

# Utilisation des meilleures pratiques pour le protocole NTP

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Terminologie](#)

[Aperçu](#)

[Présentation des périphériques](#)

[Présentation de NTP](#)

[Critères de conception NTP](#)

[Modes d'association](#)

[Mode client/serveur](#)

[Mode actif/passif symétrique](#)

[Mode de diffusion et/ou de multidiffusion](#)

[Set NTP Leap Second](#)

[Architecture NTP](#)

[Technologie d'horloge et serveurs de temps publics](#)

[Exemples de déploiements NTP](#)

[Réseau de distribution temporelle WAN](#)

[Réseau de distribution du temps de campus à strate élevée](#)

[réseau de distribution du temps de campus à faible strate](#)

[Définitions de processus](#)

[Propriétaire du processus](#)

[Objectifs du processus](#)

[Indicateurs de performance des processus](#)

[Entrées de processus](#)

[Sorties du processus](#)

[Définitions des tâches](#)

[Tâches d'initialisation](#)

[Création de la conception NTP](#)

[Créer un fichier d'amorçage](#)

[Paramètres de performances NTP de référence](#)

[Tâches itératives](#)

[Tenir à jour le fichier de démarrage](#)

[Exécuter l'analyse du noeud NTP](#)

[Examiner les rapports de noeud NTP](#)

[Identification des données](#)

[Caractéristiques générales des données](#)

---

[Identification des données SNMP](#)

[Groupe de systèmes Cisco NTP MIB](#)

[Groupe d'homologues Cisco NTP MIB - Tableau des variables d'homologues](#)

[Collecte de données](#)

[Collecte de données SNMP](#)

[Présentation des données](#)

[Rapport de noeud critique NTP](#)

[Rapport NTP sur les noeuds intéressants](#)

[Rapport de configuration NTP](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les meilleures pratiques de conception du protocole NTP.

## Conditions préalables

### Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- Protocole NTP
- Technologie d'horloge et serveurs de temps publics

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Les réseaux IP (Internet Protocol) sont rapidement passés du modèle traditionnel de fourniture au mieux à un modèle dans lequel les performances et la fiabilité doivent être quantifiées et, dans de nombreux cas, garanties par des accords de niveau de service (SLA). La nécessité de mieux comprendre les caractéristiques du réseau a conduit à d'importants efforts de recherche axés sur d'importantes mesures et capacités de mesure pour caractériser le comportement du réseau. La base de beaucoup de méthodologies métriques est la mesure du temps.

La synchronisation du temps réseau, dans la mesure requise pour l'analyse moderne des performances, est un exercice essentiel. En fonction des modèles commerciaux et des services fournis, la caractérisation des performances réseau est considérée comme un important facteur de différenciation des services par rapport à la concurrence. Dans ces cas, le déploiement de

systèmes de gestion de réseau et de ressources d'ingénierie directes pour analyser les données de performances collectées entraîne des dépenses importantes. Toutefois, si l'on n'accorde pas l'attention voulue au principe souvent négligé de la synchronisation temporelle, ces efforts sont inefficaces.

Ce document décrit une définition de processus hypothétique pour la gestion de la fonction de gestion du réseau pour le protocole NTP (Network Time Protocol). Vous pouvez utiliser cet article comme une procédure hypothétique et un exemple informatif. L'entreprise peut personnaliser cette fonction pour répondre à ses objectifs internes.

Les informations fournies par ce document sont présentées dans plusieurs sections principales :

- La section [Terminologie](#) fournit des définitions générales des termes relatifs à la synchronisation temporelle.
- La section [Overview](#) fournit des informations de base sur le matériel des éléments de réseau liés à l'heure du système, une vue d'ensemble technologique de NTP et des aspects de conception clés pour l'architecture NTP.
- La section [Exemple de déploiement NTP](#) fournit des exemples de déploiement NTP avec des exemples de configurations pour les réseaux WAN, les réseaux de campus de haute strate et les réseaux de distribution de temps de campus de basse strate.
- La section [Définitions de processus](#) fournit une vue d'ensemble des définitions de processus utilisées pour accomplir la gestion NTP. Les détails du processus sont décrits en termes d'objectifs, d'indicateurs de performance, d'entrées, de sorties et de tâches individuelles.
- La section [Définitions des tâches](#) fournit des définitions de tâches de processus détaillées. Chaque tâche est décrite en termes d'objectifs, d'entrées de tâches, de sorties de tâches, de ressources nécessaires à l'accomplissement de la tâche et de compétences professionnelles requises pour un exécutant de tâches.
- La section [Identification des données](#) décrit l'identification des données pour NTP. L'identification des données tient compte de la source des informations. Par exemple, les informations peuvent être contenues dans la base MIB (Management Information Base) du protocole SNMP (Simple Network Management Protocol), dans les fichiers journaux générés par Syslog ou par des structures de données internes auxquelles seule l'interface de ligne de commande (CLI) peut accéder.
- La section [Data Collection](#) décrit la collecte des données NTP. La collecte des données est étroitement liée à l'emplacement des données. Par exemple, les données MIB SNMP sont collectées par plusieurs mécanismes, tels que des déroutements, des alarmes et des événements de surveillance à distance (RMON) ou des interrogations. Les données gérées par les structures de données internes sont collectées par des scripts automatiques ou lorsqu'un utilisateur se connecte manuellement au système pour émettre la commande CLI et enregistrer le résultat.
- La section [Présentation des données](#) fournit des exemples de format de rapport de la façon dont les données peuvent être présentées.

## Terminologie

- Précision : proximité de la valeur absolue de l'horloge par rapport au décalage de zéro.

- Précis : lorsqu'un décalage d'horloge est égal à zéro à un moment donné.
- Dérive : mesure de la variation de l'obliquité ou deuxième dérivation du décalage d'horloge par rapport au temps.
- Résolution commune : lorsque des horloges sont comparées, il s'agit de la somme des résolutions de C1 et C2. La résolution commune indique alors une limite inférieure prudente sur la précision de tout intervalle de temps calculé par des horodatages générés par une horloge soustraits de ceux générés par l'autre.
- Noeud : désigne une instanciation du protocole NTP sur un processeur local. Un noeud peut également être appelé un périphérique.
- Décalage : différence entre l'heure indiquée par une horloge et l'heure réelle, telle que définie par le temps universel coordonné (UTC). Si l'horloge indique une heure  $T_c$  et que l'heure réelle est  $T_t$ , le décalage d'horloge est  $T_c - T_t$ .
- Peer : désigne une instanciation du protocole NTP sur un processeur distant connecté par un chemin réseau à partir du noeud local.
- Décalage relatif : la notion de temps réel est remplacée par le temps tel que rapporté par l'horloge C1, lorsque deux horloges, C1 et C2, sont comparées. Par exemple, le décalage de l'horloge C2 par rapport à C1 à un moment particulier est  $T_{c2} - T_{c1}$ , la différence instantanée de temps rapportée par C2 et C1.
- Résolution : plus petite unité de mise à jour de l'heure d'horloge. La résolution est définie en termes de secondes. Cependant, la résolution est relative à l'heure du rapport d'horloge et non à l'heure réelle. Par exemple, une résolution de 10 millisecondes signifie que l'horloge met à jour sa notion de temps par incréments de 0,01 seconde et ne signifie pas qu'il s'agit du temps réel entre les mises à jour.



Remarque : les horloges peuvent avoir de très bonnes résolutions tout en étant inexactes.

---

- Inclinaison (Skew) : différence de fréquence d'horloge, ou dérivée première de son décalage par rapport au temps.
- Synchroniser : lorsque deux horloges sont précises l'une par rapport à l'autre (le décalage relatif est égal à zéro), elles sont synchronisées. Les horloges peuvent être synchronisées et encore inexactes en termes de la façon dont ils disent l'heure vraie.

## Aperçu

### Présentation des périphériques

Le coeur du service de temps est l'horloge système. L'horloge système démarre dès que le système démarre et conserve une trace de la date et de l'heure actuelles. L'horloge système peut

être réglée à partir d'un certain nombre de sources et, à son tour, peut être utilisée pour distribuer l'heure actuelle à d'autres systèmes par le biais de divers mécanismes. Certains routeurs contiennent un système de calendrier alimenté par batterie qui effectue le suivi de la date et de l'heure lors des redémarrages du système et des pannes de courant. Ce système de calendrier est toujours utilisé pour initialiser l'horloge système lors du redémarrage du système. Elle peut également être considérée comme une source de temps faisant autorité et redistribuée via NTP si aucune autre source n'est disponible. En outre, si NTP est activé, le calendrier est mis à jour périodiquement à partir de NTP, ce qui compense la dérive inhérente dans le temps du calendrier. Lorsqu'un routeur doté d'un calendrier système est initialisé, l'horloge système est définie en fonction de l'heure de son calendrier interne alimenté par batterie. Sur les modèles sans calendrier, l'horloge système est réglée sur une constante de temps prédéterminée. L'horloge système peut être réglée à partir des sources suivantes.

