc - Tt。
- Peer -指在遠端處理器上例項化NTP協定，該遠端處理器透過網路路徑從本地節點連線。
- 相對偏移 -當比較兩個時鐘C1和C2時，實際時間的概念由時鐘C1報告的時間取代。例如，時鐘C2在特定時刻相對於C1的偏移是Tc2 - Tc1，即C2和C1報告的瞬時時間差。
- 解析度 -時鐘時間更新的最小單位。解析度是以秒來定義。但是，解析度是相對於時鐘報告時間，而不是相對於真即時間。例如，10毫秒的解析度表示時鐘以0.01秒的增量更新其時間概念，而不表示這是更新之間的實際時間量。

注意：時鐘的解析度非常高，但仍不準確。

- 傾斜 -時脈頻率差，或相對於時間偏移量的一階導數。

- 同步(Synchronize) -當兩個時鐘彼此相對準確（相對偏移為零）時，它們將被同步。時鐘可以同步，但就它們講述真即時間的能力而言，它們仍然不準確。

概觀

裝置概觀

時間服務的核心是系統時鐘。系統時鐘從系統啟動時開始運行，並跟蹤當前日期和時間。系統時鐘可以從多個源進行設定，並且反過來可以用於透過各種機制將當前時間分配到其他系統。某些路由器包含電池供電日曆系統，可跟蹤系統重新啟動和停電期間的日期和時間。此行事曆系統一律用來在系統重新啟動時初始化系統時鐘。也可以將其視為權威的時間源，如果沒有其他可用源，則透過NTP進行重新分配。此外，如果啟用NTP，日曆將從NTP定期更新，這補償了日曆時間的固有偏差。初始化具有系統日曆的路由器時，系統會根據其內部電池供電日曆中的時間設定系統時鐘。在沒有日曆的模型上，系統時鐘被設定為預定的時間常數。系統時鐘可以從下面列出的源進行設定。

- NTP
- 簡易網路時間通訊協定(SNTP)
- 虛擬整合網路服務(VINES)時間服務
- 手動配置

某些低端Cisco裝置僅支援SNTP。SNTP是NTP的簡化版本，僅供客戶端使用。SNTP只能從NTP伺服器接收時間，不能用於為其他系統提供時間服務。SNTP提供的時間通常為準確時間的100毫秒以內。此外，SNTP不會對流量進行身份驗證，但您可以配置擴展訪問清單來提供一些保護。與NTP客戶端相比，SNTP客戶端更容易受到不合規伺服器的攻擊，並且只能在不需要強身份驗證的情況下使用。

系統時鐘提供到下面列出的服務的時間。

- NTP
- VINES時間服務
- 使用者show命令
- 記錄和調試消息

系統時鐘根據UTC(也稱為葛林威治標準時間(GMT))在內部跟蹤時間。您可以配置有關本地時區和夏時制的資訊，以便正確顯示相對於本地時區的時間。系統時鐘會記錄時間是否為權威時間。如果時間不是授權的，則只能用於顯示目的，且無法重新分配。

NTP概述

NTP旨在同步電腦網路中的時間。NTP透過使用者資料包協定(UDP)運行，埠123同時作為源和目標，然後透過IP運行。NTP版本3 RFC 1305 用於在一組分散式時間伺服器和客戶端之間同步計時。網路上的一組節點透過NTP標識和配置，這些節點形成同步子網，有時也稱為重疊網路。雖然可以

存在多個主伺服器，但無需使用選舉協定。

NTP網路通常從權威時間源（例如連線到時間伺服器的無線電時鐘或原子時鐘）獲取時間。然後，NTP會將此時間分配到整個網路。NTP客戶端在其輪詢間隔（從64秒到1024秒）內與其伺服器進行事務，該輪詢間隔會根據NTP伺服器和客戶端之間的網路條件隨時間動態變化。另一種情況發生在路由器與錯誤的NTP伺服器（例如，色散較大的NTP伺服器）通訊時；路由器還會增加輪詢間隔。同步兩台電腦時每分鐘不需要超過一個NTP事務。

NTP使用層級的概念來描述一台電腦與權威時間源之間相隔的NTP跳數。例如，第1層時間伺服器直接連線了無線電時鐘或原子時鐘。然後透過NTP將其時間傳送到第2層時間伺服器，以此類推。運行NTP的電腦會自動選擇其配置為與NTP通訊的最低層數的電腦作為其時間源。此策略可有效地建立NTP發言人的自組織樹。NTP對客戶端和時間伺服器之間的關係中的以下三個關鍵變數進行穩健的估計，因此它在資料包交換網路非確定性路徑長度上表現良好。

- 網路延遲
- 時間資料包交換的分散-測量兩台主機之間的最大時鐘誤差。
- 時鐘偏移量-應用於客戶端時鐘的校正以同步它。

在長距離廣域網(WAN)（2000公里）上定期實現10毫秒級的時鐘同步，在區域網(LAN)上定期實現1毫秒級的時鐘同步。

NTP與時間不準確的電腦同步有兩種方式。首先，NTP從不與自身未同步的機器同步。其次，NTP會比較多台電腦報告的時間，即使其層級較低，也不會與時間明顯不同的電腦同步。

運行NTP（關聯）的電腦之間的通訊通常以靜態方式配置。每台電腦都獲得了必須與之形成關聯的所有電腦的IP地址。透過在具有關聯的每對機器之間交換的NTP消息，可以實現準確計時。但是，在LAN環境中，可以將NTP配置為使用IP廣播消息。此替代方案降低了配置的複雜性，因為可以將每台電腦配置為傳送或接收廣播消息。但是，由於資訊流是單向的，因此計時準確度會略微降低。

電腦上保留的時間是一項關鍵資源，強烈建議您使用NTP的安全功能，以避免意外或惡意設定不正確的時間。可用的兩種安全功能是基於訪問清單的限制方案和加密的身份驗證機制。

在某些思科IOS®軟體版本中，思科實施NTP支援第1層服務。如果版本支援ntp refclock命令，則可以連線無線電時鐘或原子時鐘。某些版本的Cisco IOS支援Trimble Palisade NTP同步套件（僅適用於Cisco 7200系列路由器）或電信解決方案全球定位系統(GPS)裝置。如果網路使用Internet上的公共時間伺服器，並且網路與Internet隔離，則Cisco實施NTP後，可以配置一台電腦，使其充當透過NTP進行同步的機器，而實際上它已透過其他方式確定時間。然後其他電腦透過NTP與該電腦同步。

NTP設計標準

同步子網中的每個客戶端（也可以是更高層客戶端的伺服器）都會選擇其中一個要同步的可用伺服器。這通常來自它可訪問的最低層級伺服器。但是，這並非總是最佳配置，因為NTP的運行前提是必須用一定程度的不信任來檢視每個伺服器時間。NTP更願意訪問較低層時間的多個源（至少三個），因為它隨後可以應用協定演算法來檢測其中任意一個源的異常。通常情況下，當所有伺服器都

同意時，NTP會根據最低層級、最接近層級（網路延遲）和宣告精度來選擇最佳伺服器。這意味著，雖然必須旨在為每個客戶端提供三個或更多個較低層時間的源，但其中幾個源只能提供備份服務，在網路延遲和層數方面品質可能較低。例如，從本機伺服器無法直接存取的低層來源接收時間的相同層級對等體，也可以提供良好的備份服務。

NTP通常首選較低層級伺服器，而不是較高層級伺服器，除非較低層級伺服器的時間明顯不同。該演算法能夠檢測時間源何時可能極不準確或瘋狂，並且在這些情況下阻止同步，即使不準確的時鐘位於較低層級。而且它永遠不能將裝置與自身未同步的另一台伺服器同步。

為了宣告伺服器是否可靠，它需要透過許多健全性檢查，例如：

- 如果監控程式在較長時間間隔後不更新此資訊，則實施必須包括可防止陷阱傳輸的正常超時。
- 還包括額外的健全性檢查以驗證和範圍限制，並避免使用非常舊的資料。
- 已增加檢查以警告振盪器已太長，而沒有從參考源進行更新。
- 在嚴重網路擁塞的情況下，當參考源快速變化時，增加peer.valid和sys.hold變數以避免不穩定。增加了peer.config 、 peer.authenticable和peer.authenticable位來控制特殊功能並簡化配置。

如果其中至少有一個檢查失敗，路由器會將其宣告為不正常。

關聯模式

接下來的幾節將介紹NTP伺服器用於相互關聯的關聯模式。

- 使用者端/伺服器
- 對稱主動/被動
- 廣播

使用者端/伺服器模式

從屬從屬從屬從屬端和伺服器通常以從屬端/伺服器模式運作，在這種模式中，從屬端或從屬伺服器可以同步處理至群組成員，但沒有任何群組成員可以同步處理至從屬端或從屬伺服器。這樣可以防止發生故障或協定攻擊。

客戶端/伺服器模式是最常見的Internet配置。它以具有無狀態伺服器的傳統遠端過程呼叫(RPC)模式運行。在此模式中，客戶端向伺服器傳送請求，並期望在未來某個時間得到回覆。在某些情況下，這被描述為輪詢操作，因為客戶端會輪詢來自伺服器的時間和身份驗證資料。使用者端是在使用者端模式下使用server指令和指定的網域名稱伺服器(DNS)名稱或位址設定的。伺服器不需要先前的組態。

在通用客戶端/伺服器模型中，客戶端向一個或多個伺服器傳送NTP消息，並在收到回覆時進行處理。伺服器交換地址和埠，覆蓋消息中的某些欄位，重新計算校驗和，並立即返回消息。NTP消息中包含的資訊允許客戶端確定相對於本地時間的伺服器時間，然後根據需要調整本地時鐘。此外，該消息還包含用於計算預期計時準確性和可靠性以及選擇最佳伺服器的資訊。

