

# 使用网络时间协议的最佳实践

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[术语](#)

[概述](#)

[设备概述](#)

[NTP 概述](#)

[NTP 设计准则](#)

[关联模式](#)

[客户端/服务器模式](#)

[对称主动/被动模式](#)

[广播和/或组播模式](#)

[设置NTP闰秒](#)

[NTP 结构](#)

[时钟技术和公共时间服务器](#)

[NTP 配置示例](#)

[WAN 时间分配网络](#)

[高层校园时间分配网络](#)

[低层校园时间分配网络](#)

[进程定义](#)

[进程所有者](#)

[进程目标](#)

[进程性能指示器](#)

[进程输入](#)

[进程输出](#)

[任务定义](#)

[初始化任务](#)

[创建NTP设计](#)

[创建种子文件](#)

[基线NTP性能参数](#)

[重复任务](#)

[维护种子文件](#)

[执行NTP节点扫描](#)

[查看NTP节点报告](#)

[数据识别](#)

[一般数据特性](#)

[SNMP 数据识别](#)

[Cisco NTP MIB系统组](#)

---

## [数据收集](#)

[SNMP 数据收集](#)

## [数据表示](#)

[NTP 临界节点报告](#)

[NTP 有趣节点报告](#)

[NTP 配置报告](#)

## [相关信息](#)

---

# 简介

本文档介绍设计网络时间协议的最佳实践。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- [网络时间协议 \(NTP\)](#)
- [时钟技术和公共时间服务器](#)

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

基于互联网协议(IP)的网络已经从传统的尽力交付模式快速发展为需要量化性能和可靠性的模式，而且在许多情况下还需要通过服务级别协议(SLA)来保证性能和可靠性。由于需要更深入地了解网络特征，因此针对表征网络行为的重要指标和测量功能开展了大量研究工作。许多度量方法的基础是时间的度量。

网络时间同步程度达到现代性能分析所要求的程度，是一项必不可少的练习。根据业务模式和提供的服务，网络性能表征被视为一项重要的竞争服务优势。在这些情况下，部署网络管理系统并指导工程资源分析收集的性能数据会耗费大量成本。然而，如果不适当关注经常被忽视的时间同步原则，这些努力就无效。

本文描述网络时间协议(NTP)网络管理功能管理的假设过程定义。您可以将此文章用作一个假设步骤和一个信息性示例。组织可对此进行定制以满足内部目标。


本文档提供的信息分为几个主要部分：

- [术语](#)部分提供有关时间同步的术语的一般定义。
- 概述部分提供系统时间相关的网元硬件的背景信息、NTP技术概述、NTP体系结构的重要设计方面。
- NTP配置示例部分提供NTP部署示例，供WAN、高层校园和低层校园时间分布式网络使用。
- [进程定义](#)部分概述了用于完成NTP管理的进程定义。流程详细信息从目标、绩效指标、输入、输出和个别任务方面进行了描述。
- [任务定义](#)部分提供了详细的进程任务定义。每项任务的描述术语包括：目标、任务输入、任务输出、完成任务所需的资源和执行任务所需的工作技能。
- [数据标识](#)部分介绍了NTP的数据标识。数据标识考虑信息的来源。例如，信息可以包含在简单网络管理协议(SNMP)管理信息库(MIB)中、系统日志生成的日志文件或只能通过命令行界面(CLI)访问的内部数据结构。
- [数据收集](#)部分介绍了NTP数据的收集。数据的收集与数据的位置密切相关。例如，SNMP MIB数据的收集采用几大机制，例如陷阱、远程监控(RMON)告警与事件、或轮询。内部数据结构维护的数据由自动脚本收集或在用户手动登录到系统以发出CLI命令并记录输出时收集。
- [数据表示法](#)部分提供了数据表示方式的报告格式示例。

## 术语

- 精度 -时钟绝对值接近零偏移量。
- Accurate -时钟偏移量在特定时间零时。
- 漂移 -歪斜变化中的测量值，或相对于时间的时钟偏移量的第二个微分。
- 联合分辨率-比较时钟时，它是C1和C2的分辨率之和。然后，联合分辨率指示由从另一个时钟生成的时间戳中减去的一个时钟生成的时间戳计算出的任何时间间隔的精度保守下限。
- Node —指在本地处理器上实例化NTP协议。节点也可以称为设备。
- 时钟报告时间和实际时间的差别，参见世界协调时间(UTC)定义。如果时钟报告时间 $T_c$ ，而真实时间是 $T_t$ ，则时钟偏移是 $T_c - T_t$ 。
- 对等体 - 参见在由来自本地节点的网络路径连接的远程处理器上安装NTP协议的相关情况。
- 相对偏移 -当比较两个时钟C1和C2时，真实时间的概念将由时钟C1报告的时间取代。例如，在一个特定时刻与C1相关的时钟C2的偏移量是 $T_{c2} - T_{c1}$ ，C2和C1报告瞬间时差。
- Resolution -更新时钟时间的最小单位。分辨率以秒为单位定义。但是，分辨率与时钟报告时间相关，与真实时间无关。例如，10毫秒解决方法表示时钟每隔0.01秒更新其时间，但并不表示该时间就是两次更新之间的实际时间数量。

---

 注意：时钟的分辨率非常高，但仍不准确。

---

- 倾斜- 时钟频率差，或相对于时间偏移量的一阶导数。
- Synchronize -当两个时钟彼此相对准确（相对偏移为零）时，将同步它们。时钟可以同步，但就它们讲述真实时间的能力而言，它们仍然不准确。

# 概述

## 设备概述

时间服务的核心是系统时钟。系统时钟从系统启动时开始运行，并跟踪当前日期和时间。可以从一定数量的来源设置系统时钟，反过来，也可以通过多种机制向其他系统分配当前时间。某些路由器包含电池供电的日历系统，可跟踪系统重启和停电期间的日期和时间。当重新启动系统时，总要使用此日历系统初始化系统时钟。如果没有其他来源可以使用，它还可以被当成一个授权的时间源，然后通过NTP重新分配。此外，如果启用NTP，日历会从NTP定期更新，这样可以补偿日历时间的内在偏差。当带有系统日历的路由器开始初始化时，系统时钟根据它内部电池供电日历的时间设置。在没有日历的型号上，系统时钟被设置为预定的时间常数。可以从下面列出的源设置系统时钟。

- NTP
- 简单网络时间协议 (SNTP)
- 虚拟集成网络服务(VINES)时间服务
- 手动配置

某些低端Cisco设备仅支持SNTP。SNTP是仅客户端的简化NTP版本。SNTP只能从NTP服务器上接收时间，并且不能用来向其他系统提供时钟服务。SNTP提供的时间通常为准确时间的100毫秒以内。另外，SNTP不验证数据流，虽然您能配置扩展访问控制列表，以提供一些防护。SNTP客户端比NTP客户端更容易受到不合规服务器的攻击，并且只能在不需要强身份验证的情况下使用。

系统时钟提供到下面列出的服务的时间。

- NTP
- VINES时间服务
- 用户show命令
- 日志记录和调试消息

系统时钟基于UTC在内部跟踪时间，也称为格林威治标准时间(GMT)。您可以配置关于本地时区和夏令时的信息，以便正确显示与本地时区相关的时间。系统时钟会记录时间是否具有权威性。如果没有授权，则时间只能用于显示目的，不能重新分配。

## NTP 概述

NTP旨在同步计算机网络中的时间。NTP通过用户数据报协议(UDP)运行，端口123同时作为源和目标，反过来通过IP运行。NTP版本3 [RFC 1305](#)用于在一组分布式时间服务器和客户端之间同步计时。使用NTP和节点，识别和配置网上的一套节点，形成同步子网，有时则指重叠网络。虽然可以存在多个主服务器，但无需选择协议。

NTP网络通常从一个可信的时间源获得时间，例如附到时钟服务器上的无线时钟或原子时钟。NTP

然后在整个网络中分配此时间。NTP客户端在其轮询间隔（从64秒到1024秒）内与其服务器进行事务，该轮询间隔随时间动态变化，具体取决于NTP服务器和客户端之间的网络条件。当路由器与不良NTP服务器（例如，具有大色散的NTP服务器）通信时，会出现另一种情况；路由器还会增加轮询间隔。同步两台计算机时每分钟不需要超过一个NTP事务。

NTP使用层的概念描述机器旁边有多少NTP跳来自可信的时间源。例如，第1层时钟服务器有无线电或原子时钟直接与它连接。然后它将时间通过NTP发送到第2层时钟服务器，等等。运行NTP的计算机自动选择其配置为与NTP通信的最低层数的计算机作为其时间源。此策略有效生成了NTP发言方的自行组织树。NTP对客户端和时间服务器之间关系中的后三个关键变量进行可靠的估计，因此它在数据包交换网络的不确定路径长度上表现出色。

- 网络延迟
- 时间数据包交换的离散-两台主机之间最大时钟误差的测量。
- Clock offset -应用于客户端时钟的修正，用于同步客户端时钟。

长距离广域网(WAN)(2000公里)10毫秒级别的时钟同步和局域网(LAN)1毫秒级别的时钟同步，通常都可以达到。

有两种方法可以使NTP不与时间不准确的计算机同步。首先，NTP从不与自身未同步的计算机同步。其次，NTP会比较多台计算机报告的时间，并且不会与时间明显不同于其他计算机的计算机同步，即使其层级较低。

运行NTP的计算机之间的通信（关联）通常是静态配置的。每台计算机都获得了必须与之建立关联的所有计算机的IP地址。通过在具有关联的每对计算机之间交换的NTP消息，可以实现准确计时。但是，在LAN环境中，可以将NTP配置为使用IP广播消息。因为可以配置每台机器发送或接收广播消息，此选择减少了配置的复杂性。但是，计时准确度会稍有降低，因为信息流是单向的。