- NTP
- Protocole SNTP (Simple Network Time Protocol)
- Service de temps VINES (Virtual Integrated Network Service)
- Configuration manuelle

Certains périphériques Cisco bas de gamme prennent uniquement en charge le protocole SNTP. Le protocole SNTP est une version simplifiée du protocole NTP, réservée aux clients. SNTP peut uniquement recevoir l'heure des serveurs NTP et ne peut pas être utilisé pour fournir des services d'heure à d'autres systèmes. Le protocole SNTP fournit généralement un délai inférieur à 100 millisecondes de l'heure exacte. En outre, SNTP n'authentifie pas le trafic, bien que vous puissiez configurer des listes de contrôle d'accès étendues pour fournir une certaine protection. Un client SNTP est plus vulnérable aux serveurs non conformes qu'un client NTP et ne doit être utilisé que dans les situations où une authentification forte n'est pas requise.

L'horloge système indique l'heure des services suivants.

- NTP
- service VINES
- Commandes show de l'utilisateur
- Journalisation et débogage des messages

L'horloge système effectue le suivi de l'heure en interne en fonction de l'heure UTC, également appelée heure GMT (Greenwich Mean Time). Vous pouvez configurer les informations relatives au fuseau horaire local et à l'heure d'été afin que l'heure soit affichée correctement par rapport au fuseau horaire local. L'horloge système effectue un suivi pour savoir si l'heure fait autorité ou non. S'il ne fait pas autorité, l'heure ne peut être disponible qu'à des fins d'affichage et ne peut pas être redistribuée.

## Présentation de NTP

NTP est conçu pour synchroniser l'heure sur un réseau de machines. Le protocole NTP s'exécute sur le protocole UDP (User Datagram Protocol), avec le port 123 comme source et comme destination, qui s'exécute à son tour sur IP. NTP Version 3 [RFC 1305](#) est utilisé pour synchroniser la mesure du temps entre un ensemble de serveurs et de clients de temps distribués. Un ensemble de noeuds sur un réseau sont identifiés et configurés avec NTP et les noeuds forment un sous-réseau de synchronisation, parfois appelé réseau de superposition. Bien que plusieurs serveurs principaux puissent exister, aucun protocole de sélection n'est requis.

Un réseau NTP obtient généralement son heure à partir d'une source de temps faisant autorité, telle qu'une horloge radio ou une horloge atomique connectée à un serveur de temps. Le protocole NTP distribue ensuite cette heure sur le réseau. Un client NTP effectue une transaction avec son serveur au cours de son intervalle d'interrogation (de 64 à 1024 secondes) qui change dynamiquement au fil du temps en fonction des conditions réseau entre le serveur NTP et le client. L'autre situation se produit lorsque le routeur communique avec un serveur NTP défectueux (par exemple, un serveur NTP avec une grande dispersion) ; le routeur augmente également l'intervalle d'interrogation. Une seule transaction NTP par minute est nécessaire pour synchroniser deux machines.

NTP utilise le concept de strate pour décrire le nombre de sauts NTP à partir d'une source temporelle faisant autorité. Par exemple, un serveur de temps de strate 1 est directement relié à une horloge radio ou atomique. Il envoie ensuite son heure à un serveur de temps de strate 2 via NTP, et ainsi de suite. Une machine qui exécute NTP choisit automatiquement la machine avec le numéro de strate le plus bas qu'elle est configurée pour communiquer avec NTP comme source de temps. Cette stratégie construit une organisation autonome efficace de haut-parleurs NTP. Le protocole NTP fonctionne bien sur les longueurs de chemin non déterministes des réseaux à commutation de paquets, car il effectue des estimations robustes des trois variables clés suivantes dans la relation entre un client et un serveur de temps.

- Délai réseau
- Dispersion des échanges de paquets de temps : mesure de l'erreur d'horloge maximale entre les deux hôtes.
- Décalage d'horloge : correction appliquée à une horloge client pour la synchroniser.

La synchronisation d'horloge au niveau de 10 millisecondes sur les réseaux étendus longue distance (WAN) (2 000 km) et au niveau de 1 milliseconde pour les réseaux locaux (LAN) est réalisée de manière régulière.

Il y a deux façons dont NTP ne se synchronise pas avec une machine dont l'heure n'est pas précise. Tout d'abord, NTP ne se synchronise jamais sur une machine qui n'est pas elle-même synchronisée. Deuxièmement, NTP compare le temps signalé par plusieurs machines et ne se synchronise pas avec une machine dont le temps est significativement différent des autres, même si sa strate est plus basse.

Les communications entre les ordinateurs qui exécutent des associations NTP sont généralement configurées de manière statique. Chaque machine reçoit l'adresse IP de toutes les machines avec lesquelles elle doit former des associations. La synchronisation précise est rendue possible par

les messages NTP échangés entre chaque paire de machines avec une association. Cependant, dans un environnement LAN, NTP peut être configuré pour utiliser des messages de diffusion IP à la place. Cette alternative réduit la complexité de configuration, car chaque machine peut être configurée pour envoyer ou recevoir des messages de diffusion. Cependant, la précision de la mesure du temps est légèrement réduite car le flux d'informations est unidirectionnel.

Le temps conservé sur une machine est une ressource critique et il est fortement recommandé d'utiliser les fonctions de sécurité de NTP pour éviter le réglage accidentel ou malveillant d'une heure incorrecte. Les deux fonctions de sécurité disponibles sont un schéma de restriction basé sur une liste d'accès et un mécanisme d'authentification chiffré.

La mise en oeuvre de NTP par Cisco prend en charge le service de strate 1 dans certaines versions du logiciel Cisco IOS®. Si une version prend en charge la commande `ntp refclock`, il est possible de connecter une horloge radio ou atomique. Certaines versions de Cisco IOS prennent en charge le kit de synchronisation NTP Trimble Palisade (routeurs de la gamme Cisco 7200 uniquement) ou le périphérique GPS (Global Positioning System) de Telecom Solutions. Si le réseau utilise les serveurs de temps publics sur Internet et que le réseau est isolé d'Internet, l'implémentation Cisco de NTP permet de configurer une machine de sorte qu'elle agisse comme si elle était synchronisée via NTP, alors qu'en fait elle a déterminé l'heure par d'autres moyens. D'autres machines se synchronisent ensuite sur cette machine via NTP.

## Critères de conception NTP

Chaque client du sous-réseau de synchronisation, qui peut également être un serveur pour les clients de strate supérieure, choisit l'un des serveurs disponibles pour la synchronisation. Il s'agit généralement des serveurs de la strate inférieure auxquels il a accès. Cependant, cette configuration n'est pas toujours optimale, car le protocole NTP fonctionne également en partant du principe que chaque heure du serveur doit être considérée avec une certaine méfiance. NTP préfère avoir accès à plusieurs sources de strate inférieure (au moins trois) puisqu'il peut alors appliquer un algorithme d'accord pour détecter la folie de l'une de ces sources. Normalement, lorsque tous les serveurs sont d'accord, NTP choisit le meilleur serveur en termes de strate la plus basse, le plus proche (en termes de délai réseau) et la précision revendiquée. Il en résulte que, même si l'on doit s'efforcer de fournir à chaque client trois sources ou plus de temps de strate inférieur, plusieurs d'entre elles ne peuvent fournir qu'un service de secours et peuvent être de moindre qualité en termes de délai réseau et de strate. Par exemple, un homologue de même strate qui reçoit du temps de sources de strate inférieure auxquelles le serveur local n'accède pas directement peut également fournir un bon service de sauvegarde.

Le protocole NTP préfère généralement les serveurs de strate inférieure aux serveurs de strate supérieure, à moins que la durée du serveur de strate inférieure ne soit sensiblement différente. L'algorithme est capable de détecter lorsqu'une source temporelle est susceptible d'être extrêmement imprécise, ou folle, et d'empêcher la synchronisation dans ces cas, même si l'horloge imprécise est à un niveau de strate inférieur. Et il ne peut jamais synchroniser un périphérique avec un autre serveur qui n'est pas lui-même synchronisé.

Afin de déclarer si le serveur est fiable, il doit passer de nombreux contrôles de santé mentale, tels que :

- Les mises en oeuvre doivent inclure des délais d'expiration de la santé qui empêchent les transmissions de déroutements si le programme de surveillance ne renouvelle pas ces informations après un intervalle prolongé.
- Des contrôles de santé supplémentaires sont inclus pour l'authentification, les limites de plage et pour éviter l'utilisation de données très anciennes.
- Des vérifications ont été ajoutées pour avertir que l'oscillateur est resté trop longtemps sans mise à jour d'une source de référence.
- Les variables peer.valid et sys.hold ont été ajoutées pour éviter les instabilités lorsque la source de référence change rapidement en raison de retards dispersifs importants dans des conditions de congestion grave du réseau. Les bits peer.config, peer.authenticable et peer.authenticable ont été ajoutés pour contrôler des fonctionnalités spéciales et simplifier la configuration.