為大量客戶端提供同步的伺服器通常作為由三個或更多個相互冗餘的伺服器組成的組運行，並且每個伺服器在客戶端/伺服器模式下與三個或更多個第1層或第2層伺服器運行，以及以對稱模式運行該組的所有其他成員。這樣可以防止發生一個或多個伺服器無法運行或提供錯誤時間的故障。NTP演算法經過精心設計，可在部分配置的同步源意外或故意提供錯誤的時間時抵禦攻擊。在這些情況下，使用特殊的投票程式來辨識虛假來源並丟棄其資料。為了保證可靠性，選定的主機可以配備外部時鐘，並用於在主伺服器和/或輔助伺服器或其之間的通訊路徑出現故障時進行備份。

在客戶端模式中配置關聯通常由配置檔案中的伺服器宣告指示，表示您希望從遠端伺服器獲取時間，但您不想為遠端伺服器提供時間。

對稱主動/被動模式

對稱主動/被動模式適用於一組低層對等體彼此作為相互備份的配置。每個對等體使用一個或多個主參考源（例如無線電時鐘）或可靠輔助伺服器的子集來操作。如果其中一個對等體丟失所有參考源或僅停止操作，其他對等體將自動重新配置，以便時間值可以從當前對等體流向隊列中的所有其他對等體。在某些上下文中，此操作被描述為推拉操作，因為對等體根據特定配置拉動或推移時間和值。

在對稱-主動模式下的關聯配置（通常由配置檔案中的對等宣告表示）向遠端伺服器表明使用者希望從遠端伺服器獲取時間，並且使用者也願意在必要時向遠端伺服器提供時間。此模式適用於涉及透過不同網路路徑互連的多個冗餘時間伺服器的配置中，目前網際網路上大多數第1層和第2層伺服器都是這種情況。

對稱模式最常用於作為互備組運行的兩台或多台伺服器之間。在這些模式下，組成員中的伺服器會根據網路抖動和傳播延遲來安排同步路徑，以實現最大效能。如果一個或多個組成員失敗，剩餘成員將根據需要自動重新配置。

當指定了另一個對等體的DNS名稱或地址時，可以使用peer命令將對等體配置為對稱活動模式。以這種方式在對稱主動模式下也會設定另一個對等點。

注意：如果未以此方式專門配置另一個對等體，則會在收到對稱主動消息時啟用對稱被動關聯。由於入侵者可以模擬對稱活動對等體並注入錯誤的時間值，因此必須始終驗證對稱模式。

廣播和/或組播模式

在準確性和可靠性要求較低的情況下，可將客戶端配置為使用廣播和/或組播模式。通常，具有相依使用者端的伺服器不會使用這些模式。其優點是不需要為特定伺服器配置客戶端，這允許所有運行客戶端使用相同的配置檔案。廣播模式要求廣播伺服器位於同一子網上。由於路由器不傳播廣播消息，因此僅使用同一子網上的廣播伺服器。

廣播模式適用於涉及一台或多台伺服器以及可能大量客戶端的配置。使用broadcast命令和本地子網地址配置廣播伺服器。廣播客戶端是使用broadcastclient命令配置的，該命令允許廣播客戶端對在任何介面上接收的廣播消息進行響應。由於入侵者可以模擬廣播伺服器並注入錯誤的時間值，因此必須始終驗證此模式。