在计算机上保留的时间是一项关键资源，强烈建议您使用NTP的安全功能，以避免意外或恶意设置错误时间。可用的两个安全功能是基于访问列表的限制方案和加密的身份验证机制。

Cisco版本的NTP支持某些Cisco IOS®软件版本中的第1层服务。如果版本支持ntp refclock命令，可以连接无线或原子时钟。Cisco IOS的某些版本支持Trimble Palisade NTP同步工具包(仅Cisco 7200系列路由器提供)或电信解决方案全球定位系统(GPS)设备。如果网络在Internet上使用公共时间服务器，并且网络与Internet隔离，则Cisco实施的NTP允许对计算机进行配置，使其如同通过NTP同步一样，但实际上它已通过其他方式确定时间。然后，其他计算机通过NTP与该计算机同步。

## NTP 设计准则

同步子网中的每个客户端（也可以是更高层客户端的服务器）都选择其中一个可用服务器进行同步。这通常来自它可以访问的最低层服务器。但是，这并非总是最佳配置，因为NTP的运行前提是每次服务器时间都必须以一定程度的不信任进行检查。NTP更喜欢使用较低层时间(至少三层)的几个来源，因为它能够运用协议算法，检测到任意部分的失常。通常，当所有服务器都同意时，NTP会根据最低层、最接近（网络延迟）和要求的精度来选择最佳服务器。这意味着，虽然必须设法为每台客户端提供三个或更多个较低层时间源，但其中一些源只能提供备份服务，在网络延迟和层级方面质量可能较差。例如，从本地服务器无法直接访问的较低层源接收时间的同一层对等体也可以提

供良好的备份服务。

NTP通常首选较低层服务器，而不是较高层服务器，除非较低层服务器的时间明显不同。该算法能够检测时间源何时可能非常不准确或不正常，并在这些情况下阻止同步，即使不准确的时钟处于较低层级。它永远无法使设备与自身未同步的其他服务器同步。

为了说明服务器是否可靠，需要经过多次健全性检查，如：

- 实施必须包括健全性超时，如果监控程序在较长的时间间隔后不更新此信息，则防止陷阱传输。
- 还包括其他健全性检查，用于身份验证、范围界限和避免使用非常旧的数据。
- 已添加检查来警告振荡器运行时间过长，没有来自参考源的更新。
- 在严重网络拥塞情况下，当参考源迅速变化时，加入有效参数peer.valid和sys.hold变量，避免参考源迅速变化。添加了peer.config、peer.authenticable和peer.authenticate位来控制特殊功能并简化配置。

如果其中至少有一个检查失败，路由器会将其宣布为不正常。

## 关联模式

接下来的部分将介绍NTP服务器用于相互关联的关联模式。

- 客户端/服务器
- 对称主动/被动
- 广播

### 客户端/服务器模式

从属客户端和服务器的运行通常采用客户端/服务器模式，客户端或从属服务器可以与组成员同步，但组成员不能与客户端或从属服务器同步。这样可以防止故障或协议攻击。

客户端/服务器模式是最常见的Internet配置。它在使用无状态服务器的传统远程过程调用(RPC)模式下运行。在此模式中，客户端向服务器发送请求，这样在未来某个时间将出现回复。在某些上下文中，则被描述为轮询操作，客户端从服务器轮询时间和鉴权数据。客户端在客户端模式下使用server命令进行配置，并指定了域名服务器(DNS)名称或地址。服务器不需要预先配置。

在一个普通的客户端/服务器型号中，客户端向一个或多个服务器发送NTP信息，并且处理接收到的回复。服务器互换地址和端口，重写消息中的某些字段，重估检查和，并立即回复消息。NTP消息中包含的信息允许客户端确定相对于本地时间的服务器时间，然后根据需要调整本地时钟。此外，该消息包括计算预期计时准确性和可靠性的信息及选择最佳服务器的信息。

为大量客户端提供同步的服务器通常作为由三个或更多相互冗余的服务器组成的组运行，并且每个服务器在客户端/服务器模式下与三个或更多第1层或第2层服务器运行，并以对称模式与组的所有其他成员运行。这提供保护措施，防护一个或多个服务器不能运行或者提供不正确的时间。NTP算法

的设计是抵抗攻击，当配置的同步源的某个小部分偶然地或故意提供不正确的的时间。在这些情况下，使用一个特殊投票程序来识别假的来源，并丢弃它们的数据。出于可靠性，所选主机可以配备外部时钟，以便在主服务器和/或备用服务器或者二者之间的通信路径发生故障时进行备份。

客户端模式下的关联配置通常由配置文件中的服务器声明表示，它表示您希望从远程服务器获取时间，但您不希望向远程服务器提供时间。

## 对称主动/被动模式


对称有源/无源模式的配置是：低层对等体组可以进行相互备份。每个对等体与一个或多个主参考源一起运行，例如无线时钟或者可靠的附属服务器的子集。如果其中一个对等体失去所有引用源或仅停止操作，其他对等体将自动重新配置，以便时间值可以从当前对等体流向队列中的所有其他对等体。在某些情况下，此操作被描述为推拉操作，因为对等体会根据特定配置拉取或推送时间和值。

在对称活动模式下的关联配置（通常由配置文件中的对等声明表示）向远程服务器表明希望从远程服务器获取时间，并且还愿意在必要时向远程服务器提供时间。此模式适用于涉及通过不同网络路径互连的许多冗余时间服务器的配置，目前互联网上的大多数第1层和第2层服务器都是如此。

对称模式最常用于作为相互冗余组运行的两台或多台服务器之间。在这些模式下，组成员中的服务器会根据网络抖动和传播延迟来安排同步路径，以实现最佳性能。如果一个或多个组成员发生故障，则剩余成员会根据需要自动重新配置。

使用peer命令并指定其他对等体的DNS名称或地址时，会在对称活动模式下配置对等体。另一个对等体也以这种方式配置为对称活动模式。

---

 **注意：**如果未以此方式专门配置另一个对等体，则会在对称活动消息到达时激活对称被动关联。由于入侵者可以模拟对称活动对等体并注入错误的时间值，因此必须始终对对称模式进行身份验证。

---

## 广播和/或组播模式

在对准确性和可靠性要求不太严格的地方，可以配置客户端使用广播和/或组播模式。通常，具有相关客户端的服务器不会使用这些模式。优点是客户端不需要为特定服务器配置，这允许所有运行中的客户端使用相同的配置文件。广播模式要求同一子网中有一台广播服务器。因为路由器没有传播广播消息，所以只有相同子网上的广播服务器被使用。

广播模式适用于涉及一台或多台服务器和大量客户端的配置。广播服务器是使用broadcast命令和本地子网地址配置的。广播客户端是使用broadcastclient命令配置的，该命令允许广播客户端响应从任何接口接收的广播消息。由于入侵者可以模拟广播服务器并注入错误的时间值，因此必须始终对此模式进行身份验证。