Si au moins une de ces vérifications échoue, le routeur la déclare folle.

## Modes d'association

Les sections suivantes décrivent les modes d'association utilisés par les serveurs NTP pour s'associer entre eux.

- Client/Serveur
- Actif/passif symétrique
- Diffusion

### Mode client/serveur

Les clients et les serveurs dépendants fonctionnent normalement en mode client/serveur, dans lequel un client ou un serveur dépendant peut être synchronisé avec un membre du groupe, mais aucun membre du groupe ne peut être synchronisé avec le client ou le serveur dépendant. Cela permet de se protéger contre les dysfonctionnements ou les attaques de protocole.

Le mode client/serveur est la configuration Internet la plus courante. Il fonctionne selon le paradigme RPC (remote-procedure-call) classique avec des serveurs sans état. Dans ce mode, un client envoie une requête au serveur et attend une réponse à un moment ultérieur. Dans certains contextes, il s'agit d'une opération d'interrogation, dans la mesure où le client interroge les données d'heure et d'authentification à partir du serveur. Un client est configuré en mode client à l'aide de la commande server et du nom ou de l'adresse DNS (Domain Name Server) spécifié. Le serveur ne nécessite aucune configuration préalable.

Dans un modèle client/serveur commun, un client envoie un message NTP à un ou plusieurs serveurs et traite les réponses reçues. Le serveur échange des adresses et des ports, remplace certains champs du message, recalcule la somme de contrôle et renvoie le message immédiatement. Les informations contenues dans le message NTP permettent au client de



déterminer l'heure du serveur par rapport à l'heure locale, puis d'ajuster l'horloge locale si nécessaire. En outre, le message inclut des informations permettant de calculer la précision et la fiabilité du chronométrage attendu, ainsi que de sélectionner le meilleur serveur.

Les serveurs qui fournissent la synchronisation à une population importante de clients fonctionnent normalement comme un groupe de trois serveurs mutuellement redondants ou plus, et chacun fonctionne avec trois serveurs strate 1 ou strate 2 ou plus en mode client/serveur, ainsi que tous les autres membres du groupe en mode symétrique. Cela offre une protection contre les dysfonctionnements dans lesquels un ou plusieurs serveurs ne fonctionnent pas ou fournissent une heure incorrecte. Les algorithmes NTP sont conçus pour résister aux attaques lorsqu'une partie des sources de synchronisation configurées fournit accidentellement ou délibérément un temps incorrect. Dans ces cas, une procédure de vote spéciale est utilisée pour identifier les sources douteuses et éliminer leurs données. Dans un souci de fiabilité, les hôtes sélectionnés peuvent être équipés d'horloges externes et utilisés pour la sauvegarde en cas de panne des serveurs primaire et/ou secondaire, ou des chemins de communication entre eux.

La configuration d'une association en mode client est généralement indiquée par une déclaration de serveur dans le fichier de configuration et indique que vous voulez obtenir du temps du serveur distant, mais que vous ne voulez pas donner du temps au serveur distant.

#### Mode actif/passif symétrique

Le mode symétrique actif/passif est destiné aux configurations dans lesquelles un groupe d'homologues de couche inférieure fonctionnent comme des sauvegardes mutuelles. Chaque homologue fonctionne avec une ou plusieurs sources de référence principales, telles qu'une horloge radio, ou un sous-ensemble de serveurs secondaires fiables. Si l'un des homologues perd toutes les sources de référence ou cesse simplement son fonctionnement, les autres homologues se reconfigurent automatiquement de sorte que les valeurs de temps puissent circuler des homologues actuels vers tous les autres homologues de la file d'attente. Dans certains contextes, il s'agit d'une opération push-pull, dans laquelle l'homologue tire ou pousse le temps et les valeurs en fonction de la configuration particulière.


La configuration d'une association en mode actif symétrique, généralement indiquée par une déclaration homologue dans le fichier de configuration, indique au serveur distant que l'on souhaite obtenir du temps du serveur distant et que l'on est également disposé à fournir du temps au serveur distant si nécessaire. Ce mode est approprié dans les configurations qui impliquent un certain nombre de serveurs temporels redondants interconnectés par divers chemins réseau, ce qui est actuellement le cas pour la plupart des serveurs de strate 1 et de strate 2 sur Internet aujourd'hui.

Les modes symétriques sont le plus souvent utilisés entre deux serveurs ou plus qui fonctionnent comme un groupe mutuellement redondant. Dans ces modes, les serveurs des membres du groupe organisent les chemins de synchronisation pour obtenir des performances maximales, en fonction de la gigue du réseau et du délai de propagation. Si un ou plusieurs membres du groupe échouent, les membres résiduels sont automatiquement reconfigurés selon les besoins.

Un homologue est configuré en mode actif symétrique avec la commande peer et lorsque le nom

DNS ou l'adresse de l'autre homologue est spécifié. L'autre homologue est également configuré en mode actif symétrique de cette manière.

---

 Remarque : si l'autre homologue n'est pas spécifiquement configuré de cette manière, une association passive symétrique est activée à l'arrivée d'un message actif symétrique. Comme un intrus peut se faire passer pour un homologue actif symétrique et injecter de fausses valeurs de temps, le mode symétrique doit toujours être authentifié.

---

## Mode de diffusion et/ou de multidiffusion

Lorsque les exigences en matière de précision et de fiabilité sont modestes, les clients peuvent être configurés pour utiliser des modes de diffusion et/ou de multidiffusion. Normalement, ces modes ne sont pas utilisés par les serveurs avec des clients dépendants. L'avantage est que les clients n'ont pas besoin d'être configurés pour un serveur spécifique, ce qui permet à tous les clients opérationnels d'utiliser le même fichier de configuration. Le mode de diffusion nécessite un serveur de diffusion sur le même sous-réseau. Étant donné que les messages de diffusion ne sont pas propagés par les routeurs, seuls les serveurs de diffusion du même sous-réseau sont utilisés.

Le mode de diffusion est conçu pour les configurations impliquant un ou plusieurs serveurs et une population de clients potentiellement importante. Un serveur de diffusion est configuré avec la commande `broadcast` et une adresse de sous-réseau local. Un client de diffusion est configuré avec la commande `broadcast client`, qui permet au client de diffusion de répondre aux messages de diffusion reçus sur n'importe quelle interface. Comme un intrus peut se faire passer pour un serveur de diffusion et injecter de fausses valeurs de temps, ce mode doit toujours être authentifié.

## Set NTP Leap Second

Vous pouvez utiliser la commande `ntp leap {add | delete}` afin d'insérer une seconde intercalaire. Il existe des options pour ajouter ou supprimer des secondes intercalaires. Il existe deux contraintes pour que cela se produise :

- L'horloge doit être synchronisée.
- La commande n'est acceptée que dans le mois précédant le saut. Il ne peut pas définir de saut si l'heure actuelle est antérieure à 1 mois de l'occurrence du saut.

Après l'avoir défini, la seconde intercalaire est ajoutée ou supprimée à la dernière seconde comme indiqué ici :

```
<#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
```

## Architecture NTP

Ces trois structures sont disponibles pour l'architecture NTP :

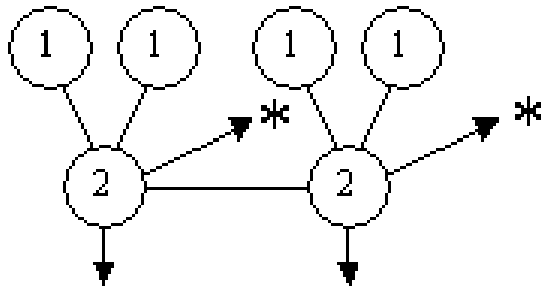
- Structure d'homologue plate
- Structure hiérarchique
- Structure en étoile

Dans une structure d'homologues plate, tous les routeurs sont homologues entre eux, avec quelques routeurs géographiquement séparés configurés pour pointer vers des systèmes externes. La convergence du temps s'allonge avec chaque nouveau membre du maillage NTP.

Dans une structure hiérarchique, la hiérarchie de routage est copiée pour la hiérarchie NTP. Les routeurs principaux ont une relation client/serveur avec des sources de temps externes, les serveurs de temps internes ont une relation client/serveur avec les routeurs principaux, les routeurs d'utilisateur interne (serveurs autres que de temps) ont une relation client/serveur avec les serveurs de temps internes, et ainsi de suite dans l'arborescence. Ces relations sont appelées échelles hiérarchiques. Une structure hiérarchique est la technique privilégiée car elle assure cohérence, stabilité et évolutivité.

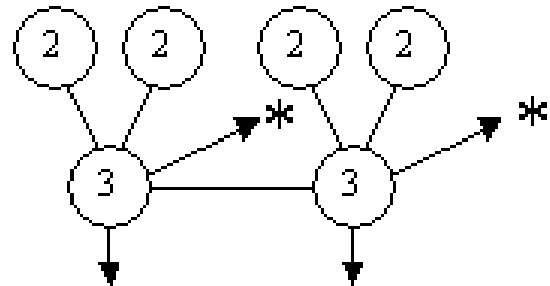
Une architecture NTP évolutive a une structure hiérarchique comme le montre le schéma suivant.