設定NTP跳越秒

您可以使用ntp leap {add | delete}命令以插入leap秒。有選項可新增或刪除leap秒。發生這種情況有兩個限制：

- 時鐘必須處於同步狀態。
- 這個指令只有在跳躍發生前的一個月內被接受。如果當前時間在跳轉出現的1個月之前，則無法設定跳躍。

設定之後，跳越秒會新增或刪除到最後一秒，如下所示：

<#root>

```
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架構

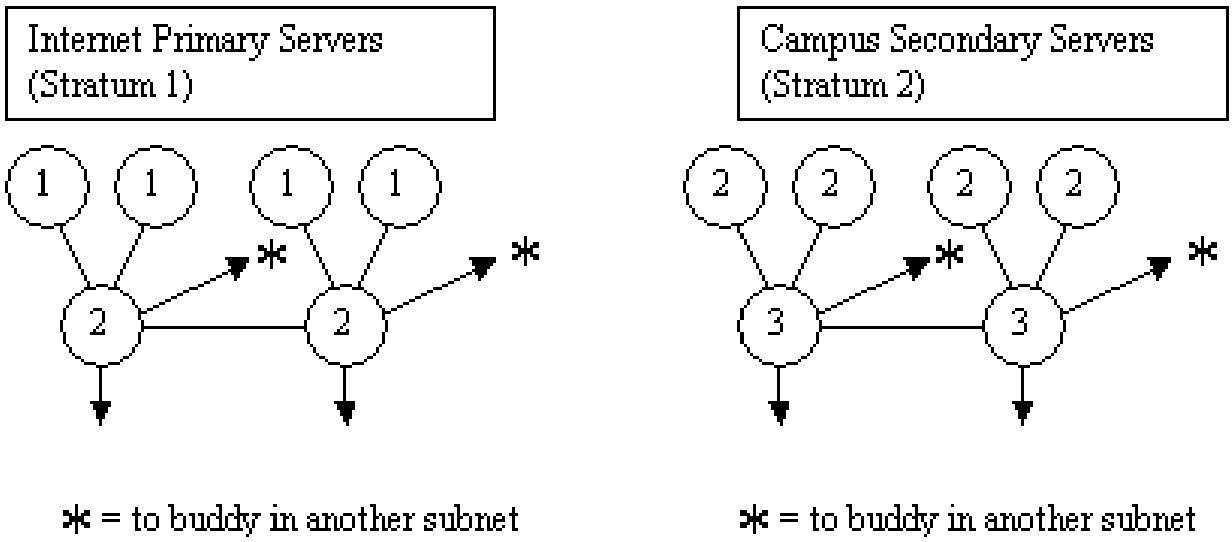
NTP體系結構可以使用以下三種結構：

- 扁平對等體結構
- 階層式結構
- 星型結構

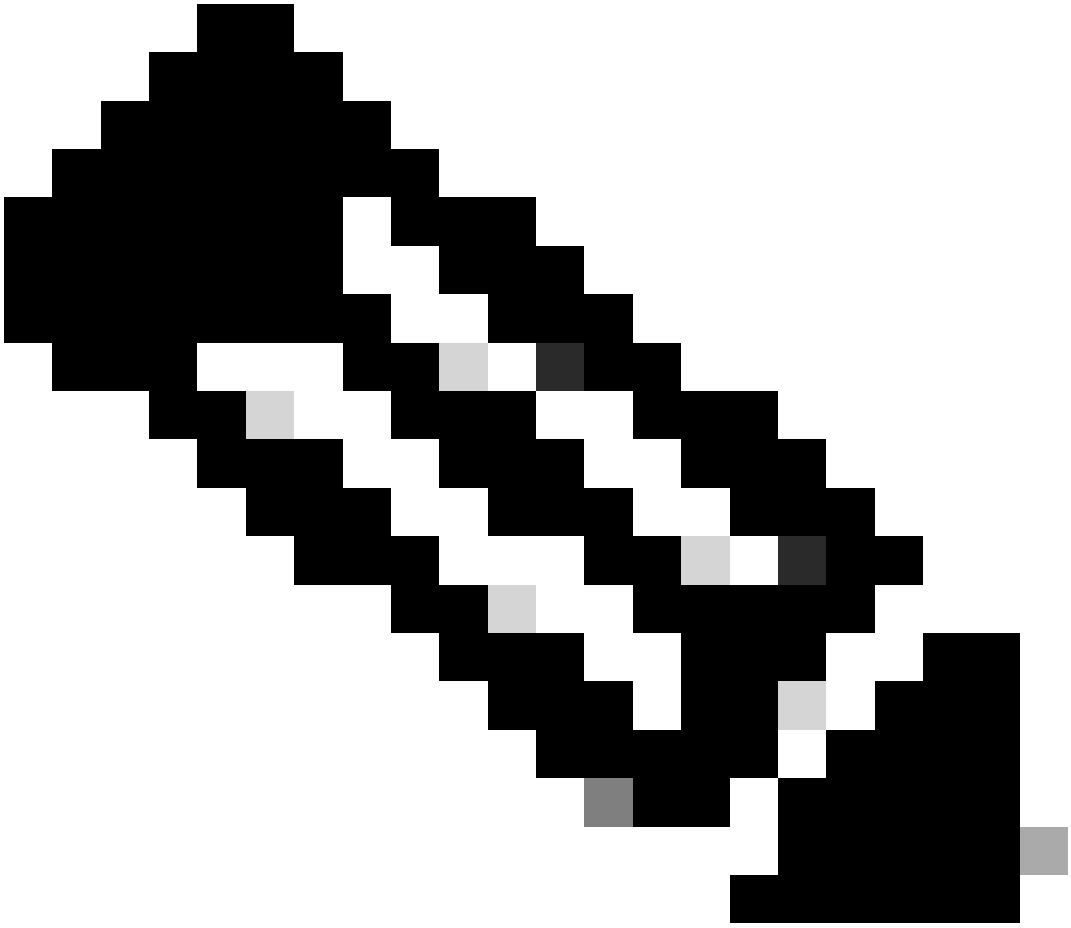
在平面對等結構中，所有路由器都相互對等，少數幾個地理上獨立的路由器配置為指向外部系統。隨著NTP網格的每個新成員，時間的收斂時間會越來越長。

在分層結構中，路由分層結構被複製到NTP分層結構中。核心路由器與外部時間源具有客戶端/伺服器關係，內部時間伺服器與核心路由器具有客戶端/伺服器關係，內部使用者（非時間伺服器）路由器與內部時間伺服器具有客戶端/伺服器關係，以此類推，向下展開樹。這些關係稱為階層比例。分層結構是首選技術，因為它提供了一致性、穩定性和可擴充性。

可擴展的NTP架構具有分層結構，如下圖所示。



可擴展的NTP架構



注意：顯示可擴展分層NTP部署的一系列圖形。第一個圖顯示了兩個NTP第2層裝置，每個連線到兩個第1層裝置（如前面的第2層裝置圖所示），另一個子網中的夥伴以星號表示。此外，每個第2層裝置都有一個向下箭頭。第二個圖具有相同的佈局，但第2層裝置是第1層裝置所在的位置，第3層裝置是第2層裝置所在的位置。第三個圖表有一個第4層裝置連線到三個第3層裝置。總之，圖中顯示了一個拓撲，其中每台裝置連線到2-3台裝置，其中一層比自己低（更好）。

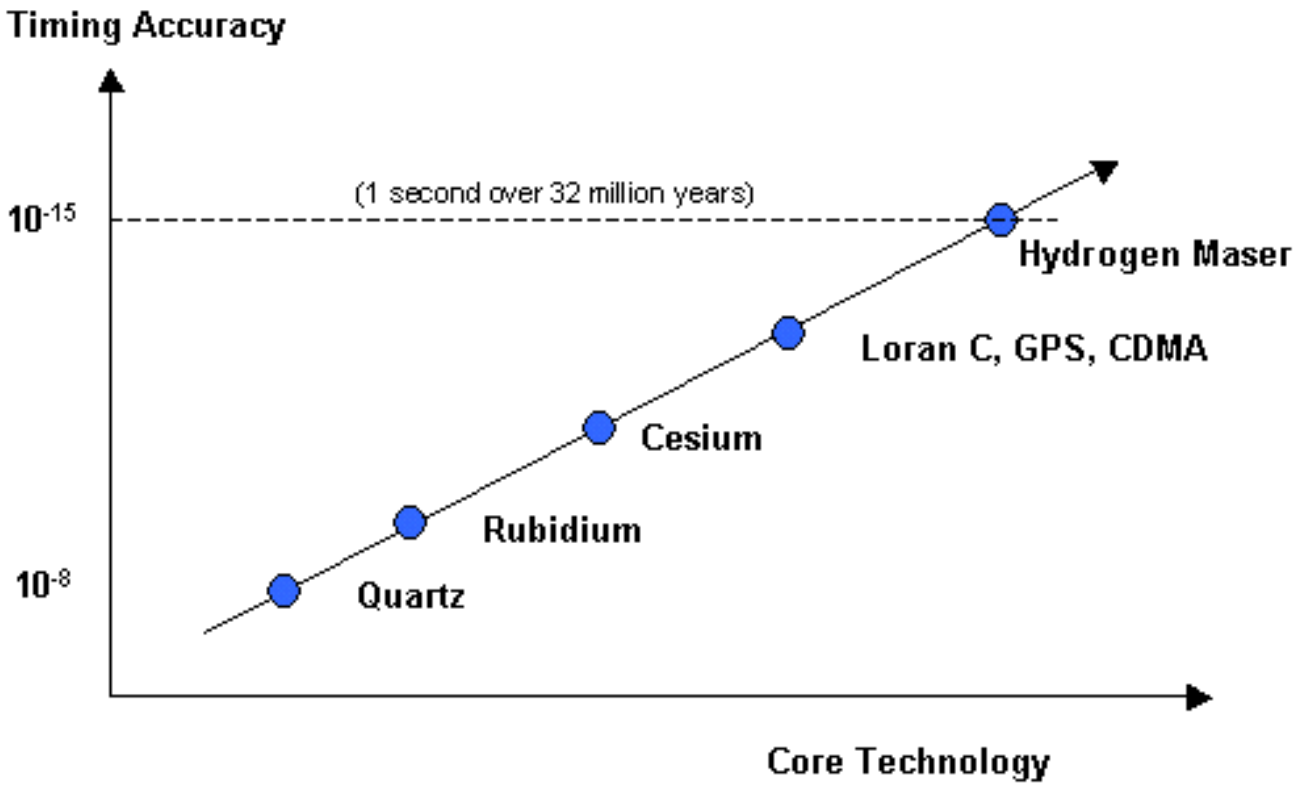
在星型結構中，所有路由器都有一個客戶端/伺服器關係，而核心中只有少量時間伺服器。專用時間伺服器是恆星的中心，通常是與外部時間源或它們自己的GPS接收器同步的UNIX系統。

時鐘技術和公共時間伺服器

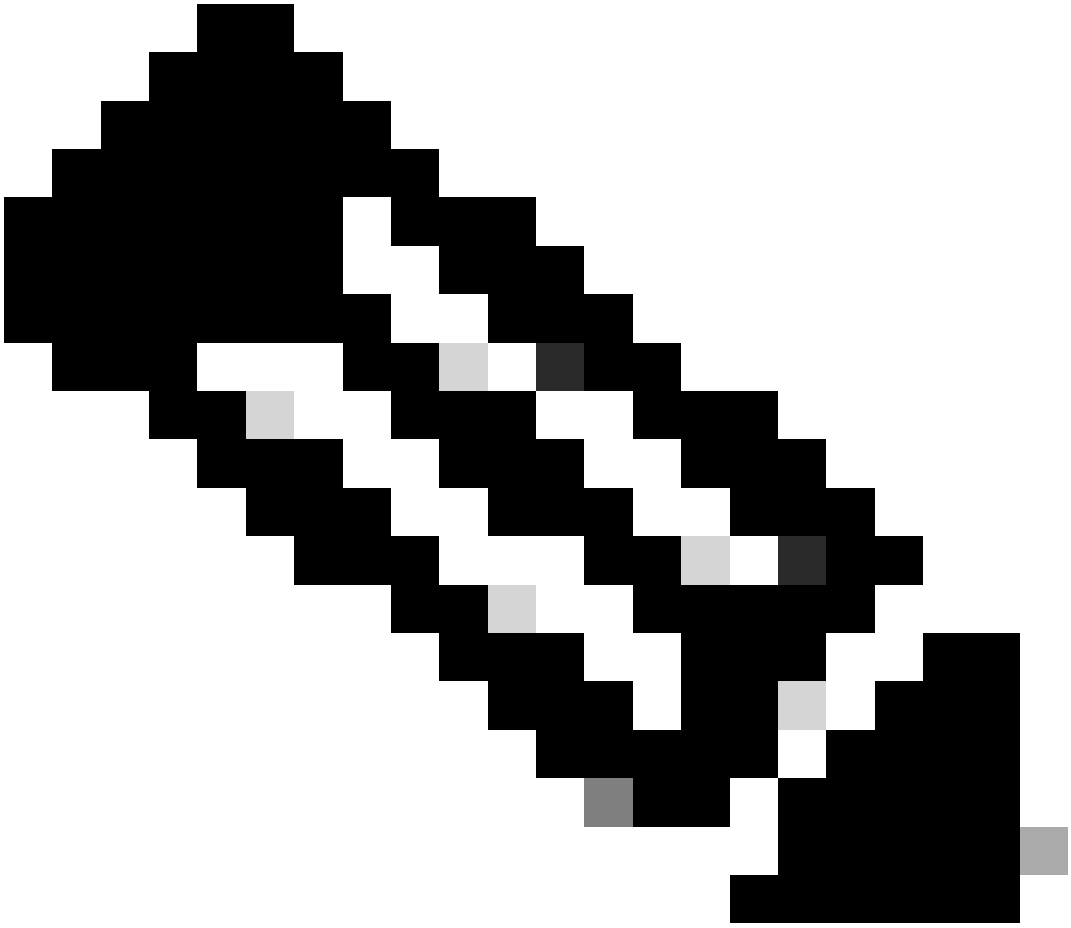