## 设置NTP闰秒

您可以使用ntp leap {add | delete}命令以插入闰秒。有添加或删除闰秒的选项。发生这种情况有两个限制条件：

- 时钟必须处于同步状态。

- 该命令仅在发生跳转之前的一个月內被接受。如果当前时间在出现跳跃1个月之前，则无法设置跳跃。

设置后，在最后一秒中添加或删除闰秒，如下所示：

```
<#root>
```

```
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 结构

以下三种结构可用于NTP架构：

- 扁平对等体结构
- 分层结构
- 星型结构

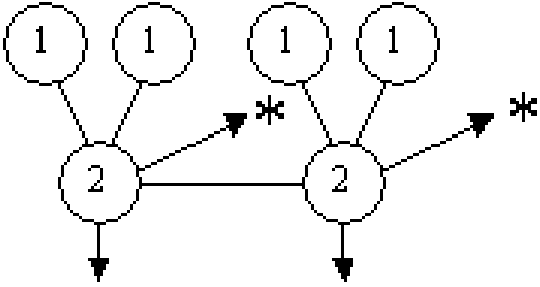
在平面对等结构中，所有路由器彼此成为对等体，少数在地理位置上分离的路由器配置指向外部系统。NTP网络的每个新成员的时间会越来越长。

在分层结构中，路由分层结构复制为NTP分层结构。核心路由器与外部时间源具有客户端/服务器关系，内部时间服务器与核心路由器具有客户端/服务器关系，内部用户（非时间服务器）路由器与内部时间服务器具有客户端/服务器关系，等等。这些关系称为层次尺度。分层结构是首选技术，因为它提供了一致性、稳定性和可扩展性。

可扩展的NTP架构具有分层结构，如下图所示。

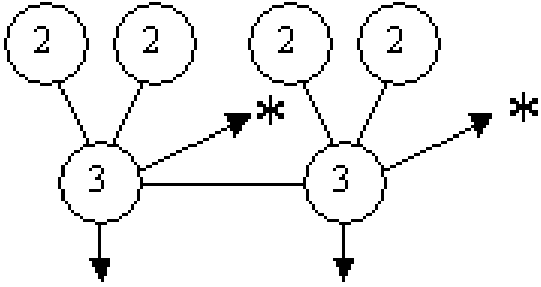


Internet Primary Servers  
(Stratum 1)



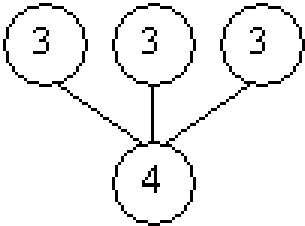
\* = to buddy in another subnet

Campus Secondary Servers  
(Stratum 2)

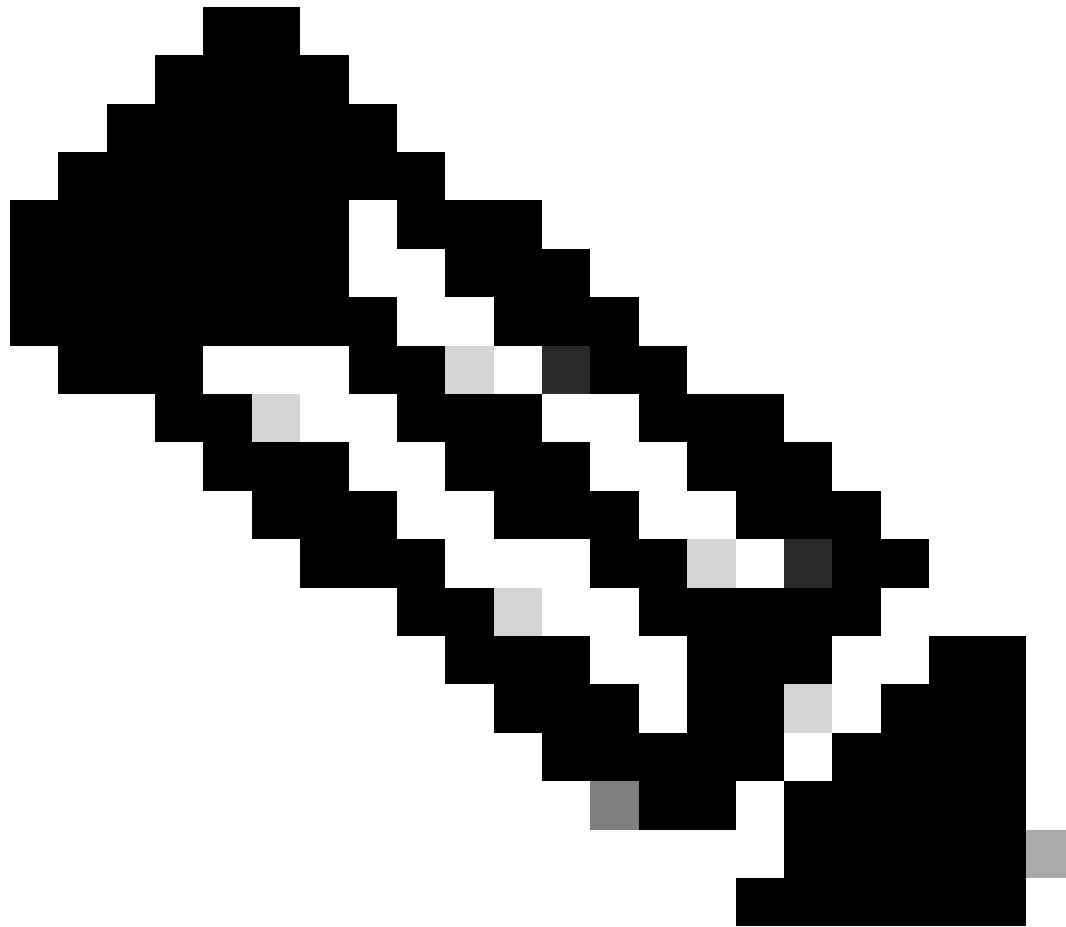


\* = to buddy in another subnet

Department Servers  
(Stratum 3)



Workstations (Stratum 4)




注意：显示可扩展的分层NTP部署的一系列图形。第一个图显示两个NTP第2层设备，每个连接到两个第1层设备（显示在前面的第2层设备图中），另一个子网中的伙伴以星号表示。此外，每个第2层设备都有一个向下箭头。第二个图具有相同的布局，但使用第2层设备（第1层设备所在的位置）和第3层设备（第2层设备所在的位置）。第三个图显示一个第4层设备连接到三个第3层设备。总之，该图显示了一个拓扑，其中每台设备连接到2-3台设备，且其第1层比自己的低（更好）。

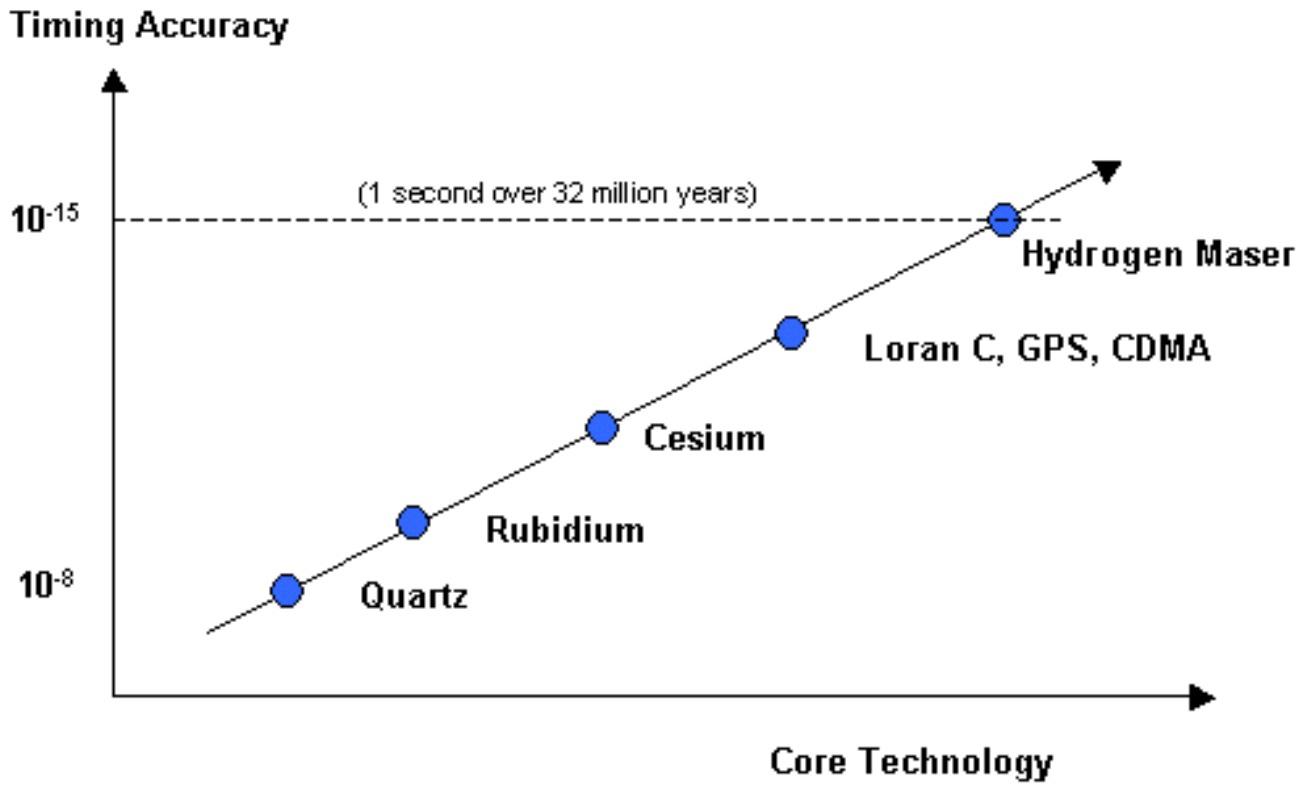