Internet Primary Servers  
(Stratum 1)



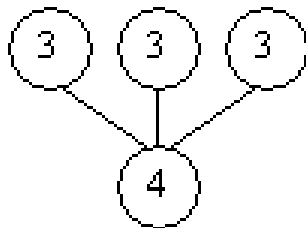
\* = to buddy in another subnet

Campus Secondary Servers  
(Stratum 2)

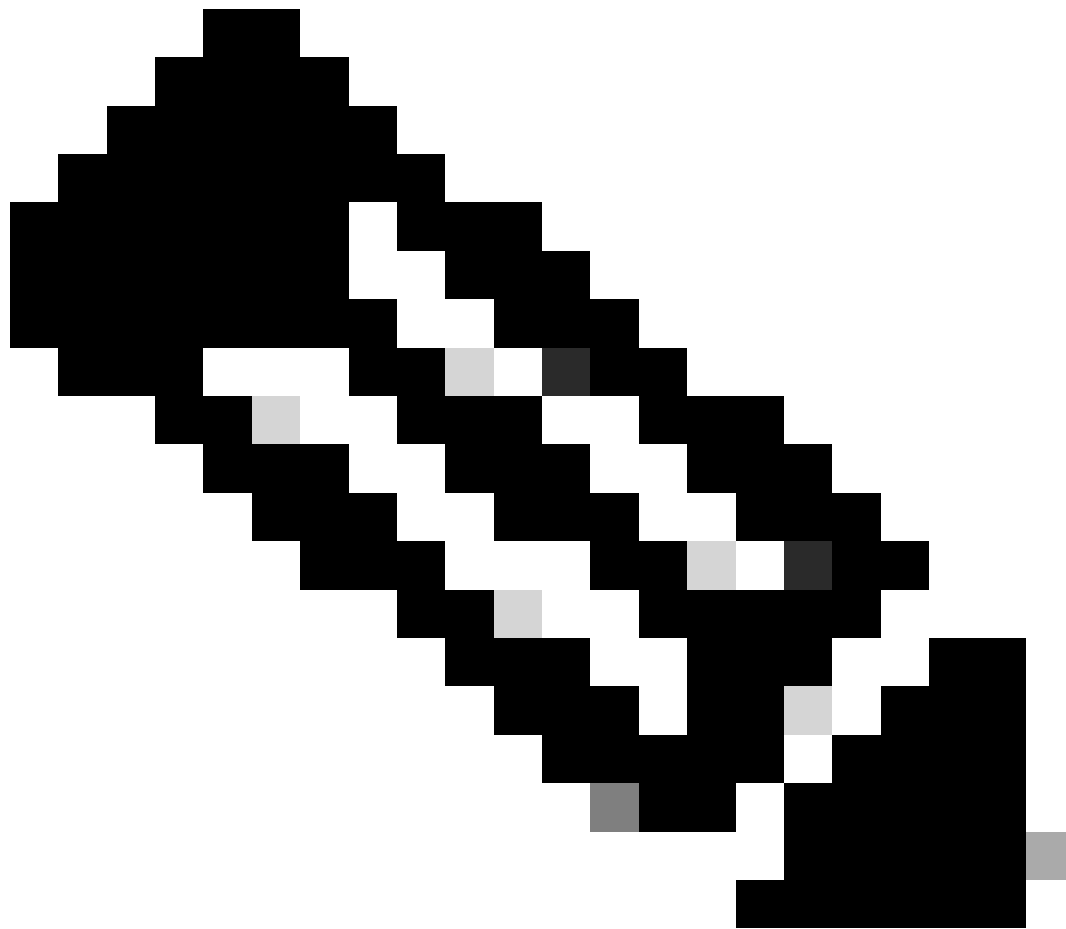


\* = to buddy in another subnet

Department Servers  
(Stratum 3)



Workstations (Stratum 4)



Remarque : série de graphiques illustrant un déploiement NTP hiérarchique et évolutif. Le premier graphique montre deux périphériques NTP de strate 2, chacun étant connecté à deux périphériques de strate 1 (illustrés dans le schéma précédent des périphériques de strate 2) et un copain dans un autre sous-réseau indiqué par un astérisque. En outre, chaque périphérique de strate 2 comporte une flèche pointant vers le bas. Le deuxième graphique présente la même disposition, mais avec les périphériques de strate 2 où se trouvaient les périphériques de strate 1 et les périphériques de strate 3 où se trouvaient les périphériques de strate 2. Le troisième graphique comporte un équipement de strate 4 connecté à trois équipements de strate 3. En résumé, l'image présente une topologie dans laquelle chaque périphérique est connecté à 2 ou 3 périphériques avec une strate inférieure d'un (meilleure que la sienne).


---

Dans une structure en étoile, tous les routeurs ont une relation client/serveur avec quelques serveurs temporels dans le coeur. Les serveurs de temps dédiés sont le centre de l'étoile et sont généralement des systèmes UNIX synchronisés avec des sources de temps externes, ou leur propre récepteur GPS.

## Technologie d'horloge et serveurs de temps publics

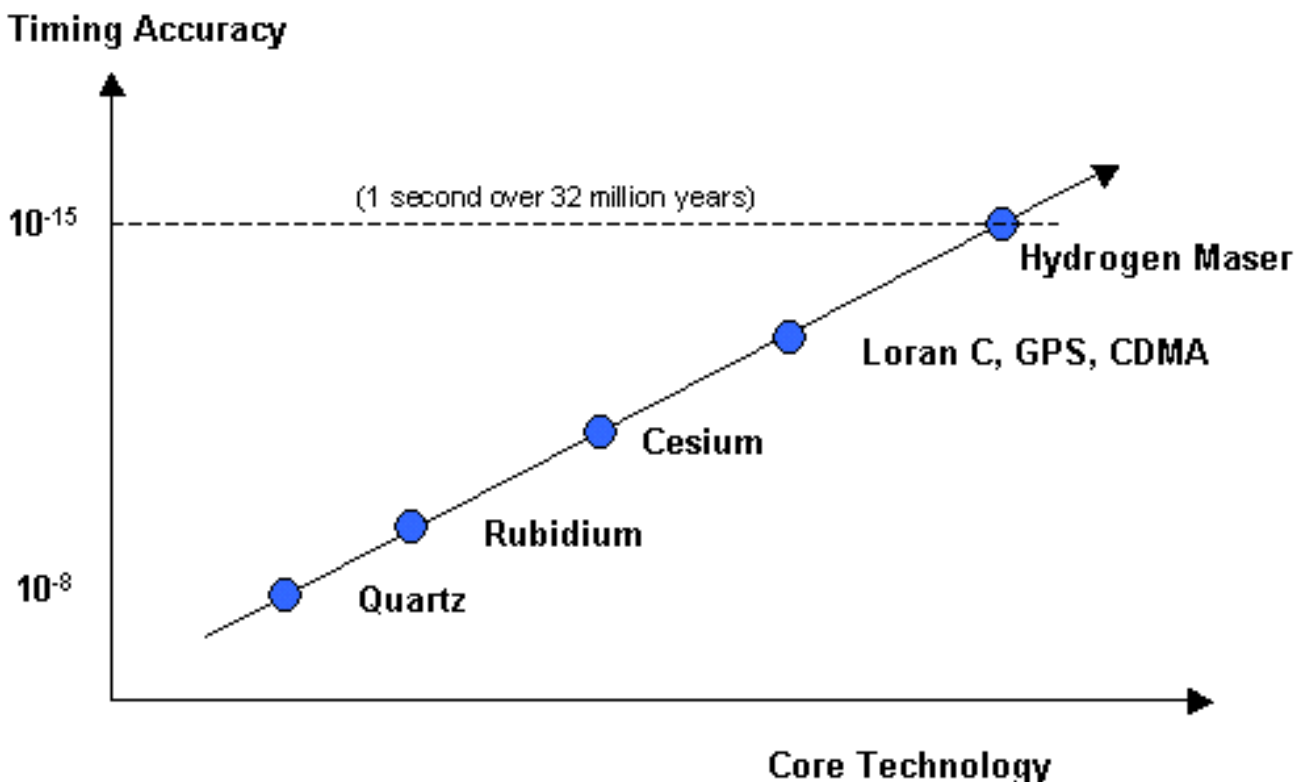
Le sous-réseau Internet NTP comprend actuellement plus de 50 serveurs publics principaux synchronisés directement avec UTC par radio, satellite ou modem. Normalement, les postes de travail client et les serveurs avec un nombre relativement réduit de clients ne sont pas synchronisés aux serveurs principaux. Environ 100 serveurs publics secondaires sont synchronisés avec les serveurs principaux et assurent la synchronisation avec un total de plus de 100 000 clients et serveurs sur Internet. Les listes de [serveurs de temps NTP publics](#) sont mises à jour fréquemment. Il existe également de nombreux serveurs privés principaux et secondaires qui ne sont pas normalement accessibles au public.