Internet NTP子網目前包括50多個透過無線電、衛星或數據機直接與UTC同步的公共主伺服器。通常，客戶端數量相對較少的客戶端工作站和伺服器不會與主伺服器同步。大約100個公共輔助伺服器與主伺服器同步，並且提供與Internet上總數超過100,000個客戶端和伺服器的同步。公共NTP時間伺服器清單經常更新。此外，還有許多通常不供公眾使用的專用主伺服器和輔助伺服器。

注意：PIX和ASA不能配置為NTP伺服器，但是它們可以配置為NTP客戶端。

在某些情況下，如果私有企業需要高度準確的時間服務，例如用於IP語音(VoIP)測量的單向度量，網路設計人員可以選擇部署私有外部時間源。下圖顯示目前技術相對準確度的比較圖表。



比較圖表



註：一個圖表，它呈現從石英（10到負第8次方）到氫激射器（10到負第15次方）的時間保持方式越來越精確。後者表示在3200萬年的時間內，精度損失約為1秒。這兩種方法中列出的其他方法（從最少到最精確）有銣原子、銫、羅蘭C、GPS和CDMA。最後三個（羅蘭C、GPS和CDMA）一起列出。

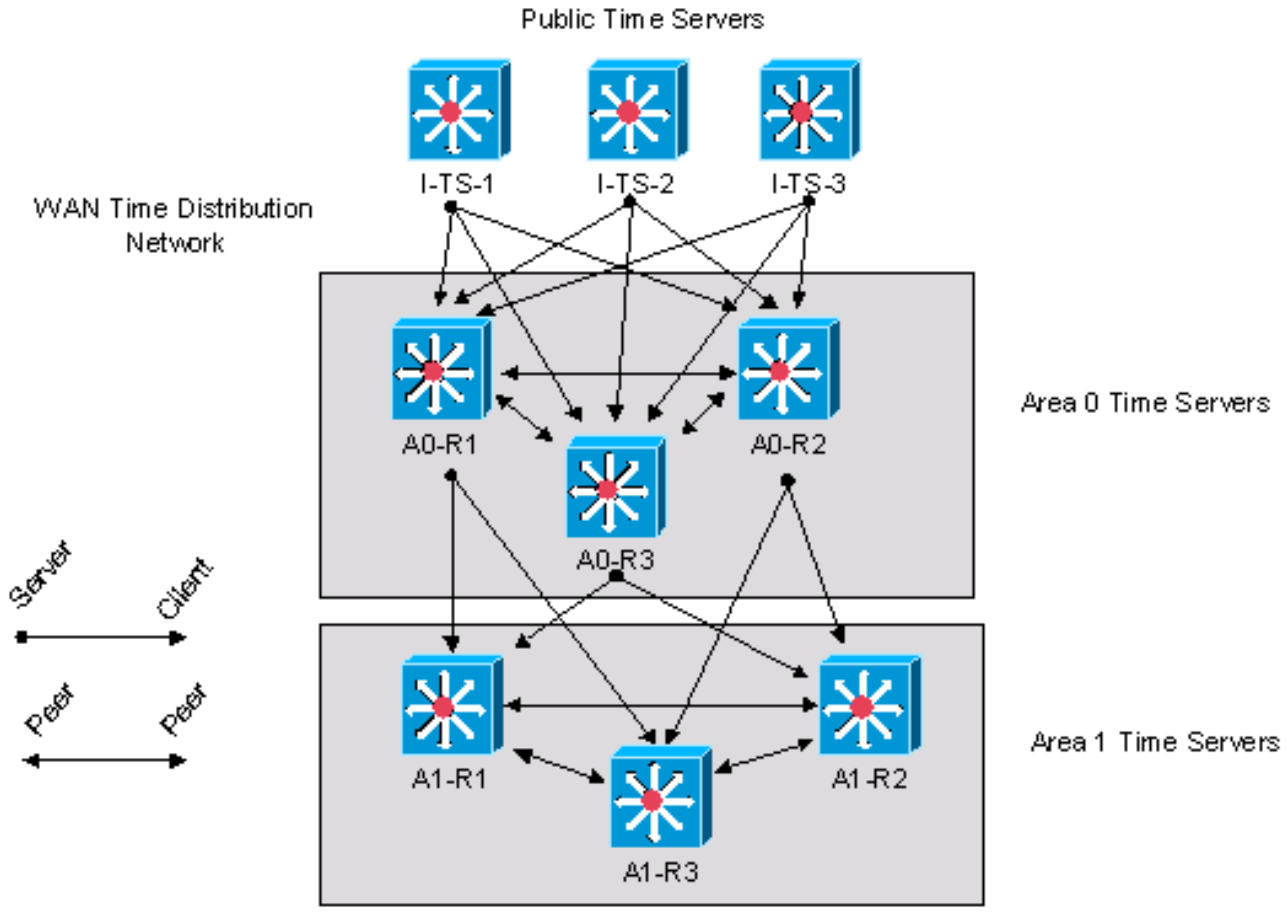
直到最近，由於外部時間源的高品質成本，外部時間源的使用尚未在企業網路中廣泛部署。但是，隨著服務品質(QoS)要求的提高以及時間技術的成本不斷降低，企業網路的外部時間源是一個可行的選擇。

NTP部署示例

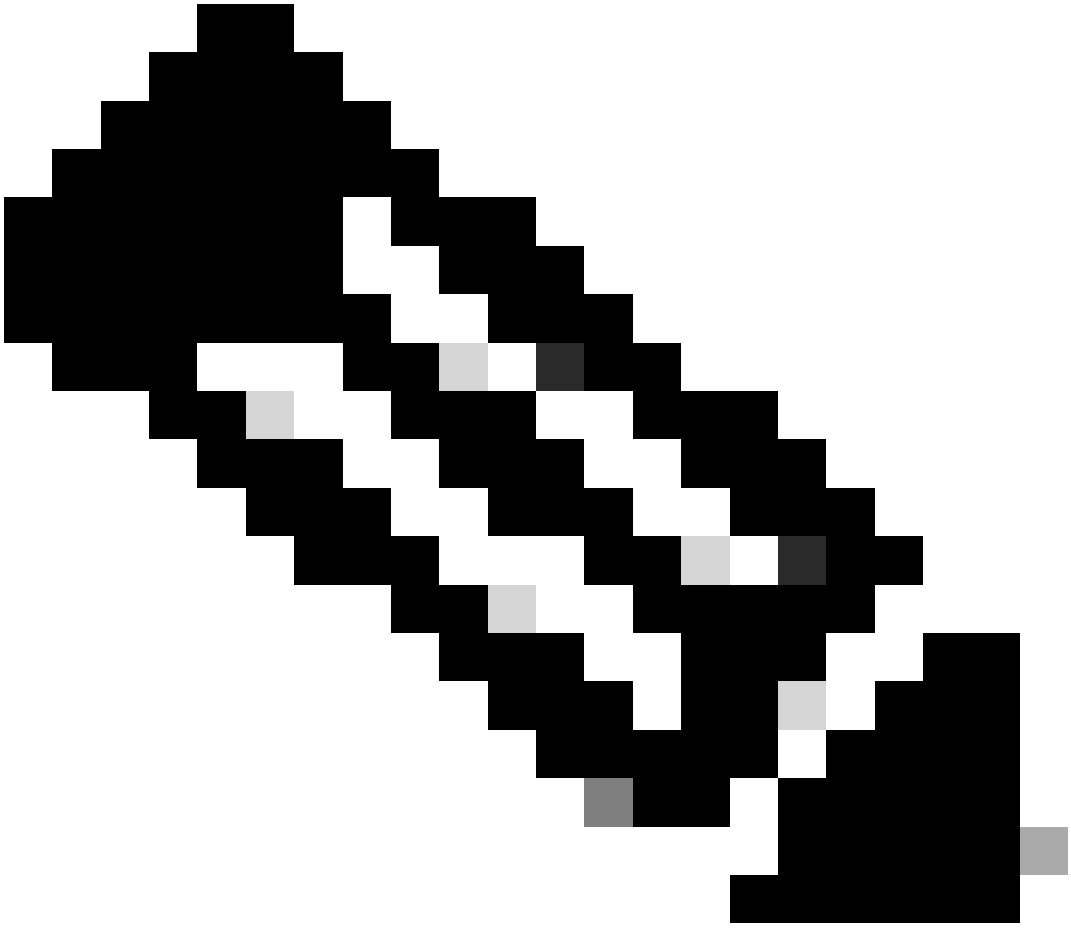
WAN時間分配網路

在下圖中，公司自治系統(AS)從三個公共時間伺服器獲取時間資訊。公司AS顯示為區域0和區域1時間伺服器。在本示例中，NTP層次結構描述了開放最短路徑優先(OSPF)層次結構。但是，OSPF不是NTP的先決條件。它僅用作說明性示例。NTP可以沿其他邏輯分層邊界部署，例如增強型內部網

關路由協定(EIGRP)分層結構或標準核心/分佈/接入分層結構。



WAN時間分配網路



注意：此圖展示了跨多個網路的NTP拓撲。區域1中的三台裝置(OSPF)是彼此的對等裝置，也是區域0中伺服器的客戶端。區域0中的三個裝置是彼此的對等裝置、公共時間伺服器的客戶端和區域1中客戶端的伺服器。公共時間伺服器只顯示為區域0中客戶端的伺服器。

本示例是裝置A0-R1的Cisco IOS配置，如前圖所示。