在星形结构中，所有路由器在核心上与几个时钟服务器有客户端/服务器的关系。专用的时钟服务器是星形的中心，并且通常是与外部时钟源或它们自己的GPS接收器同步的UNIX系统。

## 时钟技术和公共时间服务器

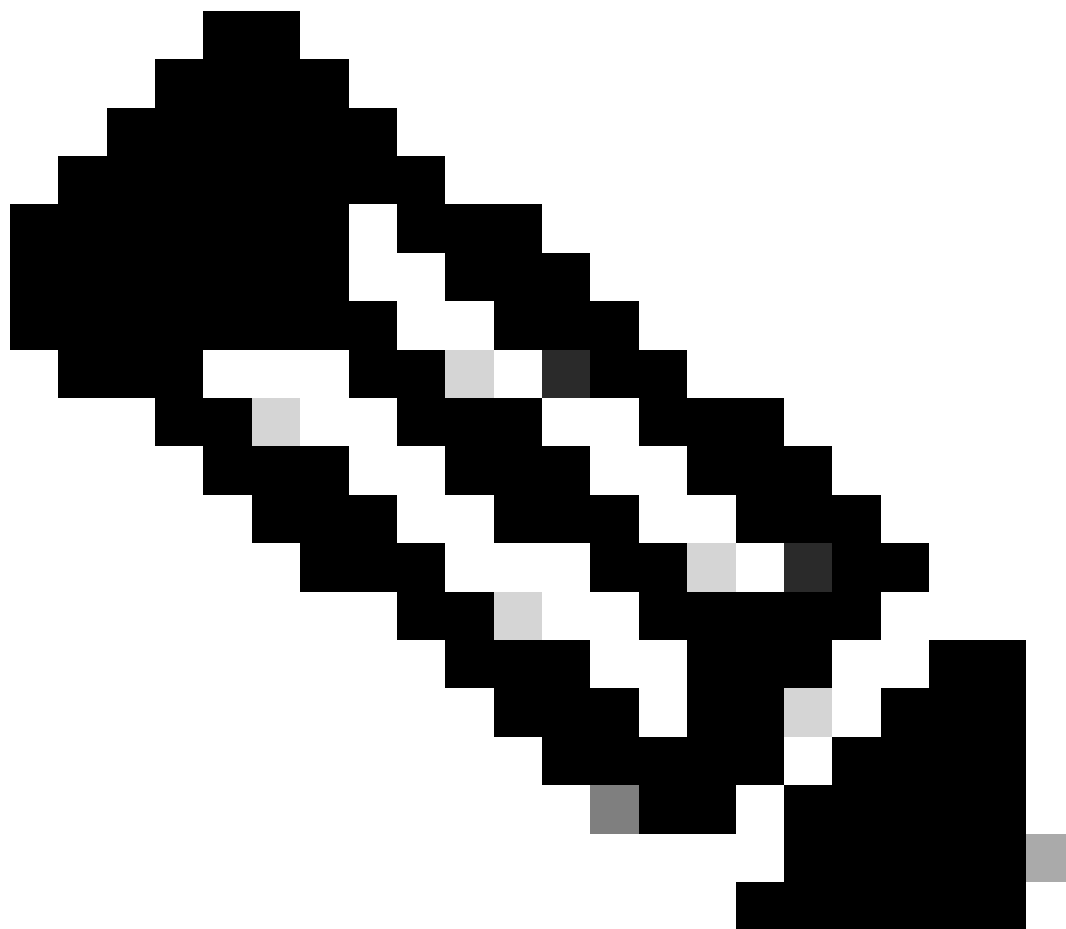
互联网NTP子网目前包括50个公共主服务器，通过无线电、卫星或调制解调器与UTC直接同步。通常，客户端数量相对较少的客户端工作站和服务器无法与主服务器同步。大约100台公共辅助服务器与主服务器同步，并提供与互联网上总数超过100,000台客户端和服务器的同步。[公共NTP时间服务器](#)列表会频繁更新。此外，还有大量通常不对公众使用的专用主服务器和辅助服务器。

 注意：PIX和ASA不能配置为NTP服务器，但是它们可以配置为NTP客户端。

在某些情况下，如果私有企业需要高度准确的时间服务，例如用于IP语音(VoIP)测量的单向度量，网络设计人员可以选择部署私有外部时间源。下图显示当前技术的相对准确度的比较图表。



比较图



注：此图显示了从石英（ $10^{-8}$ 次幂）到氢激光器（ $10^{-15}$ 次幂）的计时方法越来越精确。后者表明在3200万年的时间内精度损失约为1秒。在这两种方法之间列出的其他方法（从最小到最精确）是铷钟、铯、罗兰C、GPS和CDMA。最后三个（罗兰C、GPS和CDMA）一起列出。

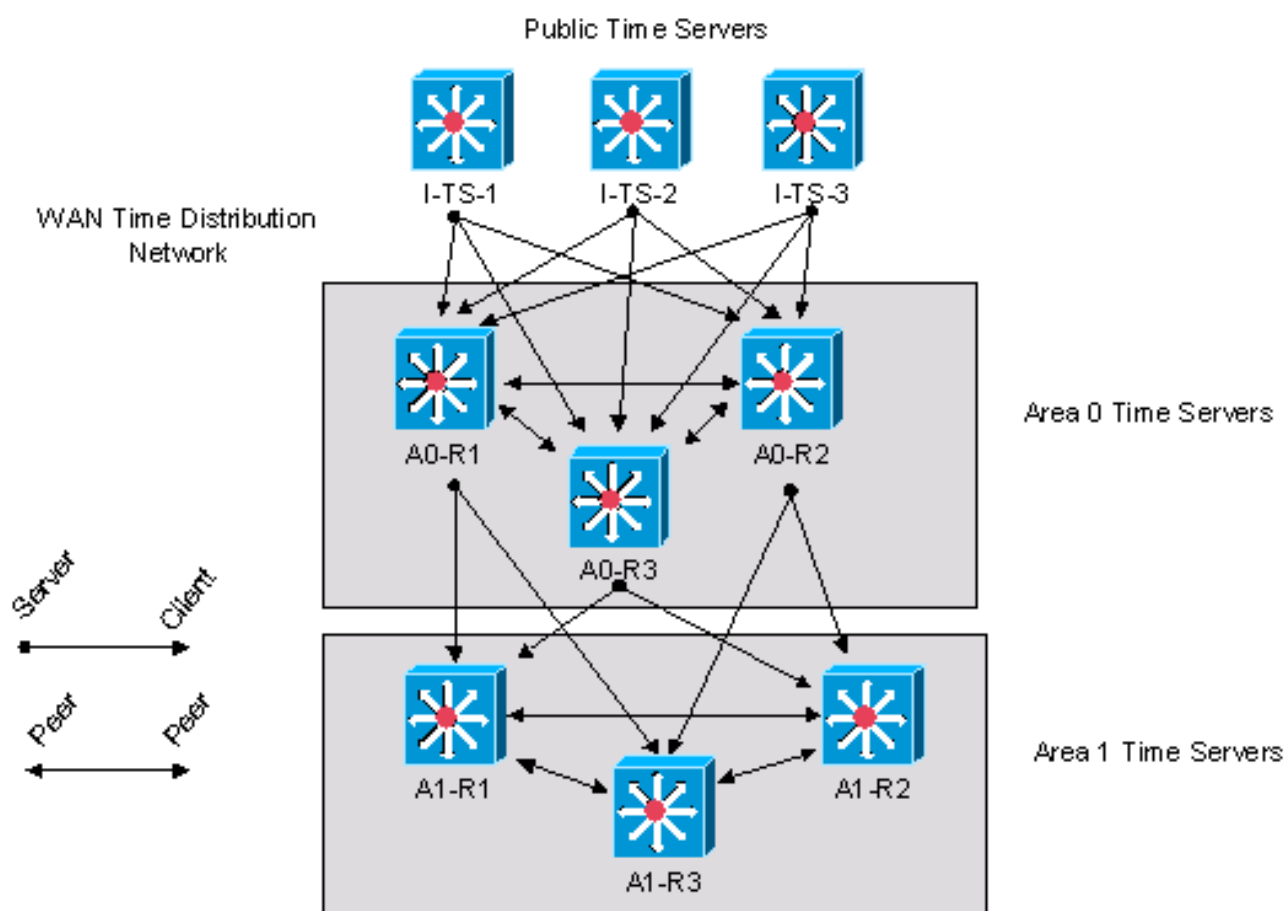
直到最近，由于高成本的质量外部时钟源，外部时钟源的使用没有在企业网络中广泛部署。但是，随着服务质量(QoS)要求的提高和时间技术的成本不断降低，企业网络的外部时间源是一个可行的选择。

## NTP 配置示例

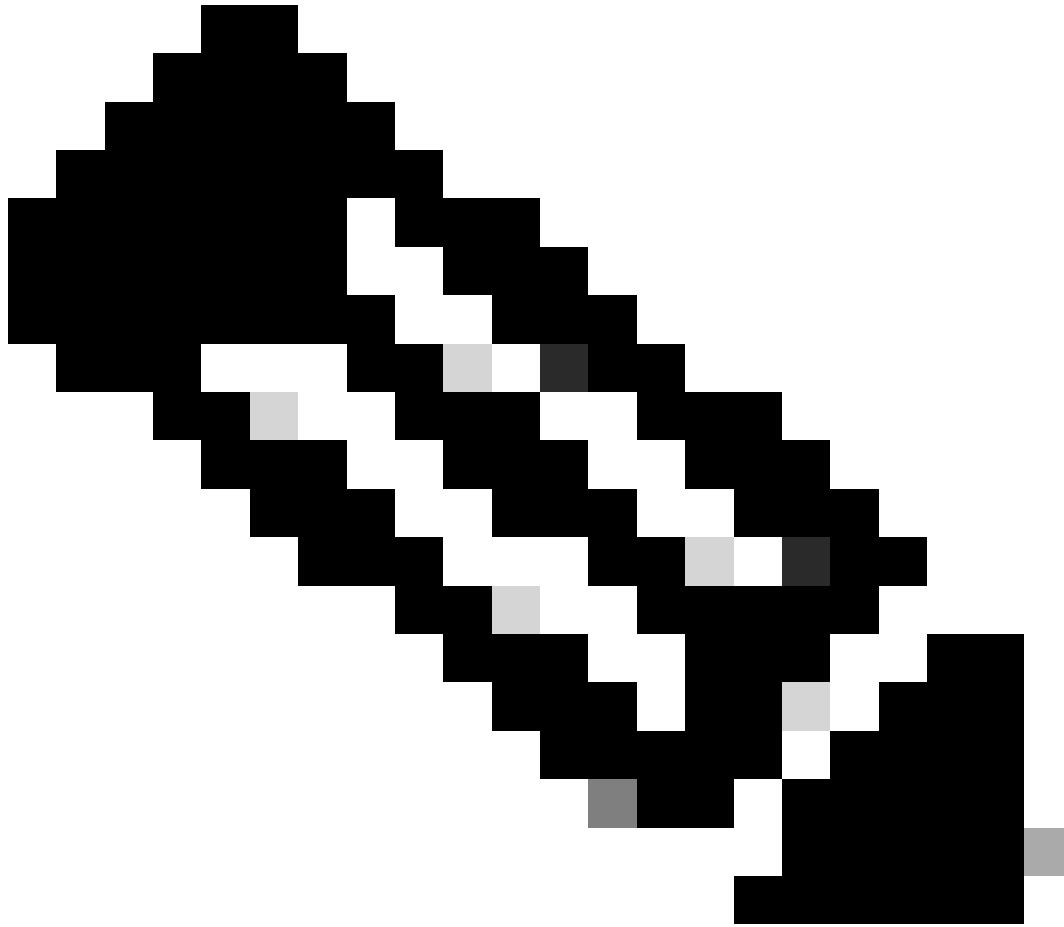
### WAN 时间分配网络

在下一个图中，公司自治系统(AS)从三个公共时间服务器获取时间信息。公司AS显示为区域0和区域1时间服务器。在本示例中，NTP层次结构描述了开放最短路径优先(OSPF)层次结构。但是，OSPF不是NTP的先决条件。它仅用作说明性示例。NTP可沿其他逻辑分层边界部署，例如增强

型内部网关路由协议(EIGRP)分层结构或标准核心/分布/接入分层结构。



WAN 时间分配网络



注意：此图展示了跨多个网络的NTP拓扑。区域1中的三台设备(OSPF)是彼此的对等体，也是区域0中服务器的客户端。区域0中的三个设备是彼此的对等体、公共时间服务器的客户端和区域1中客户端的服务器。公共时间服务器仅显示为区域0中客户端的服务器。

本示例是设备A0-R1的Cisco IOS配置，如上图所示。