---

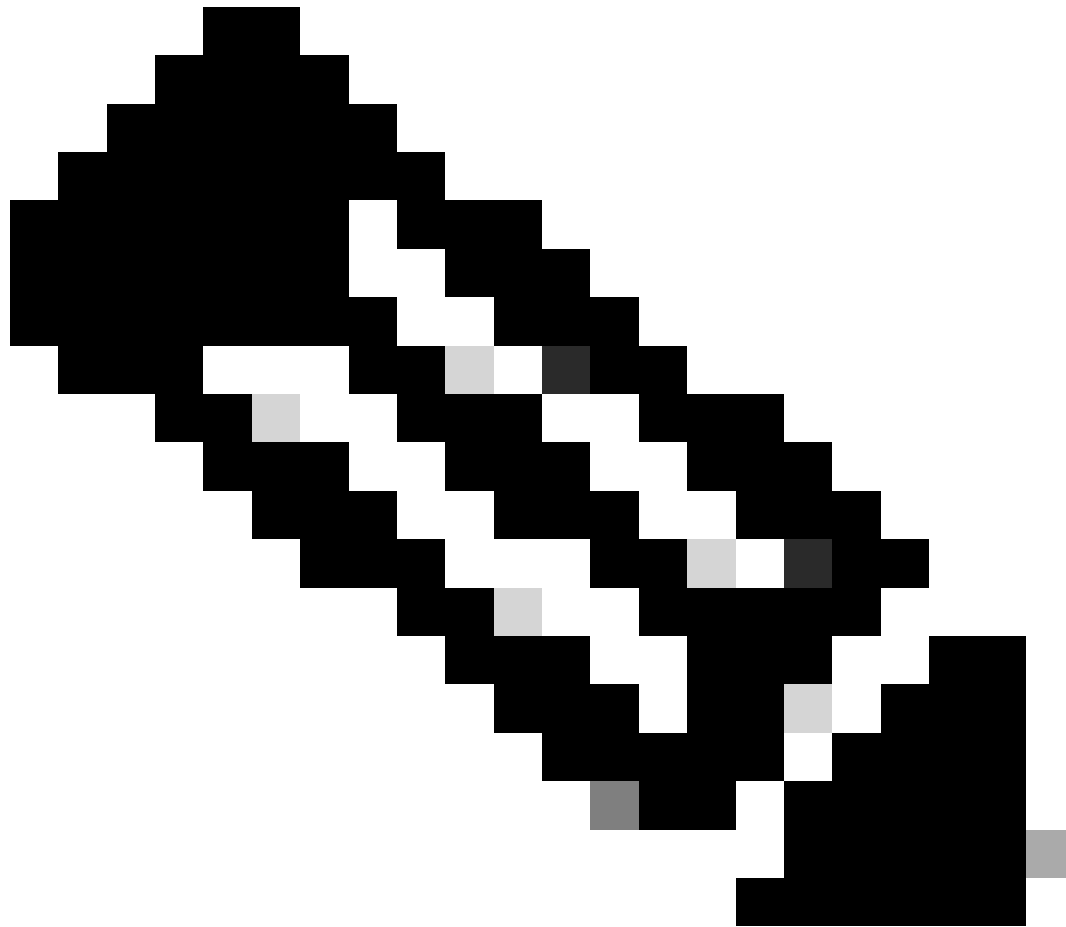
 Remarque : PIX et ASA ne peuvent pas être configurés en tant que serveur NTP, mais ils peuvent être configurés en tant que client NTP.

---

Dans certains cas, lorsque des services de temps très précis sont requis sur l'entreprise privée, tels que des mesures unidirectionnelles pour les mesures de voix sur IP (VoIP), les concepteurs de réseau peuvent choisir de déployer des sources de temps externes privées. Le schéma suivant montre un graphique comparatif de la précision relative des technologies actuelles.



Graphique Comparatif



Note : Un graphique qui présente des moyens de plus en plus précis de garder le temps du quartz (10 à la puissance négative 8) au maser à hydrogène (10 à la puissance négative 15). Ce dernier indique une perte de précision d'environ 1 seconde sur 32 millions d'années. Les autres méthodes énumérées entre ces deux (du moins au plus précis) sont le rubidium, le césium, le Loran C, le GPS et le CDMA. Les trois derniers (Loran C, GPS et CDMA) sont répertoriés ensemble.

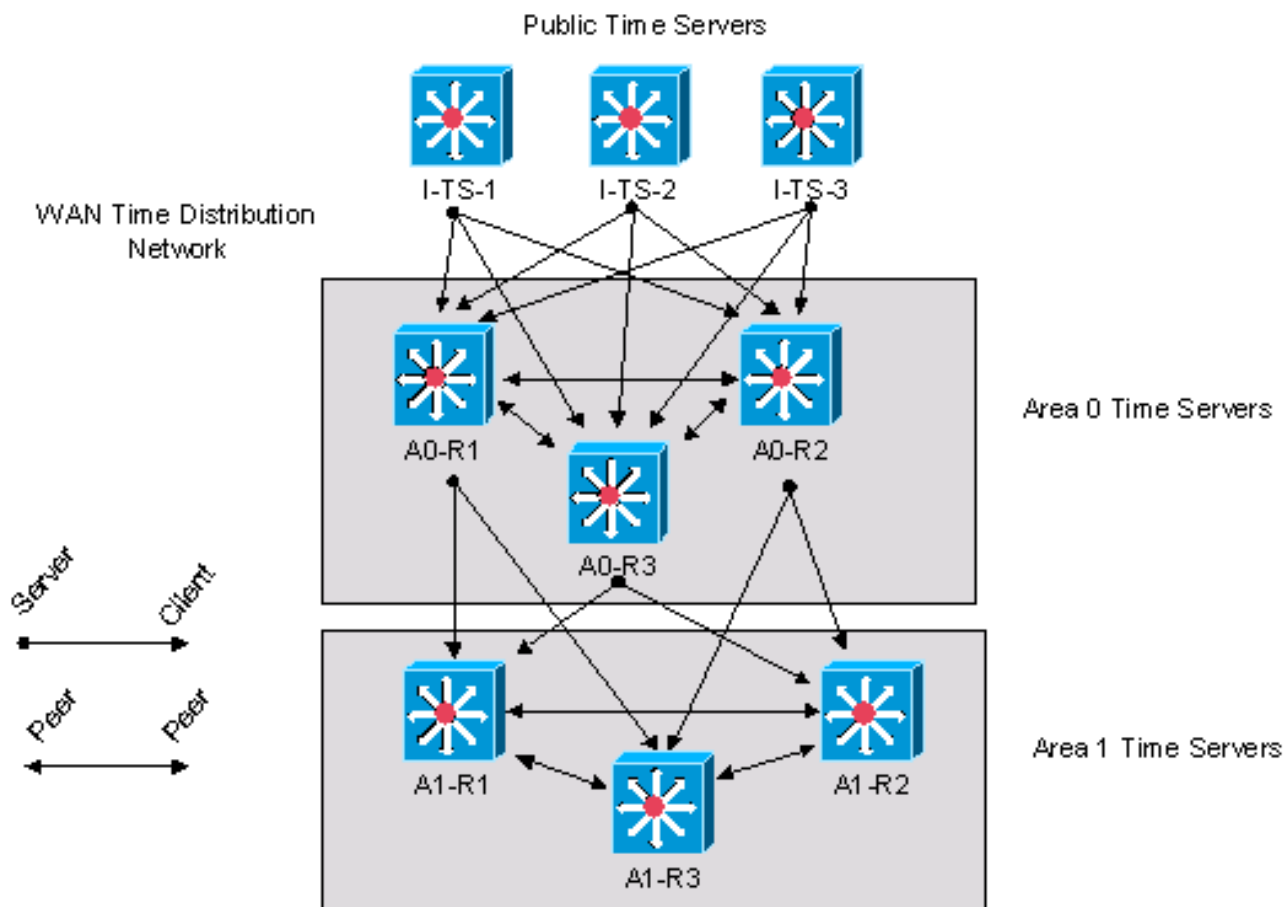
---

Jusqu'à récemment, l'utilisation de sources de temps externes n'avait pas été largement déployée dans les réseaux d'entreprise en raison du coût élevé des sources de temps externes de qualité. Cependant, à mesure que les exigences de qualité de service (QoS) augmentent et que le coût de la technologie de gestion du temps continue de diminuer, les sources de temps externes pour les réseaux d'entreprise constituent une option viable.