```
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.
```

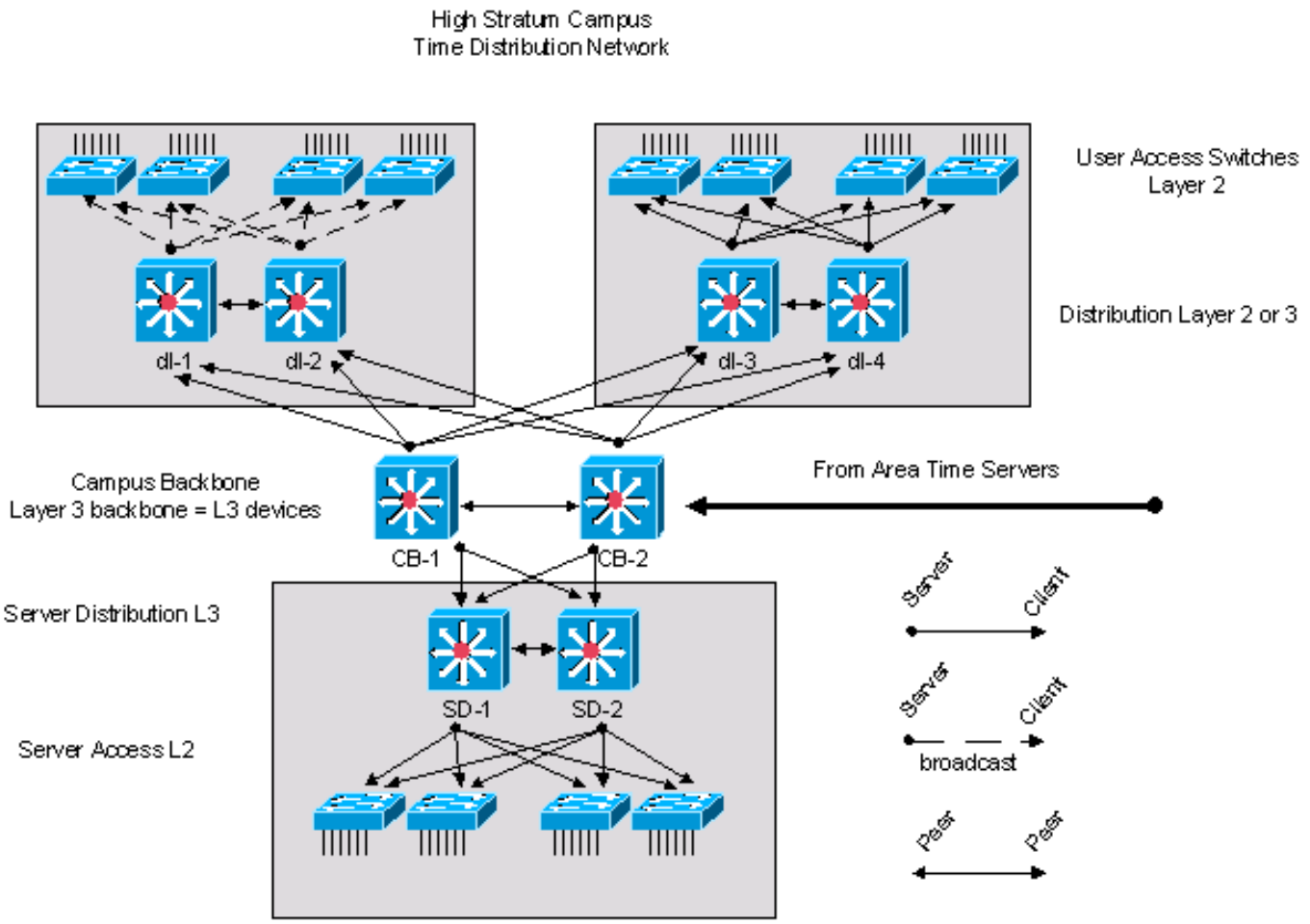
```
!--- Cisco IOS can then obtain its clock from
!--- the hardware calendar.