```
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 <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>
```

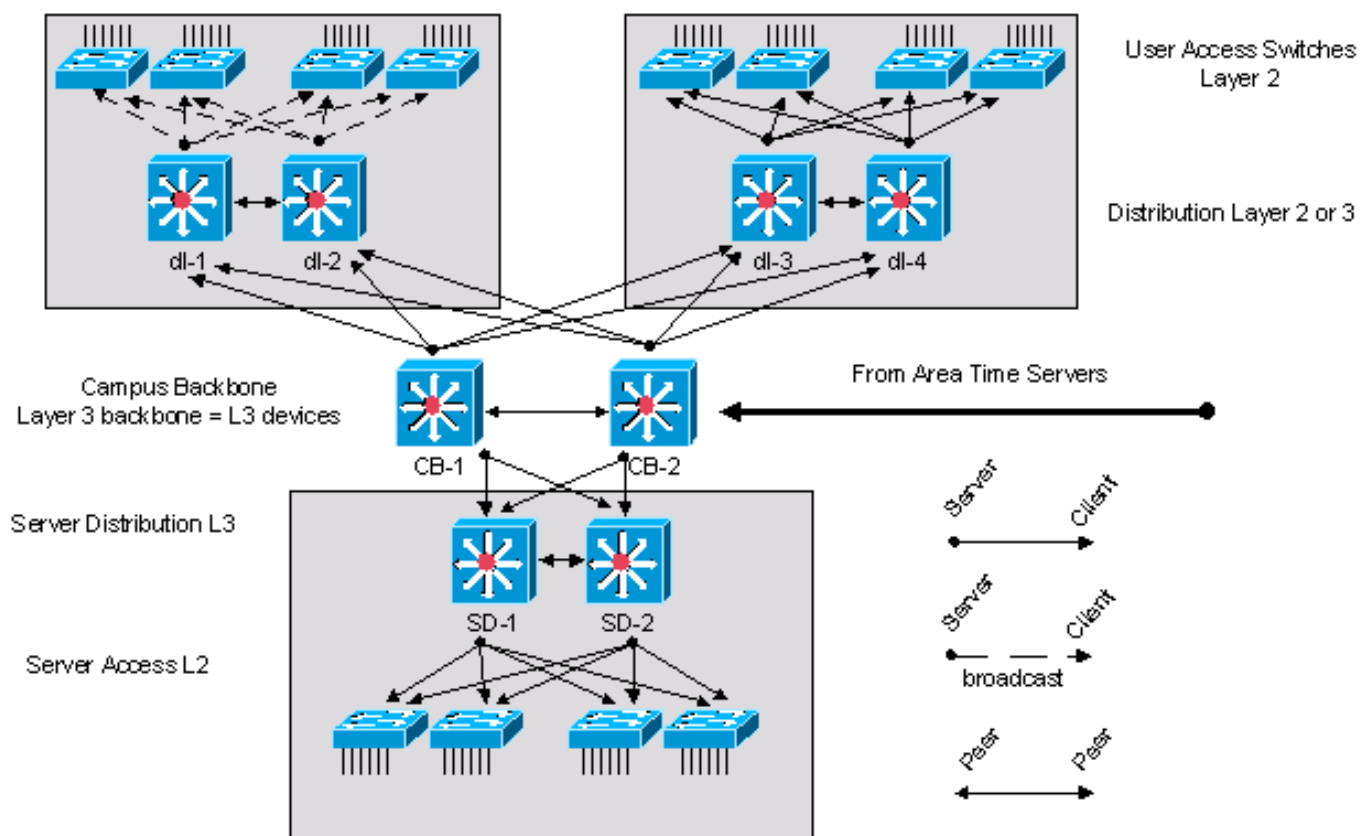
## 高层校园时间分配网络

上一节描述了WAN时间分配网络。此部分在层次结构中向下移动一步，以讨论在高层园区网络的时间分配。

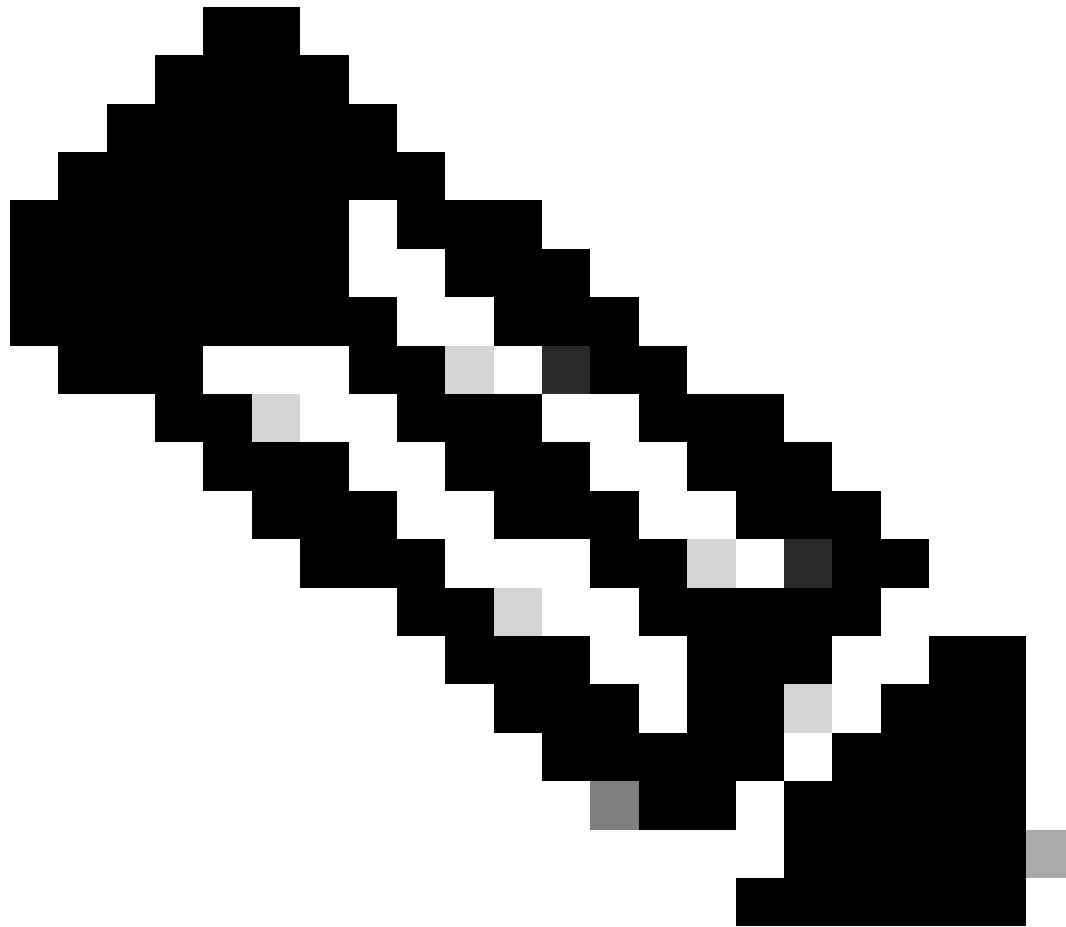
人们认为，高层园区网络中时间分配的主要区别在于广播关联模式的潜在用途。如前所述，广播关联模式简化了LAN的配置，但降低了时间计算的准确性。因此，必须权衡维护成本与性能测量的准确性。



### High Stratum Campus Time Distribution Network



高层校园时间分配网络



注意：标题为“高层园区时间分配网络”的图，其中包括通用的三层拓扑（主干、分布、接入）。接入交换机是分布层交换机的客户端，分布层交换机是主干交换机的客户端，而主干交换机是区域时间服务器的客户端（如图所示）。分布层交换机分为多对交换机，并且只与对中的另一台交换机存在对等关系。两个主干交换机也是彼此的对等体。四个接入交换机（左上角）显示为带点箭头的广播客户端，而所有其他客户端-服务器和对等关系均为非广播。

上图中所示的高层园区网络来自标准的思科园区网络设计，包含三个组件。园区核心由两个第3层设备组成，标记为CB-1和CB-2。位于图较低的部分的服务器组件有标记为SD-1和SD-2的二个L3路由器。服务器块中的其他设备是第2层设备。在左上方，有一个标准的访问块，带有标记为dl-1和dl-2的二个L3分布设备。其余设备是第2层交换机。在此客户端访问块中，使用广播选项分配时间。在右上角，有另一个使用客户端/服务器时间分配配置的标准访问块。

园区主干设备在客户端/服务器模型中同步到区域时间服务器。

以下是dl-1第3层分布设备的配置：

*!--- In this case, d1-1 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 <d1-2>  
access-list 5 deny any
```