## Exemples de déploiements NTP

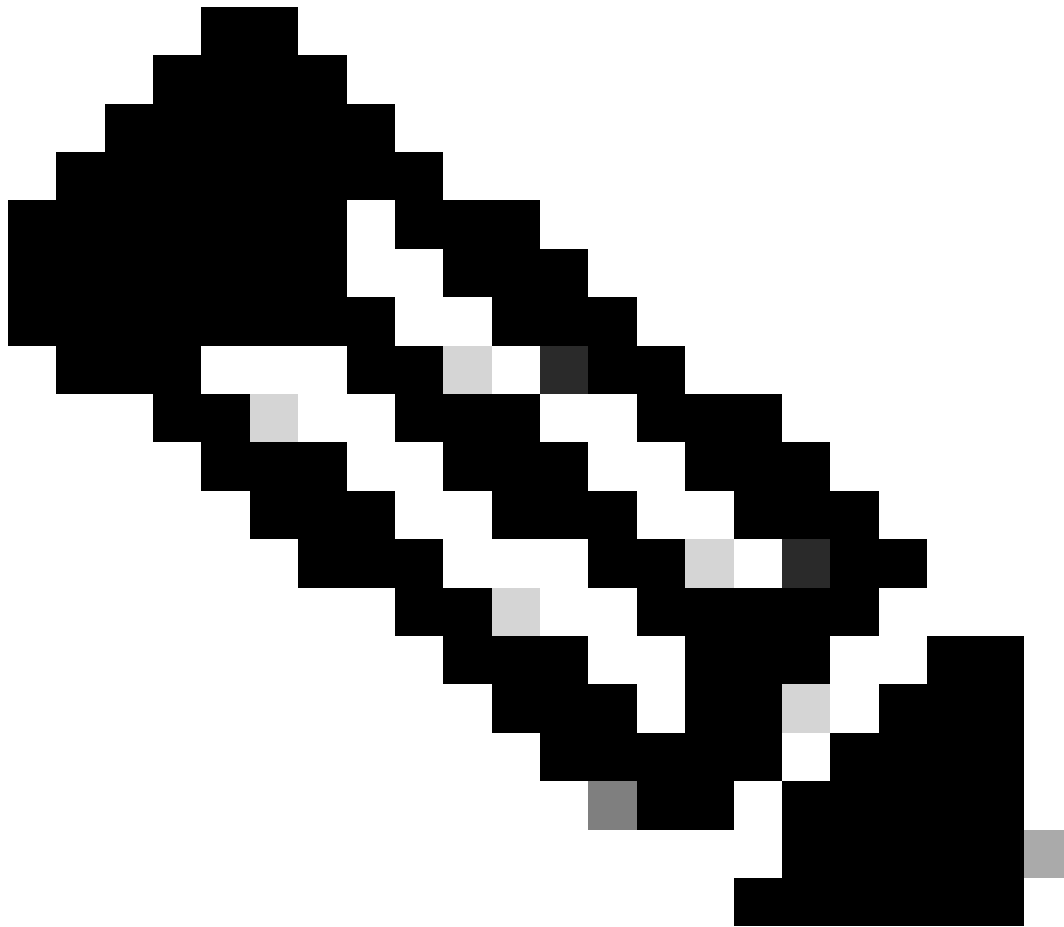
Réseau de distribution temporelle WAN

Dans le schéma suivant, un système autonome d'entreprise (AS) obtient des informations de temps à partir de trois serveurs de temps publics. Le système autonome d'entreprise est représenté par les serveurs de temps de la zone 0 et de la zone 1. Dans cet exemple, la hiérarchie NTP décrit la hiérarchie OSPF (Open Shortest Path First). Cependant, OSPF n'est pas une condition préalable au protocole NTP. Il n'est utilisé qu'à titre d'exemple. Le protocole NTP peut être déployé le long d'autres frontières hiérarchiques logiques, telles qu'une hiérarchie EIGRP (Enhanced Interior Gateway Routing Protocol) ou la hiérarchie de base/distribution/accès standard.



Réseau de distribution temporelle WAN





Remarque : diagramme présentant une topologie NTP qui couvre plusieurs réseaux. Trois périphériques de la zone 1 (OSPF) sont des homologues et des clients de serveurs de la zone 0. Trois périphériques de la zone 0 sont des homologues, des clients de serveurs de temps publics et des serveurs de clients de la zone 1. Les serveurs de temps publics sont uniquement affichés en tant que serveurs pour les clients dans la zone 0.