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 <AO-R2>
access-list 5 permit <AO-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>
```

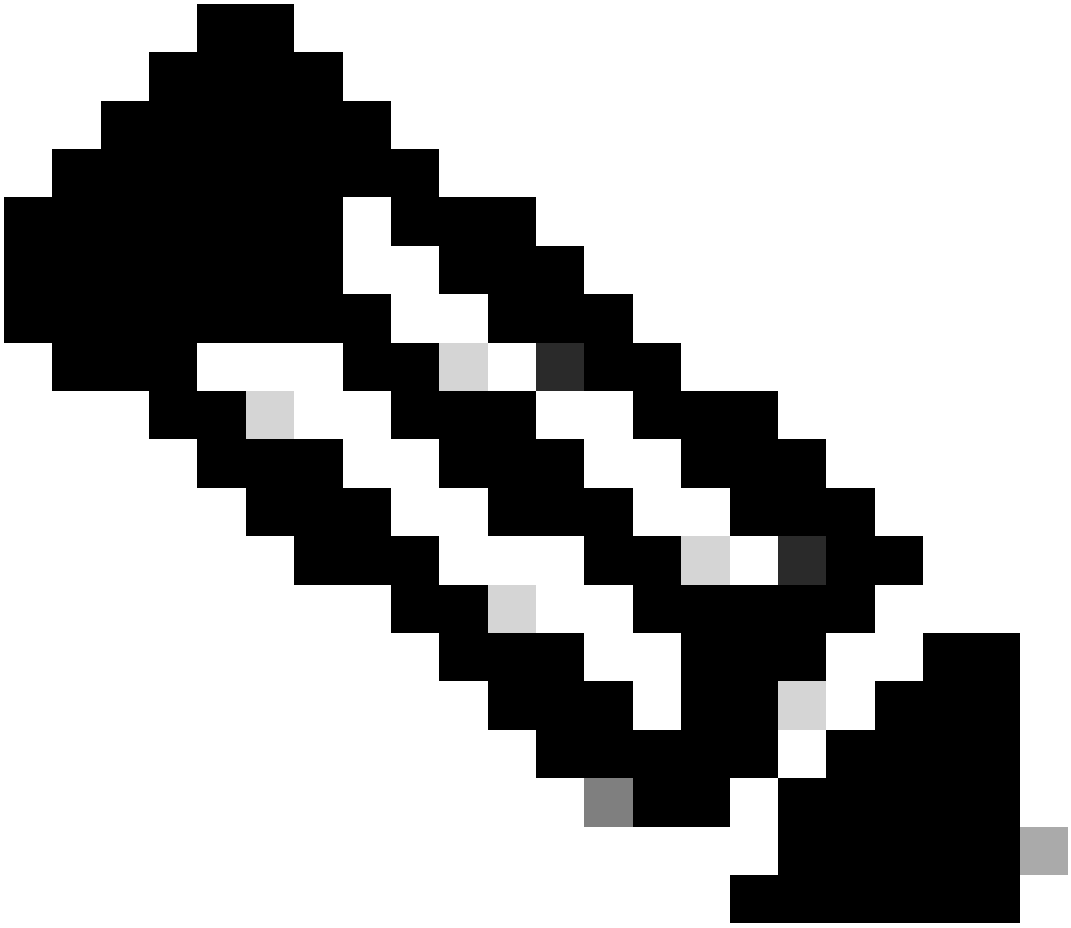
高層園區時間分配網路

上一節描述了WAN時間分配網路。本部分在層次結構中下移一步，討論高層園區網路中的時間分配。

人們認為，高層園區網路中時間分配的主要差異是廣播關聯模式的可能使用。如前所述，廣播關聯模式簡化了LAN的配置，但降低了時間計算的準確性。因此，必須權衡維護成本與效能測量的準確性。


High Stratum Campus
Time Distribution Network
User Access Switches
Layer 2
Distribution Layer 2 or 3
dl-1
dl-2
dl-3
dl-4
Campus Backbone
Layer 3 backbone = L3 devices
From Area Time Servers
CB-1
CB-2
Server Distribution L3
SD-1
SD-2
Server Access L2
Server
Client
Server
Client
broadcast
Peer
Peer

高層園區時間分配網路



註：標題為「High Stratum Campus Time Distribution Network」的圖，其中包括通用三層拓撲（主幹、分佈、接入）。接入交換機是分佈層交換機的客戶端，分佈層交換機是主幹交換機的客戶端，而主幹交換機是區域時間伺服器的客戶端（圖中未顯示）。分佈層交換機被分為兩組，並且僅與對中的另一交換機具有對等關係。兩台主幹交換器也是彼此的對等交換器。四個接入交換機（左上角）顯示為帶點箭頭的廣播客戶端，而所有其他客戶端-伺服器和對等體關係是非廣播的。

上圖中所示的高層園區網路來自標準的思科園區網路設計，包含三個元件。園區核心包含兩個標籤為CB-1和CB-2的第3層裝置。位於圖下方的伺服器元件包含兩個第3層路由器，標籤為SD-1和SD-2。伺服器塊中的其他裝置是第2層裝置。左上角有一個標準訪問塊，帶有兩個標籤為dl-1和dl-2的第3層分佈裝置。其餘裝置為第2層交換機。在此客戶端訪問塊中，使用廣播選項分配時間。在右上方，還有另一個使用客戶端/伺服器時間分配配置的標準訪問塊。

園區主幹裝置與客戶端/伺服器模型中的區域時間伺服器同步。

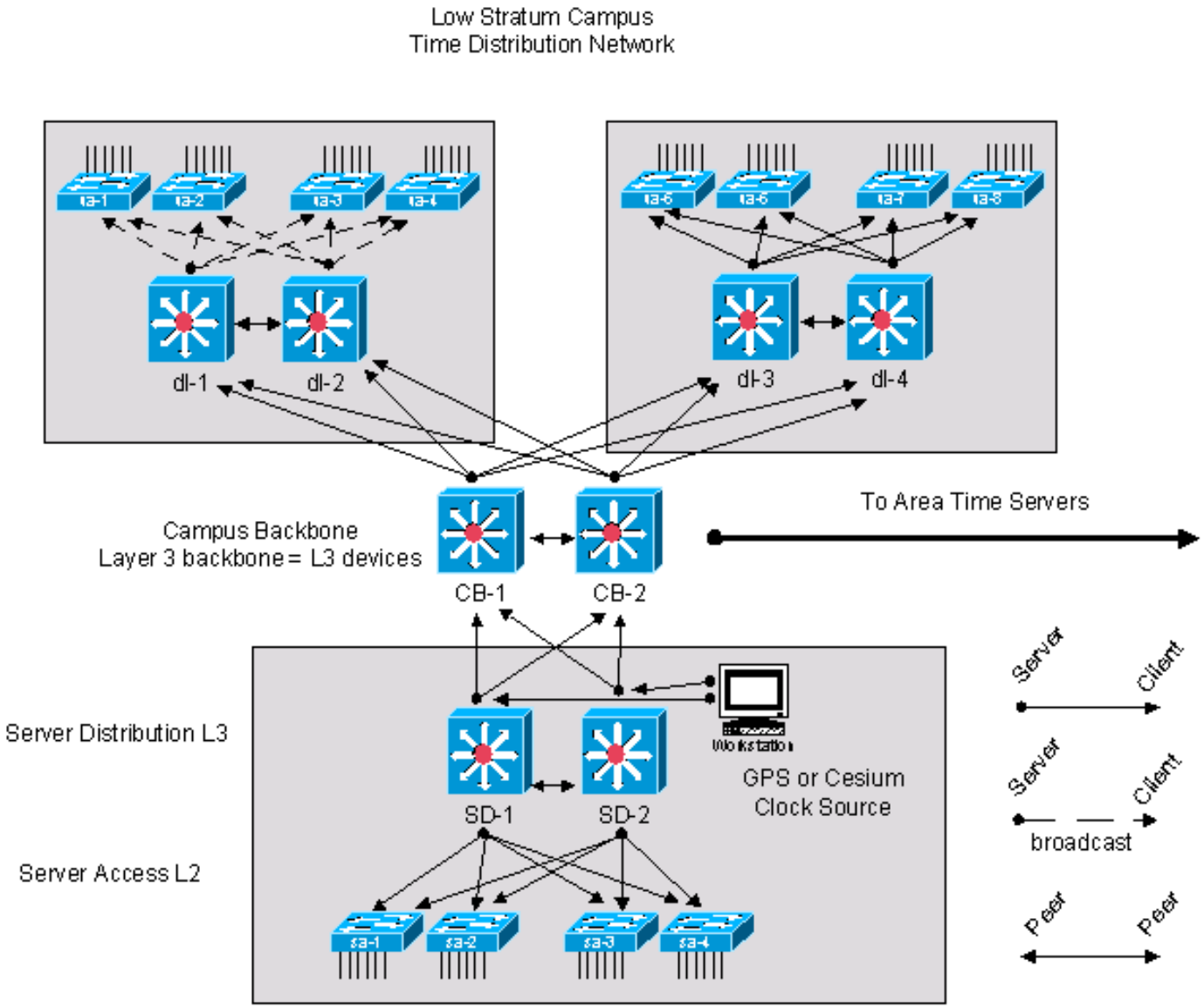
以下是dl-1第3層分佈裝置的配置：