*!--- Restricts the IP addresses for the peers  
!--- and clients.*

```
ntp access-group peer 5
```

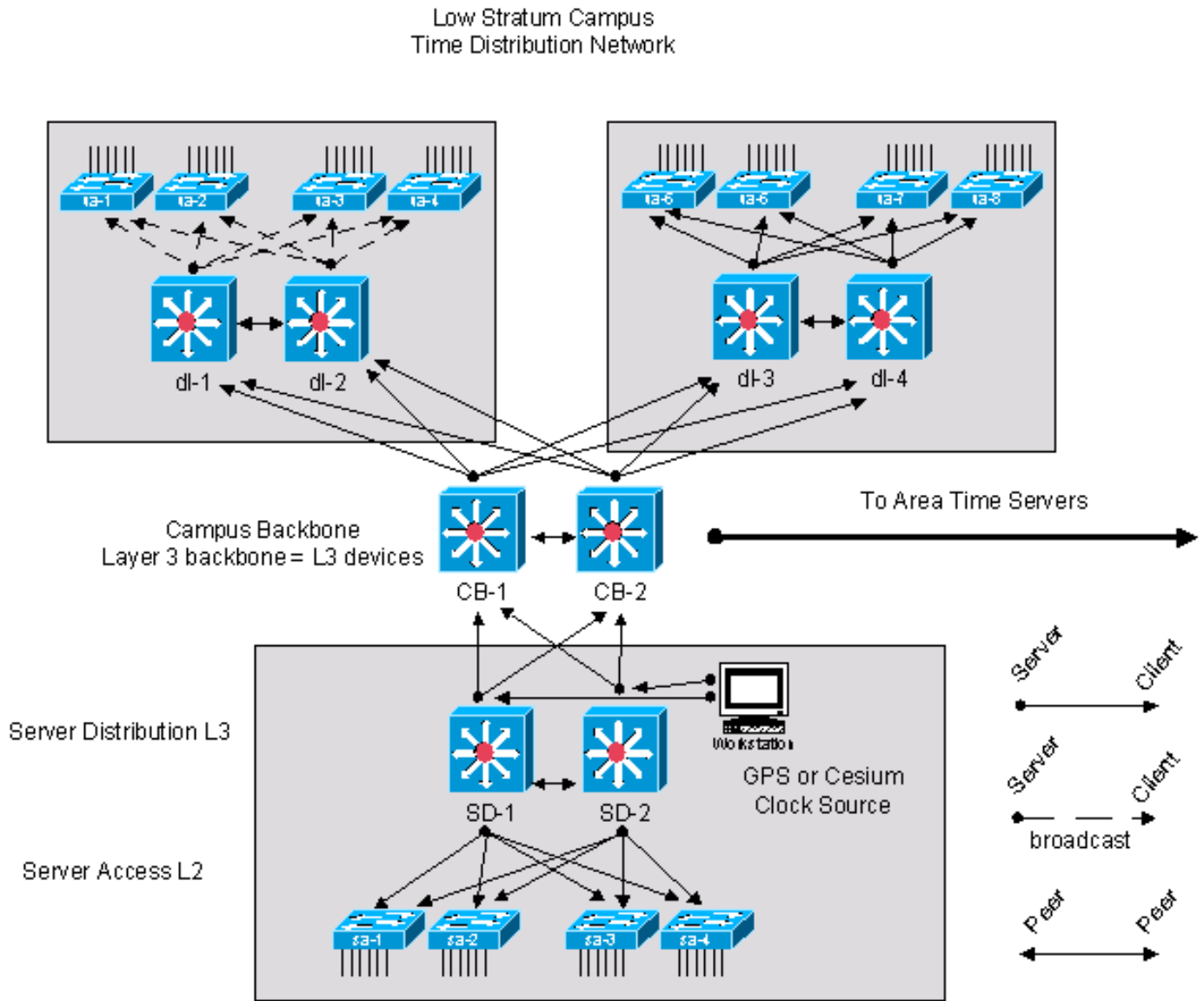
*!--- Fault tolerant configuration polling 2  
!--- local time servers and 1 local peer.*

```
ntp server <CB-1>  
ntp server <CB-2>  
ntp peer <d1-2>
```

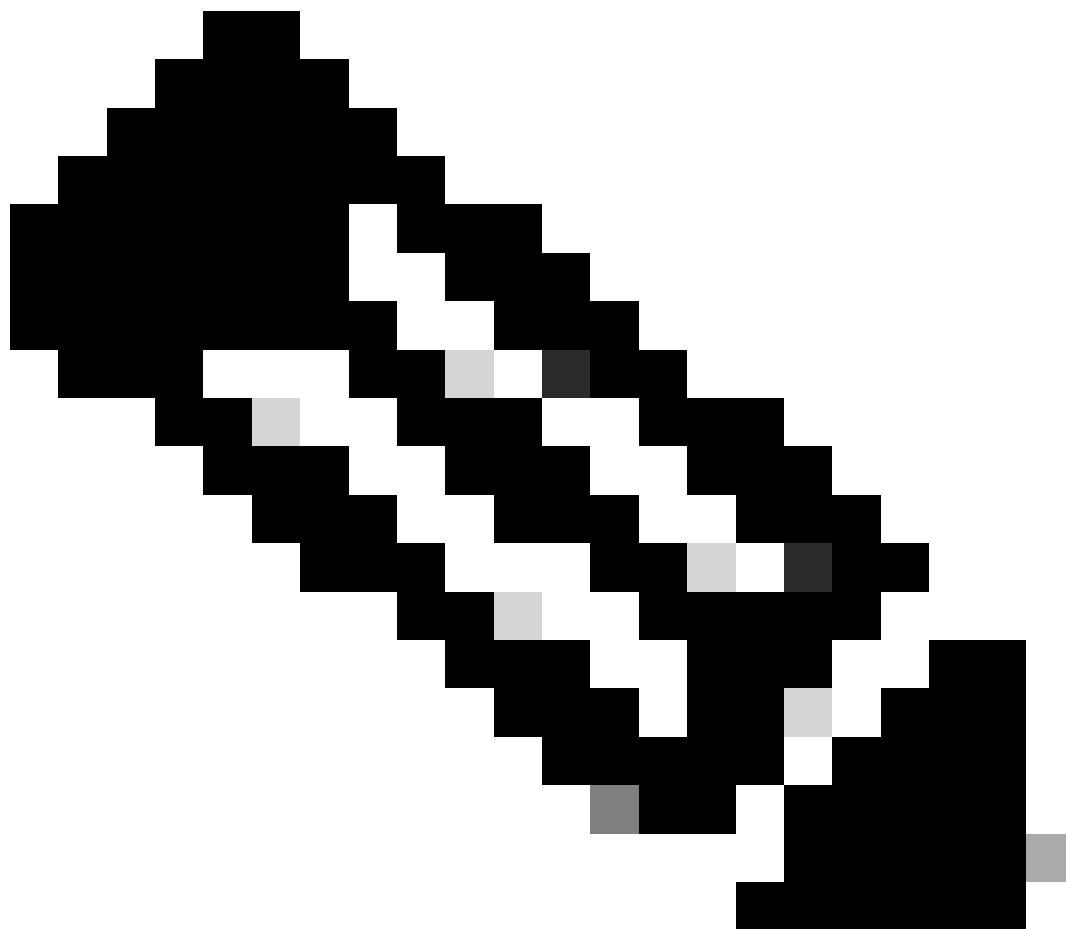
低层校园时间分配网络

在下图中，在低层园区网络的中央数据中心提供GPS或Cs时间源。这会在专用网络上调配第1层时间源。如果专用网络中有多个GPS或Cesium时间源，则必须修改专用网络中的时间分配以利用可用的时间源。

通常，上述示例采用相同的原理和配置。案例的主要区别是同步树的根是专用时间源而不是来自互联网的公共时钟源。这就改变了时间分配网络的设计，以利用高精度专用时间源。私有时间源分布在整个私有网络中，遵循了前面几节中介绍的层次性和模块化原则。