---

Cet exemple est la configuration de Cisco IOS pour le périphérique A0-R1, comme illustré dans le schéma précédent.

```
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.*

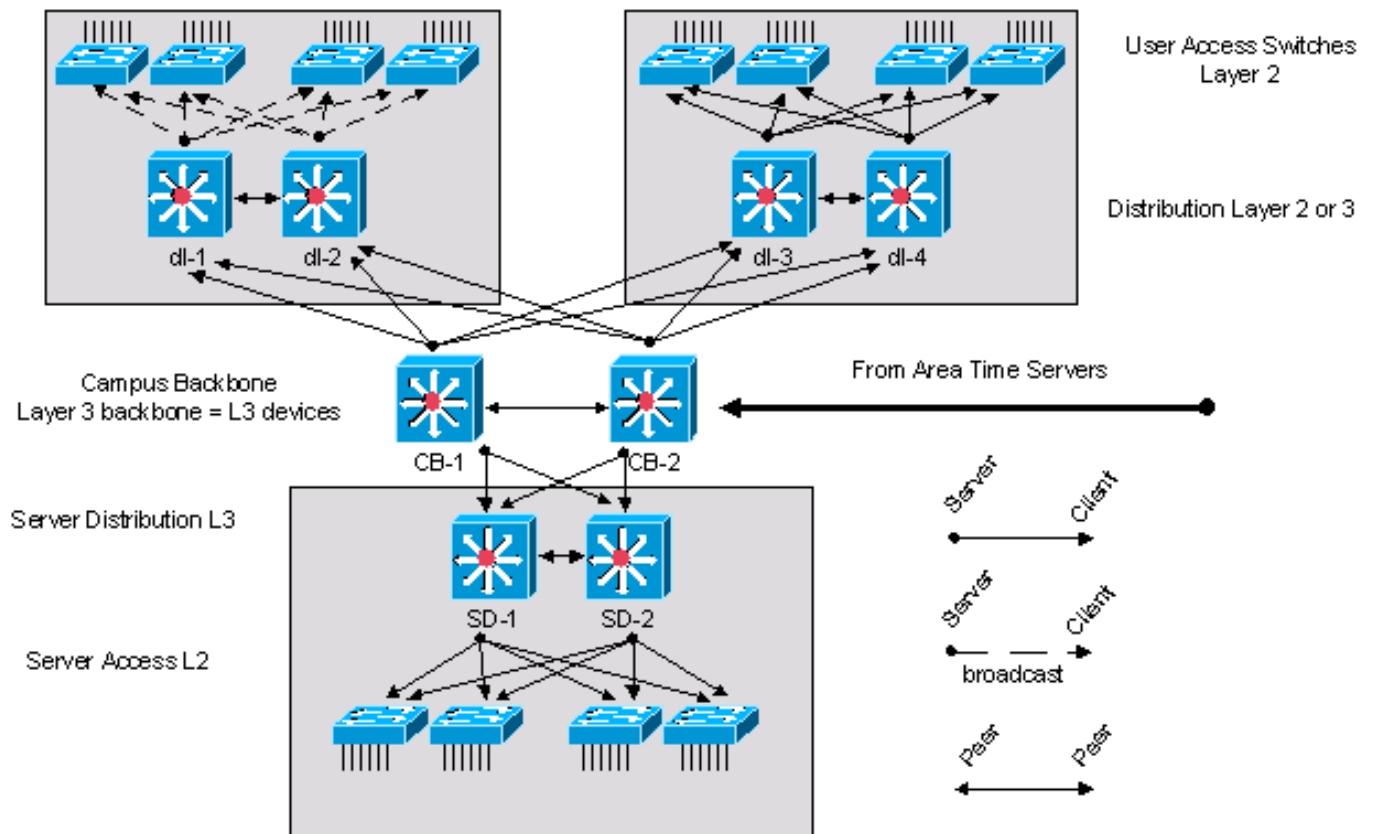
```
ntp server <I-TS-1>  
ntp server <I-TS-2>  
ntp server <I-TS-3>  
ntp peer <A0-R2>  
ntp peer <A0-R3>
```

## Réseau de distribution du temps de campus à strate élevée

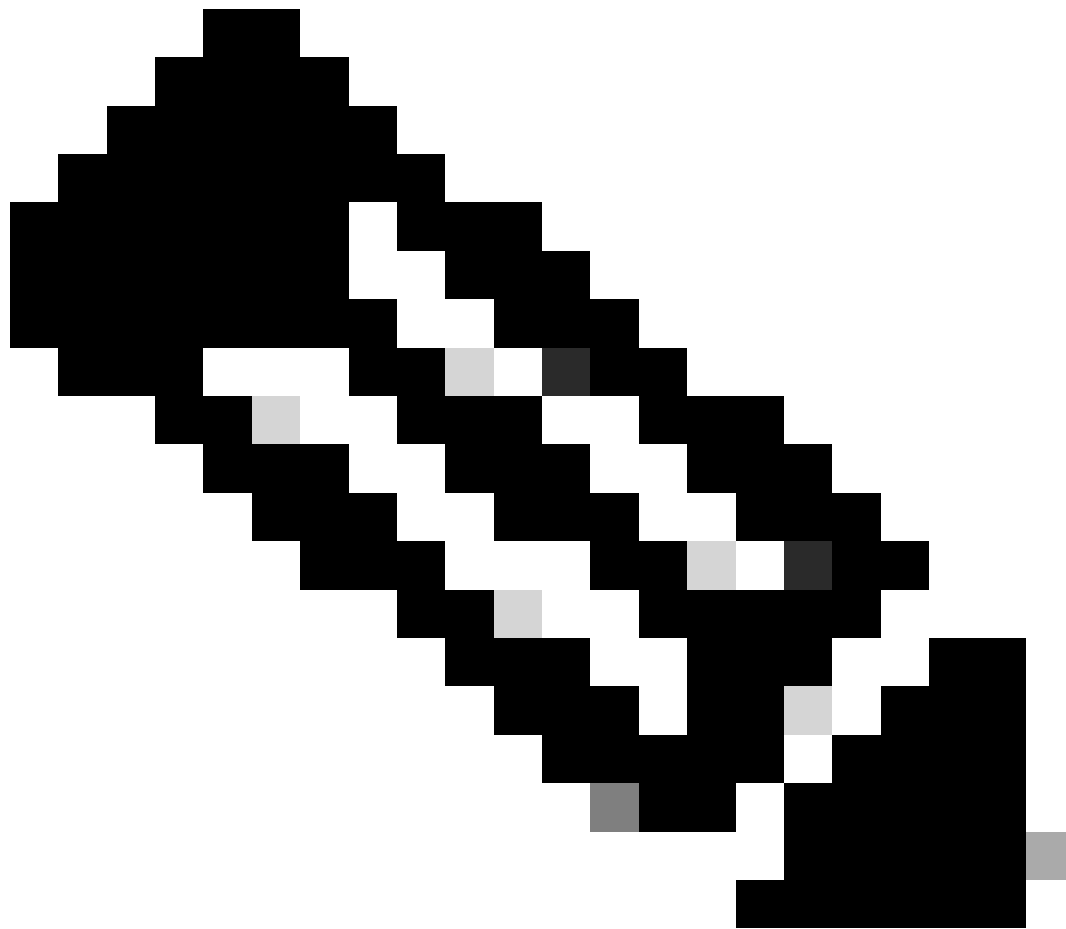
La section précédente décrivait un réseau de distribution du temps WAN. Cette section descend d'un niveau dans la hiérarchie pour aborder la répartition du temps sur un réseau de campus de haute strate.

La principale différence pour la distribution temporelle sur un réseau de campus de strate supérieure est l'utilisation potentielle du mode d'association de diffusion. Comme décrit précédemment, le mode d'association de diffusion simplifie les configurations des réseaux locaux, mais réduit la précision des calculs de temps. Par conséquent, l'arbitrage des coûts d'entretien doit être considéré par rapport à l'exactitude des mesures de performance.

High Stratum Campus  
Time Distribution Network



Réseau de distribution du temps de campus à strate élevée



Remarque : un schéma intitulé High Stratum Campus Time Distribution Network qui inclut une topologie générique à trois niveaux (backbone, distribution, accès). Les commutateurs d'accès sont des clients de commutateurs de distribution, les commutateurs de distribution sont des clients de commutateurs de réseau fédérateur et les commutateurs de réseau fédérateur sont des clients de serveurs de temps de zone (non représentés). Les commutateurs de distribution sont divisés en paires et ont une relation d'homologue uniquement avec l'autre commutateur de la paire. Les deux commutateurs de réseau fédérateur sont également des homologues. Quatre commutateurs d'accès (en haut à gauche) sont représentés comme des clients de diffusion avec des flèches en pointillés, tandis que toutes les autres relations client-serveur et homologue-homologue ne sont pas de diffusion.

---

Le réseau de campus de couche supérieure, illustré dans le schéma précédent, est issu de la conception de réseau de campus Cisco standard et contient trois composants. Le coeur du campus se compose de deux périphériques de couche 3 étiquetés CB-1 et CB-2. Le composant serveur, situé dans la section inférieure de la figure, comporte deux routeurs de couche 3 étiquetés SD-1 et SD-2. Les autres périphériques du bloc serveur sont des périphériques de

couche 2. En haut à gauche, il y a un bloc d'accès standard avec deux périphériques de distribution de couche 3 étiquetés dl-1 et dl-2. Les autres périphériques sont des commutateurs de couche 2. Dans ce bloc d'accès client, l'heure est distribuée avec l'option de diffusion. En haut à droite, il y a un autre bloc d'accès standard qui utilise une configuration de distribution de l'heure client/serveur.

Les périphériques de réseau fédérateur de campus sont synchronisés avec les serveurs de temps de zone dans un modèle client/serveur.

Voici la configuration des périphériques de distribution dl-1 de couche 3 :