```
!--- 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>
```

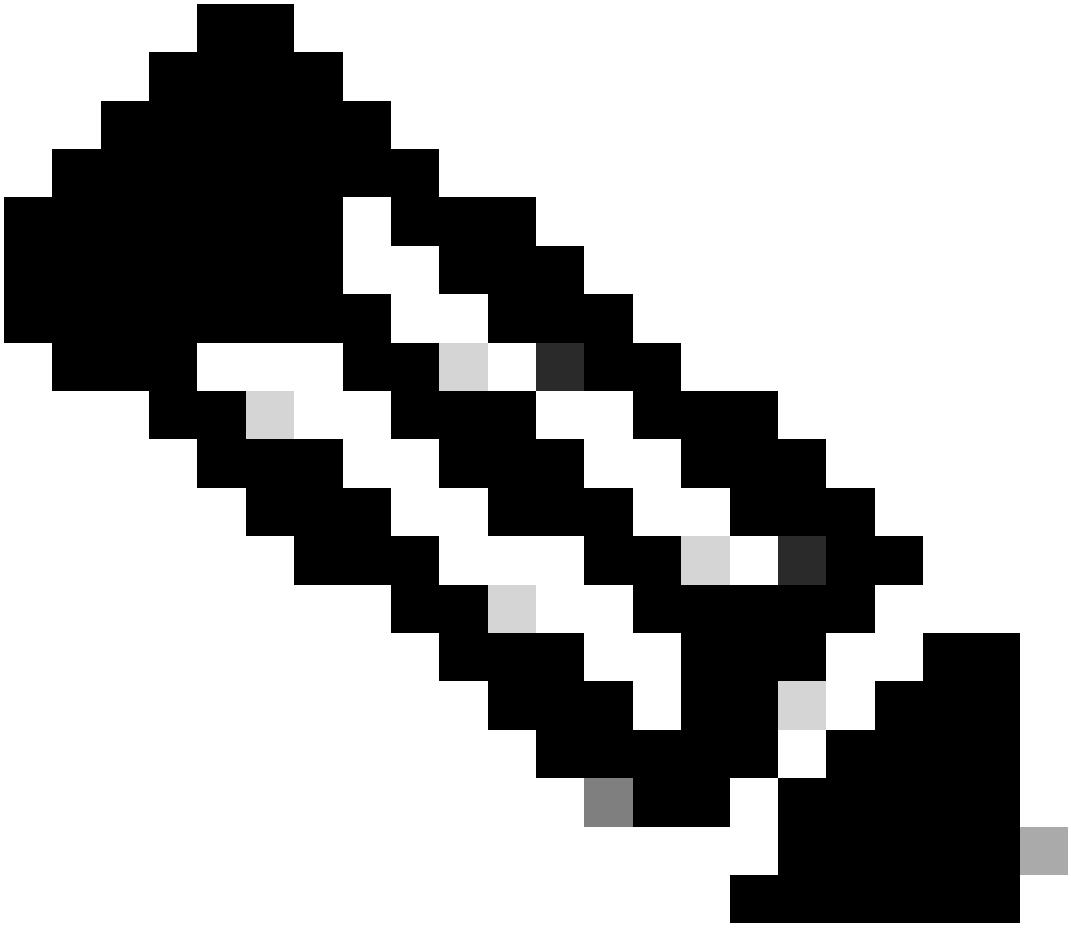
低層園區時間分配網路

在下圖中，在低層園區網路的中央資料中心提供GPS或銫時間源。這會在私人網路上提供第1層時間來源。如果私有網路中有多個GPS或銫時間源，則必須修改私有網路中的時間分配以利用可用的時間源。

一般而言，與先前範例相同的原則與組態亦適用。在這種情況下，主要的區別是同步樹的根是私有時間源，而不是來自Internet的公有時間源。這改變了時間分配網路的設計，以利用高精度專用時間源。私有時間源分佈在整個私有網路中，其層次和模組化原則已在前面幾節中介紹。



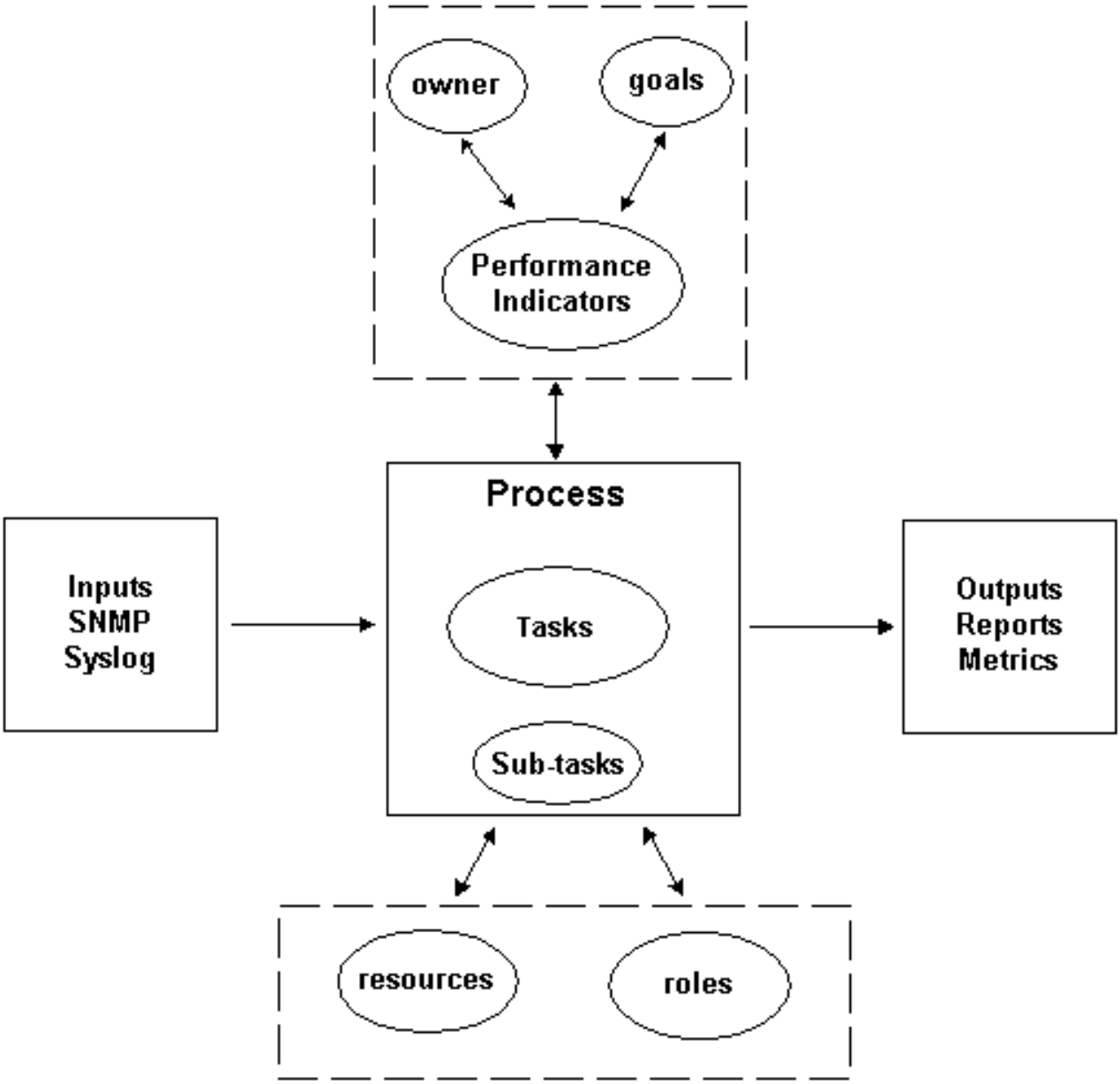
低層園區時間分配網路



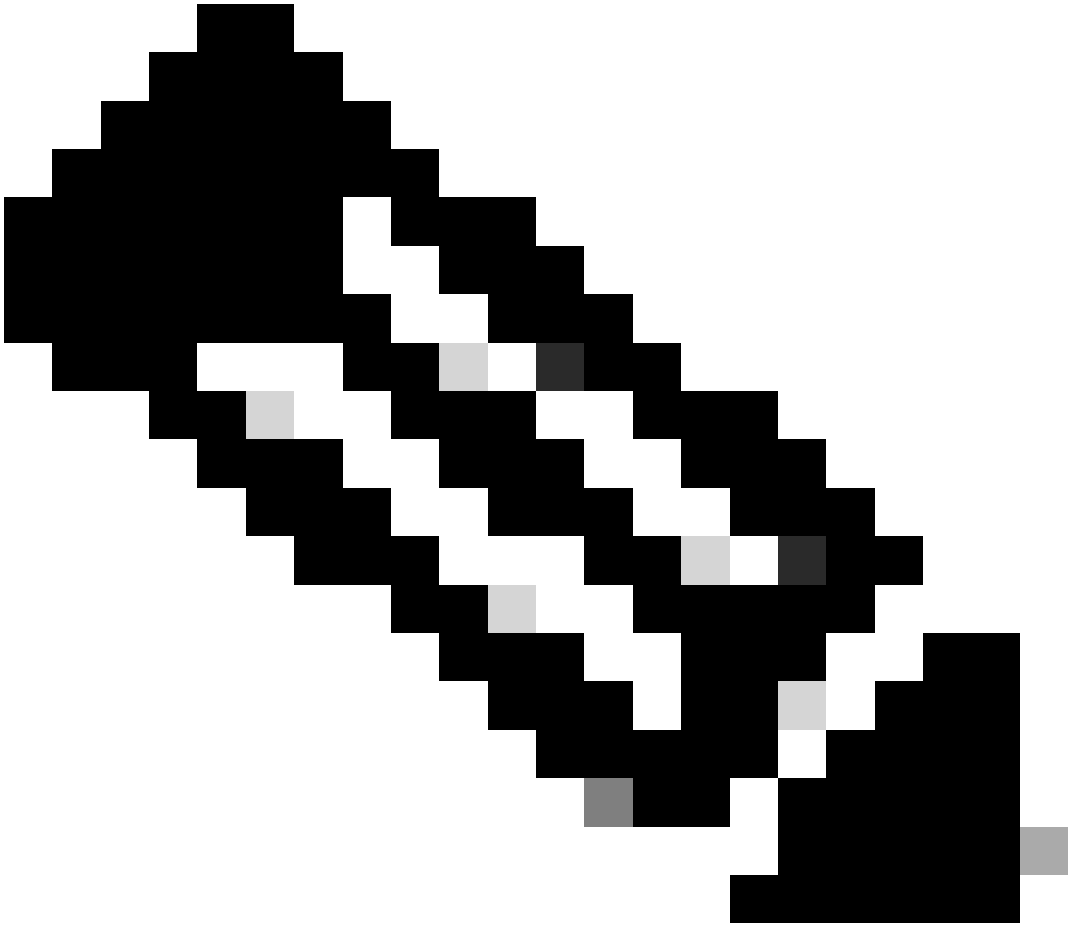
註：標題為「低層園區時間分配網路」的圖，其中包括通用三層拓撲（主幹、分佈、接入）。 兩台配電開關連線了GPS或鈀鐘。直接連線到這些分佈層交換機的接入層交換機和主幹交換機是這些分佈層交換機的客戶端。網路上的所有其它分佈層交換機都是主幹交換機的客戶端，其餘的接入層交換機也是其直連分佈層交換機的客戶端。 四個接入交換機（左上角）顯示為帶點箭頭的廣播客戶端，而所有其他客戶端-伺服器和對等體關係是非廣播的。

流程定義

流程定義是由代理程式所執行的一系列動作、活動及變更，這些代理程式旨在達成目的或達成目標。 過程控制是計畫和調整的過程，目的是以有效和高效的方式執行過程。如下圖所示。


owner
goals
Performance Indicators
Process
Inputs
SNMP
Syslog
Tasks
Sub-tasks
Outputs
Reports
Metrics
resources
roles

一系列流程



附註：指定此檔案所使用之處理方式的圖表。有五個地區。左側區域具有實心邊界。它包含輸入、SNMP和系統日誌。從左側區域到中心區域有一個單向箭頭。右側區域也有實心邊界。它包含輸出、報告和度量。有從中央區域到右側區域的單向箭頭。頂部區域有虛線邊界。它包含所有者、目標和績效指標。這三個圓周圍都有實心的邊界。在(a)擁有者與績效指標(b)目標與績效指標之間以及(c)頂端區域與中心區域之間有雙向箭頭。底部區域也有一個虛線邊框。它包含資源和角色。這兩個圓周圍都有實心的邊界。有雙向箭頭看起來可將資源和角色與中心區域連線起來，但它們會停在底部區域的邊界處。中心區域具有實心邊界和標題為「流程」的標題。它還包含每個「任務」和「子任務」之一。每個都有一個實心圓形邊界。任務在圓圈內的空格比圖形中的任何其他專案都多。

流程的輸出必須符合由組織定義的基於業務目標的運營規範。如果流程符合一組規範，則該流程被視為有效，因為它可以重複、測量、管理，並且有助於實現業務目標。如果以最小的努力開展活動，則認為該進程是有效的。

程式擁有者

流程跨越不同的組織邊界。因此，由單一流程擁有者負責流程定義是很重要的。擁有者是決定並報

告流程是否有效與高效的焦點。如果流程無法有效或有效率，則流程所有者將推動流程的修改。流程的修改由變更控制和稽核流程控制。

程式目標

建立流程目標是為了設定流程定義的方向和範圍。目標還用於定義用於衡量流程有效性的指標。

此過程的目的是提供在NTP設計階段要記錄的標準，並為已部署的NTP架構提供稽核功能，以確保長期符合預期設計。

流程績效指標

流程績效指標用於衡量流程定義的有效性。績效指標必須是可衡量和可量化的。例如，下面列出的績效指標可以是數字指標，也可以是按時間衡量的。

- 在整個流程中循環所需的時間長度。
- 為了在NTP問題影響使用者之前主動檢測這些問題所需的執行頻率。
- 與流程執行相關的網路負載。
- 處理作業所建議的更正動作數目。
- 作為處理結果執行的更正動作數目。
- 實施更正操作所需的時間長度。
- 更正作業的積壓。
- 故障排除或問題診斷中的錯誤歸因於NTP相關問題。
- 在種子檔案中新增、移除或修改的專案數。這是準確性和穩定性的指示。

處理輸入

流程輸入用於定義流程的條件和先決條件。很多時候，辨識流程輸入會提供有關外部相依性的資訊。接下來提供與NTP管理相關的輸入清單。

- NTP設計文檔
- SNMP輪詢收集的NTP MIB資料

處理輸出

流程輸出定義如下：

- 本文檔的資料呈現部分中定義的NTP配置報告
- NTP更正操作

工作定義

接下來的部分定義了與NTP管理相關的初始化和迭代任務。

初始化工作

初始化任務在流程實施期間執行一次，不得在流程的每次迭代期間執行。

建立NTP設計

當您驗證先決條件作業時，如果判定任何一項作業未實作，或無法提供足夠資訊以有效滿足此程式的需求，則處理擁有者必須將此事實記錄並提交給管理層。下表概述了先決條件初始化任務。

先決條件任務	說明
任務目標	為符合設計要求和成本目標的NTP架構建立詳細的設計文檔。
工作輸入	• 設計技術與經濟需求 • 當前網路設計文檔 • 定義要在設計中記錄以啟用管理功能的必要方面的標準 • IT應用部署資訊 • 效能監控要求
工作輸出	NTP設計文檔。
任務資源	網路工程師架構師網路運營架構師。
任務角色	由工程和運營稽核人員批准的網路設計技術網路設計成本由負責的預算經理批准。

建立種子檔案

NTP管理過程需要使用種子檔案來消除網路發現功能的需要。種子檔案記錄由NTP進程管理的一組路由器，還用作協調組織中變更管理進程的焦點。例如，如果將新節點輸入網路，則需要將其增加到NTP種子檔案中。如果由於安全要求而對SNMP社群名稱進行了更改，這些修改需要在種子檔案中反映出來。下表概述了如何建立種子檔案。

先決條件任務	說明
任務目標	建立標識三種網路裝置類別的種子檔案：

	1. 關鍵裝置-經常輪詢配置資訊 2. 有趣的裝置-輪詢頻率較低 3. 所有啟用NTP的裝置-輪詢最低數量
工作輸入	NTP設計文檔網路拓撲文檔。
工作輸出	種子檔案。
任務資源	設計標準，可用於辨識和優先處理NTP架構中涉及的節點。

基線NTP效能引數

可用於監控NTP網路的若干參數列現出一些正常的預期變化。基線處理過程用於表徵正常的預期變化，並設定定義意外或異常情況的閾值。此任務用於為NTP體系結構確定變數集的基線。

程序	說明
任務目標	基線變數引數。
工作輸入	標識變數引數cntpSysRootDelay cntpSysRootDispersion cntpPeersRootDelay cntpPeersRootDispersion cntpPeersOffset cntpPeersDelay cntpPeersDisperiod。
工作輸出	基線值和閾值。
任務資源	收集SNMP資料和計算基線的工具。
任務角色	網路工程師NMS工程師。

迭代任務

在過程的每個迭代期間執行迭代任務，並且確定和修改其頻率以便改進效能指標。

維護種子檔案

種子檔案對NTP管理流程的有效實施至關重要。因此，必須主動管理種子檔案的當前狀態。影響種

子檔案內容的網路更改需要由NTP管理進程所有者進行跟蹤。

程序	說明
任務目標	維持種子檔案的正確性
工作輸入	有關網路更改的資訊
工作輸出	種子檔案
任務資源	有關變更的報告、通知和會議
任務角色	網路工程師NMS工程師

執行NTP節點掃描

收集此過程定義的重要掃描、相關掃描和配置掃描的相關資訊。以不同的頻率執行這三個掃描。

關鍵節點是被視為對效能收集資料點非常重要的裝置。關鍵節點掃描經常執行，例如每小時執行一次，或在變更前後按需執行。相關節點是被認為對NTP體系結構的整體完整性很重要，但無法在時間同步樹中進行關鍵效能資料收集的裝置。該報告定期執行，例如每天或每月。配置報告是一個全面且資源密集型的報告，用於根據設計記錄描述整體NTP部署配置。此報告的執行頻率較低，例如每月或每季度。需要考慮的重要一點是，報告的收集頻率可以根據NTP體系結構和業務需求的穩定性進行調整。

程序	說明
工作目標	監控NTP架構
工作輸入	網路裝置資料
工作輸出	報告
任務資源	用於收集資料和生成報告的軟體應用程式
任務角色	網路工程師

檢視NTP節點報告

此任務要求稽核並分析關鍵、相關和配置報告。如果偵測到問題，則必須啟動更正動作。

程序	說明
工作輸入	掃描報告
工作輸出	穩定性分析更正操作
任務資源	訪問網路裝置以進行進一步調查和驗證
任務角色	網路工程師

資料標識

一般資料特性

下表介紹了分析NTP體系結構時認為重要的資料。

資料	說明
節點ID	配置了NTP的裝置

同儕節點	為裝置配置的對等體
同步源	選取要同步的對等專案
NTP配置資料	用於判斷NTP設計一致性的引數
NTP品質資料	用於描述NTP關聯品質的引數

SNMP資料標識

Cisco NTP MIB系統群組

NTP SNMP資料由Cisco-NTP-MIB定義。有關支援此MIB的版本的當前資訊，請使用CCO Feature Navigator工具並選擇MIB Locator選項。可透過語音、電話和消息技術的TAC工具頁面訪問此工具。

Cisco NTP MIB中的系統組提供了運行NTP的目標節點的資訊。目標節點是SNMP查詢的目標。

物件名稱	物件說明
cntpSysStratum	本地時鐘的層。如果該值設定為1（主參考），則執行RFC-1305第3.4.6部分中描述的主時鐘過程 呼叫。：：= { cntpSystem 2 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.2
cntpSysPrecision	帶符號的整數，表示系統時鐘的精確度（以秒為單位）到最接近的冪為2。該值必須舍入為下一個較大的冪2。例如，50-Hz (20 ms)或60-Hz (16.67 ms)的功率頻率時鐘被賦值為-5 (31.25 ms)，而1000-Hz (1 ms)晶體控制時鐘被賦值為-9 (1.95 ms)。：：= { cntpSystem 3 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.3