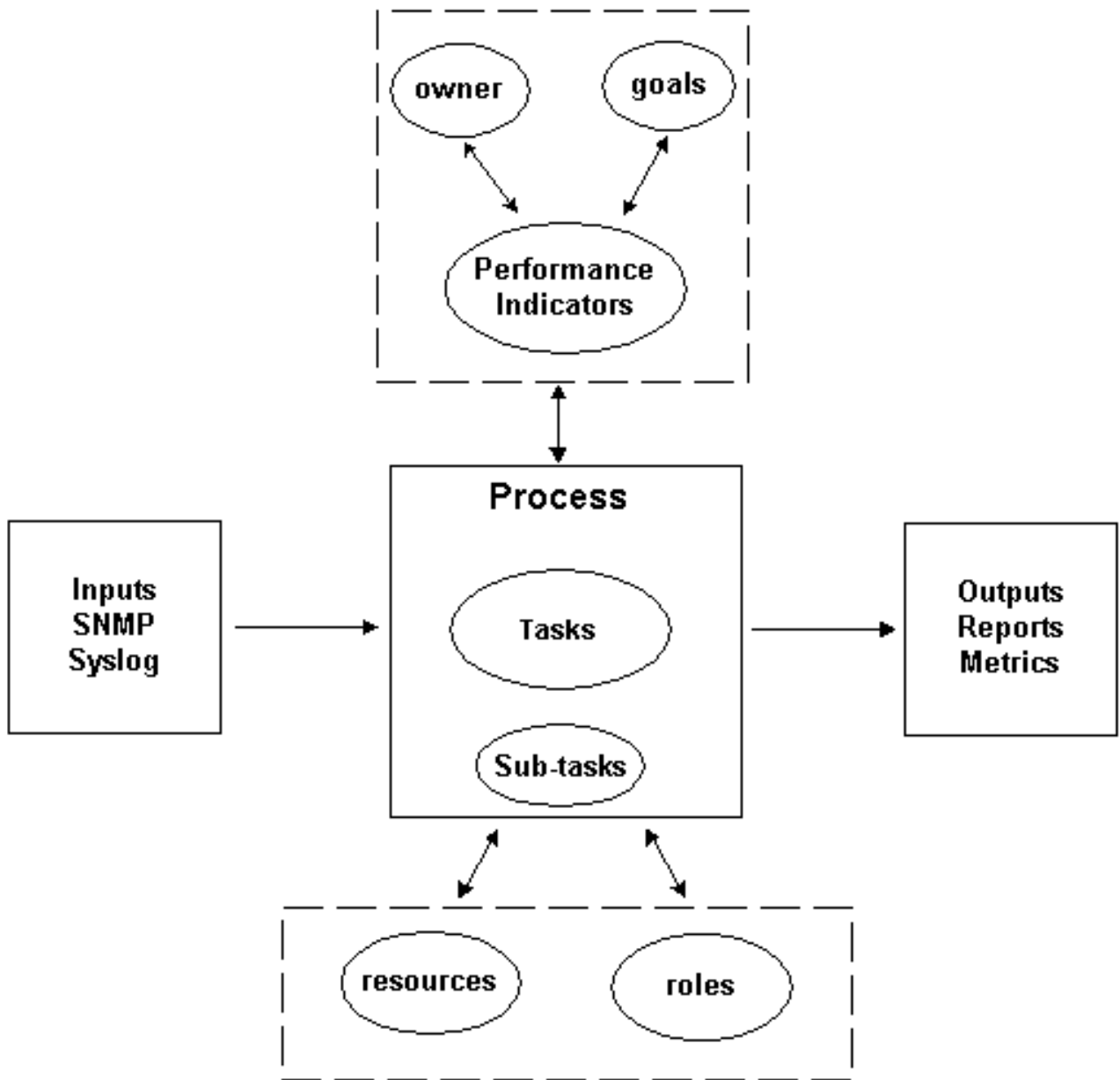
低层校园时间分配网络



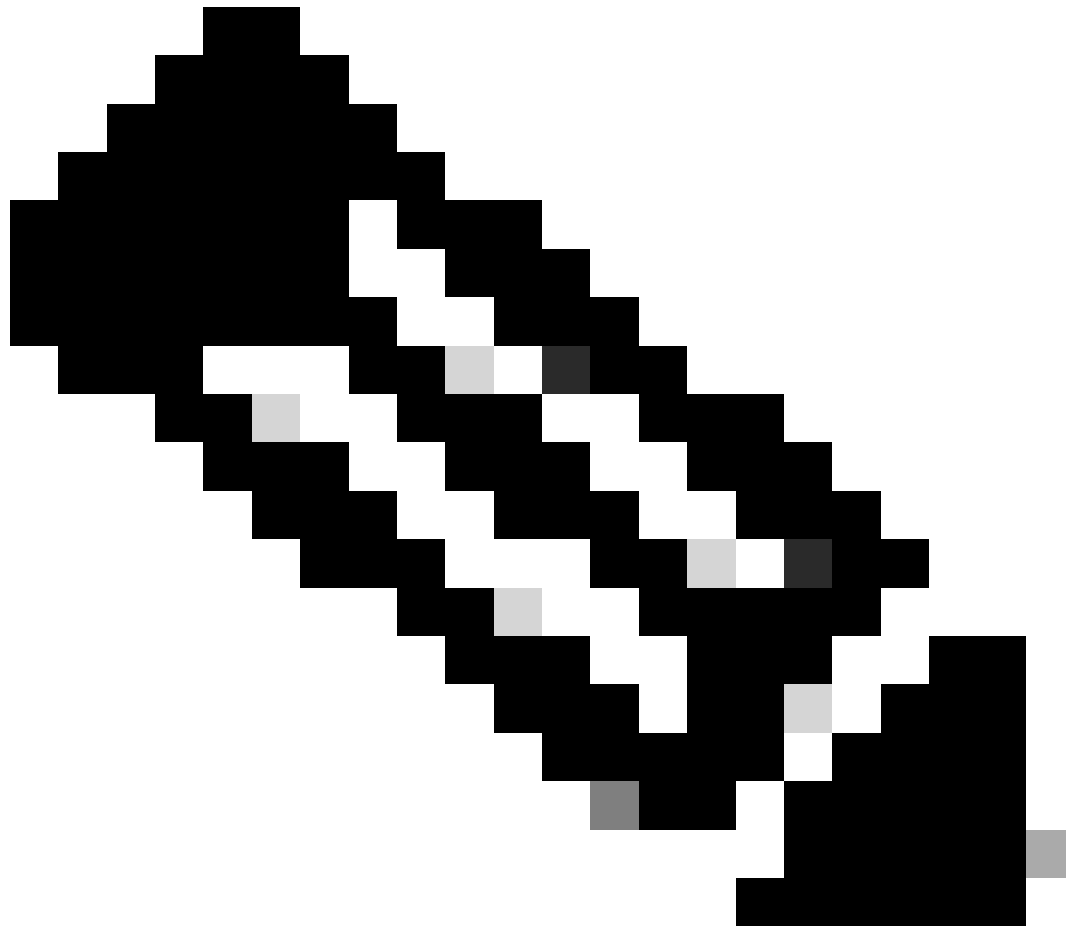
注意：标题为“低层园区时间分布网络”的图，其中包括通用的三层拓扑（主干、分布、接入）。两台分布层交换机都连接了GPS或铯钟。直接连接到这些分布层交换机的接入层交换机和主干交换机是这些分布层交换机的客户端。网络中的所有其他分布层交换机都是主干交换机的客户端，其余的接入层交换机也是其直连分布层交换机的客户端。四个接入交换机（左上角）显示为带点箭头的广播客户端，而所有其他客户端-服务器和对等关系均为非广播。

## 进程定义

流程定义是由座席执行的一系列相关操作、活动和更改，用于满足目的或实现目标。过程控制是计划和调整的过程，目的是以有效和高效的方式执行过程。如下图所示。



一系列流程



注意：指定本文档所用进程的含义的图。有五个地区。左侧区域具有实心边框。它包含输入、SNMP和系统日志。从左侧区域到中心区域有一个单向箭头。右侧区域也有稳定的边界。它包含输出、报告和度量。从中心区域到右侧区域有一个单向箭头。顶部区域有一个虚线边框。它包含所有者、目标和绩效指标。这三个圆周围都有稳定的边界。(a)所有者与绩效指标(b)目标和绩效指标(c)顶部区域和中心区域之间有双向箭头。底部区域也有一个虚线边框。它包含资源和角色。这两个圆圈周围都有稳定的边界。有双向箭头看起来用于将资源和角色与中心区域连接，但它们停在底部区域的边界处。中心区域有一个实心边框和一个标题，标题写着“进程”。它还包含每个Task和Sub-tasks。每个接口都有一个实心圆形边框。任务在圆圈内的空白空间大于图形中的任何其他项目。

流程的输出必须依照组织定义的操作规范，并且基于业务目标。如果程序依照某套标准，并且程序可以重复被执行、能被测量和被管理，并且对业务目标有用，程序则视为有效，如果活动开展时只付出最低限度的努力，该过程也被认为是高效的。

## 进程所有者

流程跨越各种组织边界。所以，拥有负责流程定义的单个进程所有者很重要。所有者是确定和报告

流程是否有效和高效率的焦点。如果该进程无效，那么进程所有者加建将执行进程修改。流程的修改由变更控制和审阅流程控制。

## 进程目标

建立进程目标以设置进程定义的方向和范围。目标也用于定义用来测量进程效果的尺度。

此流程的目标是提供NTP设计阶段要记录的标准，并为已部署的NTP架构提供审核功能，以确保长期符合预期设计。

## 进程性能指示器

流程绩效指标用于衡量流程定义的有效性。业绩指标必须是可衡量和可量化的。例如，下面列出的绩效指标为数字或按时间衡量。

- 循环执行整个过程所需的时间。
- 在影响用户之前，所需的执行频率，以便提前发现NTP问题。
- 与进程执行相关的网络负载。
- 进程建议的更正操作数。
- 作为该过程的结果而实施的纠正措施的数量。
- 实施纠正措施所需的时间。
- 纠正措施积压。
- 与NTP相关问题导致的故障排除或问题诊断错误。
- 种子文件中添加、删除或修改的项目数。这是准确性和稳定性的一个指标。

## 进程输入

流程输入用于定义流程的标准和前提条件。很多时候，进程输入的识别会提供有关外部依赖性的信息。下面提供了与NTP管理相关的输入列表。

- NTP设计文档
- SNMP轮询收集的NTP MIB数据

## 进程输出

过程输出定义如下：

- 本文档[数据演示](#)部分中定义的NTP配置报告
- NTP纠正措施



# 任务定义

接下来的部分定义了与NTP管理相关的初始化和迭代任务。

## 初始化任务

初始化任务在流程实施期间执行一次，不能在流程的每个迭代期间执行。

### 创建NTP设计

在验证前提任务时，如果确定任何一项任务未实施或未提供足够的信息来有效地满足此程序的需要，则流程所有者必须记录此事实并将其提交给管理层。下表列出了先决条件初始化任务。

前期任务	描述
任务目标	创建满足设计要求和成本目标的NTP架构详细设计文档。
任务输入	<ul style="list-style-type: none"><li>• 设计技术和经济要求</li><li>• 当前网络设计文档</li><li>• 定义要在设计中记录以启用管理功能的必要方面的标准</li><li>• IT应用部署信息</li><li>• 性能监控要求</li></ul>
任务输出	NTP设计文档。
任务资源	网络工程师架构师网络运营架构师。
任务角色	由工程和运营审核员批准网络设计技术由负责的预算经理批准网络设计成本。

### 创建种子文件

NTP管理进程需要使用种子文件，取消对网络发现功能的需要。种子文件将记录受NTP程序监管的路由器集，用作一个焦点，与组织中的变化管理程序一起调整。例如，如果新节点输入到网络中，它们需要添加到NTP种子文件。如果由于安全需求而变更SNMP属性名称，那些修改应反映在种子文件中。下表概述如何创建种子文件。

前期任务	描述
任务目标	创建标识三种网络设备类别的种子文件：

	<ol style="list-style-type: none"> <li>1. 关键设备-经常轮询配置信息</li> <li>2. 相关设备-轮询频率较低</li> <li>3. 所有启用NTP的设备-轮询最低数量</li> </ol>
任务输入	NTP设计文档网络拓扑文档。
任务输出	种子文件。
任务资源	设计标准，可用于确定NTP架构中涉及的节点及其优先顺序。

### 基线NTP性能参数

可用于监控NTP网络的几个参数显示一些正常的预期变化。设立基线的流程用来标明正常的预期变化，并设置定义意外或异常状况的门限值。此任务用于为NTP架构的变量参数集设定基线。

Process	描述
任务目标	基线变量参数。
任务输入	确定变量参数cntpSysRootDelay cntpSysRootDispersion cntpPeersRootDelay cntpPeersRootDispersion cntpPeersOffset cntpPeersDelay cntpPeersDispersion。
任务输出	基线值和阈值。
任务资源	收集SNMP数据和计算基线的工具。
任务角色	网络工程师NMS工程师。

### 重复任务

流程反复或者它们频率已经确定、并进行修改后，请执行迭代任务，以改进性能指数。

### 维护种子文件

种子文件对NTP管理流程的有效实施至关重要。因此，必须主动管理种子文件的当前状态。更改影

响种子文件内容的网络需要由NTP管理流程所有者跟踪。

Process	描述
任务目标	维护种子文件的准确性
任务输入	有关网络更改的信息
任务输出	种子文件
任务资源	有关变更的报告、通知和会议
任务角色	网络工程师NMS工程师

### 执行NTP节点扫描

收集有关此过程定义的关键、相关和配置扫描的信息。以不同的频率运行这三种扫描。

关键节点是被视为对性能收集数据点非常重要的设备。经常执行重要节点扫描，例如每小时或者根据改变前后的需求。相关节点是指被认为对NTP架构的整体完整性很重要，但无法在关键性能数据收集的时间同步树中的设备。此报告会定期执行，例如每天或每月。配置报告是完整的资源密集型报告，用来表现设计记录的整个NTP部署配置。此报告的执行频率较低，例如每月或每季度。要考虑的重点是，报告的收集频率可以根据NTP体系结构和业务需要的稳定性进行调整。

Process	描述
任务目标	监控NTP架构
任务输入	网络设备数据
任务输出	报告
任务资源	用于收集数据和生成报告的软件应用程序
任务角色	网络工程师

### 查看NTP节点报告

此任务要求审核并分析关键、相关和配置报告。如果检测到问题，则必须启动更正操作。

Process	描述
任务输入	扫描报告
任务输出	稳定性分析纠正措施
任务资源	访问网络设备以进行进一步调查和验证
任务角色	网络工程师

## 数据识别

### 一般数据特性

下表介绍了在分析NTP架构时被视为重要的数据。

数据	描述
节点Id	配置了NTP的设备
对等体	为设备配置的对等体

同步源	选定的同步对等体
NTP配置数据	用于判断NTP设计一致性的参数
NTP质量数据	用于描述NTP关联质量的参数

## SNMP 数据识别

### Cisco NTP MIB系统组

NTP SNMP数据由Cisco-NTP-MIB定义。有关支持此MIB的版本的当前信息，请使用CCO功能导航器工具并选择MIB定位器选项。此工具可通过语音、电话和消息技术的TAC工具页面访问。

[Cisco NTP MIB](#)中的系统组提供了运行NTP的目标节点的信息。目标节点是SNMP查询的目标。

对象名称	对象说明
cntpSysStratum	本地时钟的层。如果值设置为1 ( 主要参考 ) ，则表示 <a href="#">RFC-1305</a> 第3.4.6部分中介绍的主时钟过程调用。 ::= { cntpSystem 2 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.2
cntpSysPrecision	带符号的整数，指示系统时钟的精度 ( 以秒为单位 ) ，最接近于2的幂。该值必须舍入为下一个较大的幂2。例如，50赫兹(20毫秒)或60赫兹(16.67毫秒) 功率频率时钟被赋予值-5 (31.25毫秒)，而1000赫兹(1毫秒)晶体控制时钟被赋予值-9 (1.95毫秒)。 ::= { cntpSystem 3 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.3
cntpSysRootDelay	一个带符号的固定点编号，表示到同步子网根目录的主参考源的总往返延迟 ( 以秒为单位 ) 。 ::= { cntpSystem 4 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRootDispersion	用秒钟表示的最大错误与同步子网根的主要参考源相关。只有大于零的正值是可能的。 ::= { cntpSystem 5 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRefTime	上次更新本地时钟的本地时间。如果本地时钟从未同步，则该值为零。 ::= { cntpSystem 7 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.7
cntpSysPeer	包含充当同步源的对等体的cntpPeersVarTable中对应对等体条目的唯一关联标识符cntpPeersAssocId的当前同步源。如果没有对等体，则值为0。 ::= { cntpSystem 9 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.9
cntpSysClock	当前本地时间。本地时间从特定机器的硬件时钟得出，并根据使用的设计按间隔增加。 ::= { cntpSystem 10 }对象标识符= .1.3.6.1.4.1.9.9.168.1.1.10

### Cisco NTP MIB对等体组-对等体变量表

Cisco NTP MIB的对等体组提供有关目标节点的对等体的信息。

对象名称	对象说明
cntpPeersVarTable	此表提供本地NTP服务器所关联的对等体的信息。对等体也是在不同主机上运行的NTP服务器。这是cntpPeersVarEntry ::= { cntpPeers 1 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1的表
cntpPeersVarEntry	每个对等体的条目提供从特定对等体NTP服务器检索的NTP信息。每个

	对等体由唯一的关联标识符标识。当用户配置NTP服务器与远端对等体相连时，自动创建条目。同样，当用户从NTP服务器删除对等关联时，条目也会被删除。管理站还可以通过设置cntpPeersPeerAddress、cntpPeersHostAddress、cntpPeersMode的值来创建条目，并将cntpPeersEntryStatus设置为活动(1)。至少，管理站必须为cntpPeersPeerAddress设置值，使行激活。INDEX { cntpPeersAssocId } ::= { cntpPeersVarTable 1 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1
cntpPeersAssocId	大于零的整数值能独特识别本地NTP服务器连接的对等体。 ::= { cntpPeersVarEntry 1 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1.1
cntpPeersConfigured	此位表示关联是根据配置信息创建的，即使对等体不可达，也不能取消关联。 ::= { cntpPeersVarEntry 2 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1.2
cntpPeersPeerAddress	对等设备的IP地址。创建新关联时，必须先为此对象设置值，然后才能激活该行。 ::= { cntpPeersVarEntry 3 }对象标识符=.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) }当创建新的对等体关联时，如果没有为此对象指定值，则该关联默认为symmetricActive (1)。 ::= { cntpPeersVarEntry 8 } object identifier = .1.3.6.1.4.1.9.9.168.1.1.2.1.1.1.8
cntpPeersStratum	对等体时钟的层。 ::= { cntpPeersVarEntry 9 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1.9
cntpPeersRootDelay	带符号的固定点编号，表示从对等设备到同步子网根目录的主参考源的总往返延迟（以秒为单位）。 ::= { cntpPeersVarEntry 13 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1.13
cntpPeersRootDispersion	对等体时钟的最大错误（以秒表示）与同步子网的根的主要参考源相关。只有大于零的正值是可能的。 ::= { cntpPeersVarEntry 14 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1.1.14
cntpPeersRefTime	上次更新其时钟时对等体的本地时间。如果对等体时钟从未同步，则该值为零。 ::= { cntpPeersVarEntry 16 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1.1.16
cntpPeersReach	移位寄存器、用于确定对等设备的可达性状态，其中有些位从最低有效位（最右侧）进入。如果该寄存器中至少有一个比特设置为1(对象为非零)，对等体则被视为可达。移位寄存器中的数据由NTP协议过程填充。 ::= { cntpPeersVarEntry 21 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersOffset	对等时钟相对于本地时钟的估计偏差（以秒为单位）。主机确定使用NTP时钟过滤器算法的此对象的值。 ::= { cntpPeersVarEntry 23 }对象标识符=.1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersDelay	估计得出的对等体时钟的最大错误与它们之间的网络路径的本地时钟相关（用秒钟表示）。主机确定使用NTP时钟过滤器算法的此对象的值。 ::= { cntpPeersVarEntry 24 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1.1.24
cntpPeersDispersion	估计得出的对等体时钟的最大错误与它们之间的网络路径的本地时钟相

	关 ( 用秒钟表示 )。主机确定使用NTP时钟过滤器算法的此对象的值。 : := { cntpPeersVarEntry 25 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1.1.25
--	---

## 数据收集

### SNMP 数据收集

此程序需要的所有信息可以通过SNMP查询收集。为了解析数据并生成报告，必须开发自定义脚本或软件程序。

## 数据表示

### NTP 临界节点报告

关键节点是所选性能数据收集点的同步树中非常重要的设备。如果存在被监控的高收入VoIP服务并且收集了单向延迟变化度量，则记录时间戳的源节点和目的节点被视为关键节点。

在本示例中，NTP设计是在示例OSPF层次结构之后建立的。因此，下文所述的报告将被格式化，以便按设备的OSPF区域对NTP设备进行分组。如果节点在多个区域具有接口，则报告生成软件必须决定可以将该节点列出哪个区域以用于报告目的。如前所述，OSPF不是NTP的必备条件。本文档中仅将其用作说明性示例。

区域	设备	设备数据	价值
AreaId #n	DeviceId #1	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	
	DeviceId #n	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	

### NTP 有趣节点报告

相关节点报告的格式与关键节点报告的格式相同。相关节点是被认为对整体NTP架构很重要，但无法直接促进关键性能监控点的时间同步的节点。

## NTP 配置报告

配置报告是收集有关整体NTP架构信息的综合报告。此报告用于记录和验证设计记录中的NTP部署。

区域	设备	对等体	对等体数据	价值
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				

## 相关信息

- [RFC 1305网络时间协议](#)
- [RFC 2330 IP性能指标框架](#)
- [基本Cisco IOS功能每个ISP必须考虑v2.84](#)
- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。