cntpSysRootDelay	一個帶符號的固定點編號，表示到同步子網根的主參考源的總往返延遲（以秒為單位）。：：= { cntpSystem 4 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRootDi散佈	相對於同步子網根位置的主要參考源的最大錯誤（秒）。只能有大於零的正值。：：= { cntpSystem 5 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRefTime	上次更新本地時鐘的本地時間。如果本地時鐘從未同步，則值為零。：：= { cntpSystem 7 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.7
cntpSysPeer	包含作為同步源的對等體的cntpPeersVarTable中相應對等體條目的唯一關聯識別符號cntpPeersAssocId的當前同步源。如果沒有對等體，則值為零。：：= { cntpSystem 9 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.9
cntpSysClock	當前本地時間。本地時間從特定機器的硬體時鐘得出，並根據使用設計按時間間隔遞增。：：= { cntpSystem 10 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.1.10

Cisco NTP MIB對等體組-對等體變數表

Cisco NTP MIB的對等體組提供有關目標節點的對等體的資訊。

物件名稱	物件說明
cntpPeersVarTable	此表格提供本機NTP伺服器具有關聯的對等端的資訊。對等體也是運行在不同主機上的NTP伺服器。這是cntpPeersVarEntry ：：= { cntpPeers 1 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1的表
cntpPeersVarEntry	每個對等體的條目提供從特定對等體NTP伺服器檢索的NTP資訊。每個對等體由唯一的關聯識別符號標識。當使用者將NTP伺服器配置為與遠端對等體關聯時，會自動建立條目。同樣，當使用者從NTP伺服器中刪除對等

	關聯時，條目也會被刪除。管理站還可以透過設定cntpPeersPeerAddress、cntpPeersHostAddress、cntpPeersMode值並將cntpPeersEntryStatus設定為活動(1)來建立條目。至少，管理站必須設定cntpPeersPeerAddress的值，使該行變為活動狀態。INDEX { cntpPeersAssocId } ：：= { cntpPeersVarTable 1 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1
cntpPeersAssocId	大於零的整數值，用於唯一標識與本地NTP伺服器相關聯的對等體。：：= { cntpPeersVarEntry 1 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.1
cntpPeersConfigured	這是一個位，表示該關聯是根據配置資訊建立的，即使對等體不可達，也不能取消關聯。：：= { cntpPeersVarEntry 2 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.2
cntpPeersPeerAddress	對等體的IP地址。建立新關聯時，必須先設定此物件的值，才能使列成為作用中列。：：= { cntpPeersVarEntry 3 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.3
cntpPeersMode	語法INTEGER { unspecified (0)， symmetricActive (1)， symmetricPassive (2)，客戶端(3)，伺服器(4)，廣播(5)， reservedControl (6)， reservedPrivate (7) }建立新的對等關聯時，如果未為此對象指定值，則預設為symmetricActive (1)。 ：：= { cntpPeersVarEntry 8 }對象識別符號= .1.3.6.1.4.1.9.168.1.2.1.1.8
cntpPeersStratum	對等時鐘的層。：：= { cntpPeersVarEntry 9 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.9
cntpPeersRootDelay	帶符號的固定點編號，表示從對等體到同步子網根主參考源的總往返延遲（以秒為單位）。：：= { cntpPeersVarEntry 13 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.13
cntpPeersRootDi散佈	與同步子網根的主參考源相對的對等時鐘的最大誤差（以秒為單位）。只能有大於零的正值。：：= { cntpPeersVarEntry 14 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.14
cntpPeersRefTime	對等裝置上次更新其時鐘時的本地時間。如果對等時鐘從未同步，則值為零。：：= { cntpPeersVarEntry 16 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.16
cntpPeersReach	一種移位暫存器、用於確定對等體可達性狀態、位從最低有效位（最右側）進入。如果此暫存器中的至少一個位設定為1（對象為非零），則對等體被視為可訪問。移位暫存器中的資料由NTP協定過程填充。：：= { cntpPeersVarEntry 21 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersOffset	對等時鐘相對於本地時鐘的估計偏移量（以秒為單位）。主機確定使用NTP時鐘過濾器演算法的此對象的值。：：= { cntpPeersVarEntry 23 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersDelay	對等時鐘相對於它們之間的網路路徑上的本地時鐘的估計往返延遲（以秒為單位）。主機確定使用NTP時鐘過濾器演算法的此對象的值。：：= { cntpPeersVarEntry 24 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.24
cntpPeers分散	對等時鐘相對於它們之間的網路路徑上的本地時鐘的估計最大誤差（以秒為單位）。主機確定使用NTP時鐘過濾器演算法的此對象的值。：：= { cntpPeersVarEntry 25 }對象識別符號= .1.3.6.1.4.1.9.9.168.1.2.1.1.25

資料收集

SNMP資料收集

此過程所需的所有資訊均可透過SNMP查詢收集。為了分析資料並生成報告，必須開發自定義指令碼或軟體程式。

資料簡報

NTP關鍵節點報告

關鍵節點是在所選效能資料收集點的同步樹中非常重要的裝置。如果存在受監控的高收入VoIP服務並且收集了單向延遲變化度量，則記錄時間戳的源節點和目標節點被視為關鍵節點。

在本示例中，NTP設計是緊接著一個示例OSPF分層結構建立的。因此，下面描述的報告將被格式化，以便按裝置的OSPF區域對NTP裝置進行分組。如果節點在多個區域都有介面，則報告產生軟體必須決定節點可列出哪個區域以供報告之用。如前所述，OSPF不是NTP的先決條件。本檔案僅將其用作說明性範例。

區域	裝置	裝置資料	價值
AreaId #n	DeviceId #1	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDi散佈	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	
	DeviceId #n	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDi散佈	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	

NTP相關節點報告

相關節點報告的格式與關鍵節點報告的格式相同。相關節點是被認為對整個NTP架構很重要，但無法直接促進關鍵效能監控點的時間同步的節點。

NTP配置報告

配置報告是收集有關整個NTP架構資訊的綜合報告。此報告用於記錄和驗證設計記錄中的NTP部署

。

區域	裝置	對等	對等資料	價值
AreaId #n	DeviceId #n	PeerId #1	cntpPeersAssocId	
			cntpPeersConfigured	
			cntpPeersPeerAddress	
			cntpPeersMode	
			cntpPeersStratum	
			cntpPeersRootDelay	
			cntpPeersRootDi散佈	
			cntpPeersRefTime	
			cntpPeersReach	
			cntpPeersOffset	
			cntpPeersDelay	
			cntpPeers分散	
		PeerId #n	cntpPeersAssocId	
			cntpPeersConfigured	
			cntpPeersPeerAddress	
			cntpPeersMode	
			cntpPeersStratum	
			cntpPeersRootDelay	
			cntpPeersRootDi散佈	
			cntpPeersRefTime	
			cntpPeersReach	
			cntpPeersOffset	
			cntpPeersDelay	
			cntpPeers分散	

相關資訊

- RFC 1305網路時間通訊協定
- RFC 2330 IP效能測量結果架構
- 每個ISP必須考慮的Cisco IOS基本功能v2.84
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。