```
!--- 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.
```

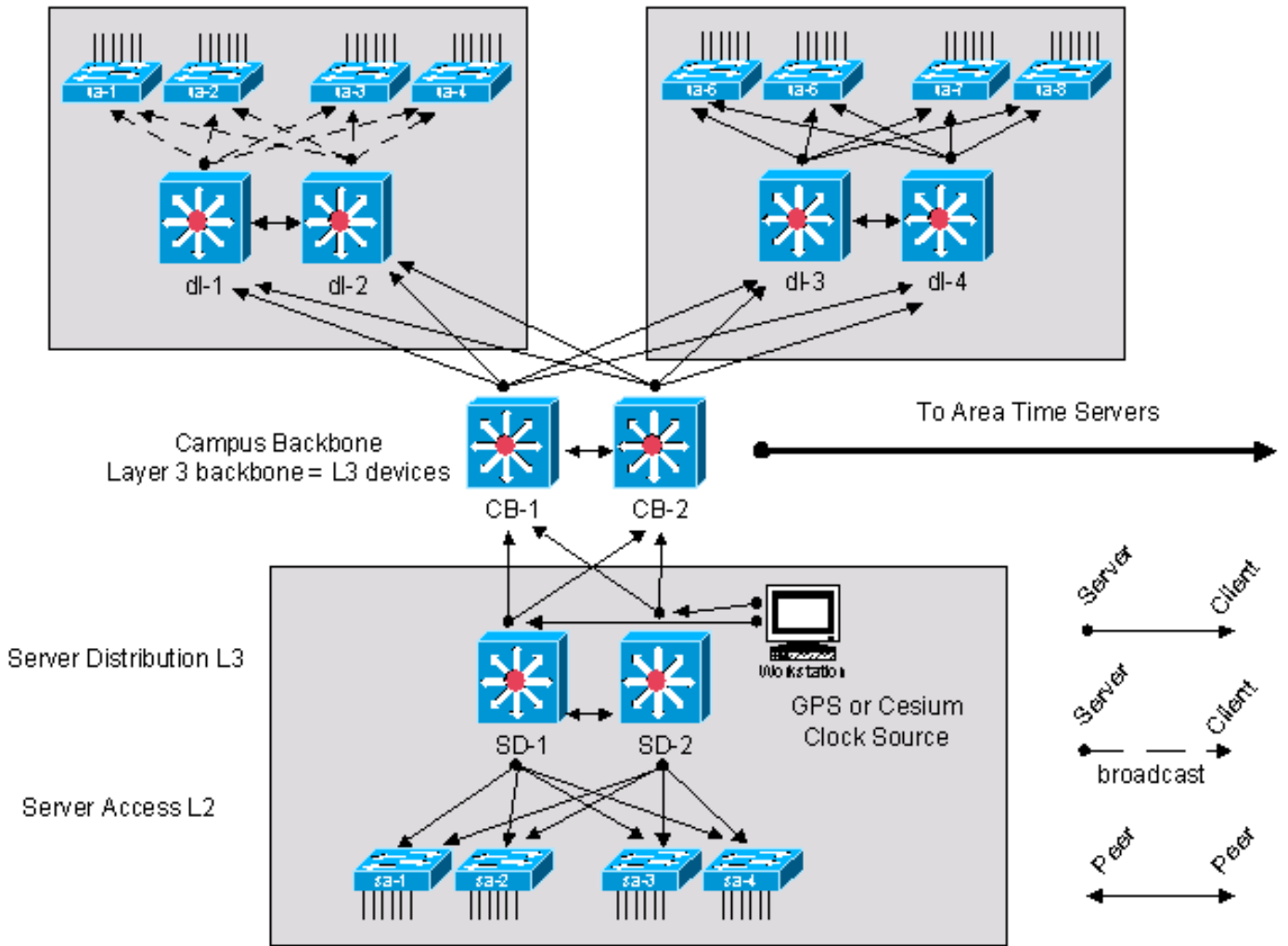
```
ntp server <CB-1>  
ntp server <CB-2>  
ntp peer <d1-2>
```

## réseau de distribution du temps de campus à faible strate

Dans le schéma suivant, une source de temps GPS ou Cesium est fournie au centre de données central pour le réseau de campus de strate inférieure. Cela permet d'obtenir une source temporelle de strate 1 sur le réseau privé. S'il existe plusieurs sources de temps GPS ou Cesium dans le réseau privé, la répartition du temps dans le réseau privé doit être modifiée pour tirer parti des sources de temps disponibles.

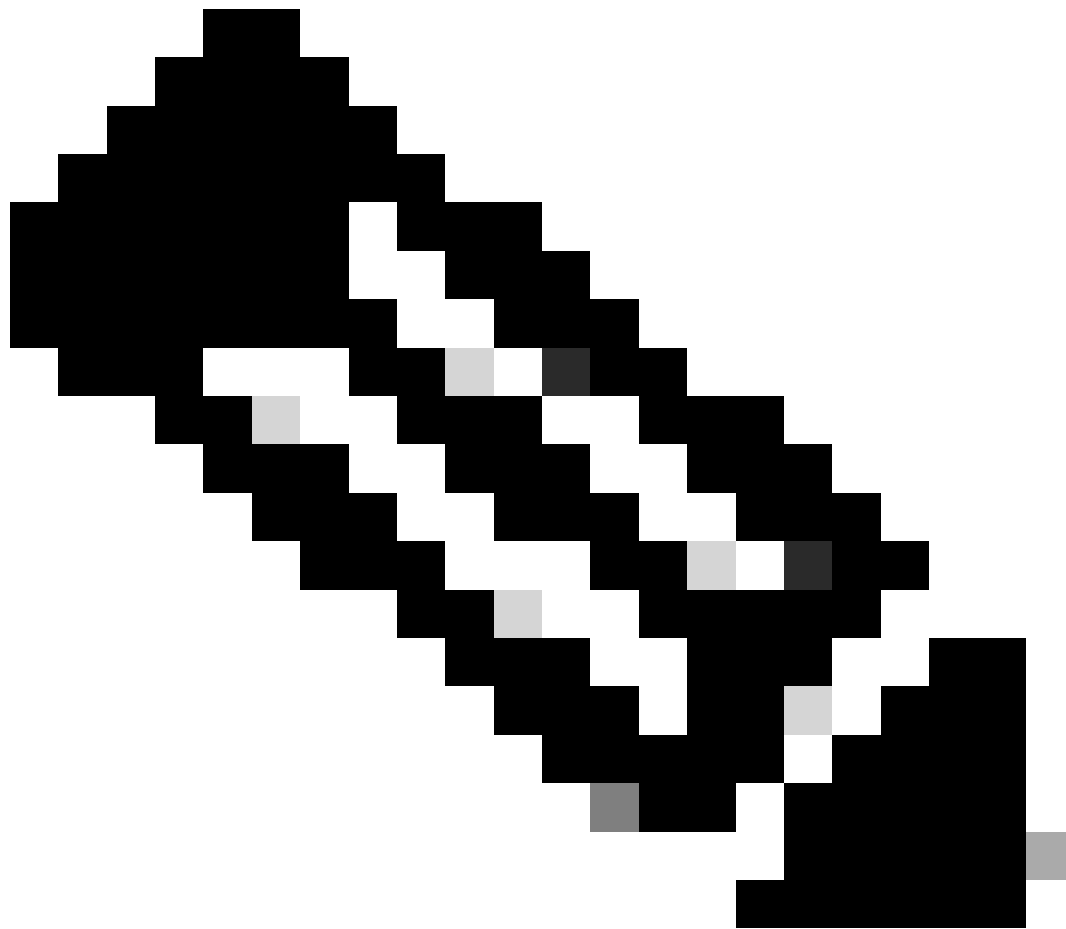
En général, les mêmes principes et configurations s'appliquent comme avec les exemples précédents. La principale différence dans ce cas est que la racine de l'arborescence de synchronisation est une source de temps privée plutôt qu'une source de temps publique provenant d'Internet. Cela modifie la conception du réseau de distribution du temps pour tirer parti de la source de temps privé de haute précision. La source temporelle privée est répartie sur l'ensemble du réseau privé selon les principes de hiérarchie et de modularité décrits dans les sections précédentes.

Low Stratum Campus  
Time Distribution Network



réseau de distribution du temps de campus à faible strate





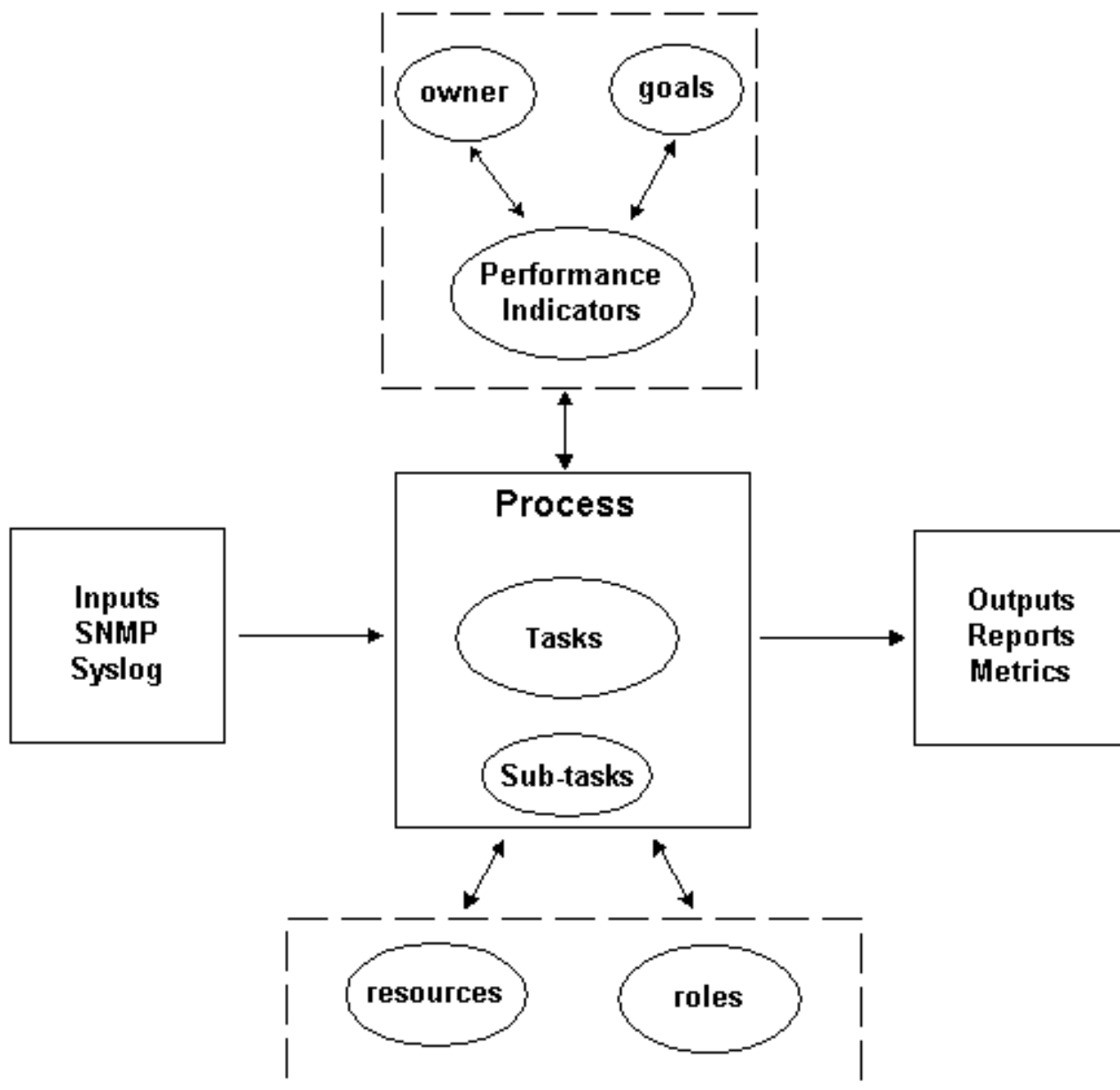
Remarque : un schéma intitulé Low Stratum Campus Time Distribution Network qui inclut une topologie générique à trois niveaux (backbone, distribution, accès). Deux commutateurs de distribution sont équipés d'horloges GPS ou au césium. Les commutateurs d'accès directement connectés à ces commutateurs de distribution et les commutateurs de réseau fédérateur sont des clients de ces commutateurs de distribution. Tous les autres commutateurs de distribution du réseau sont des clients des commutateurs de réseau fédérateur, et les autres commutateurs d'accès sont également des clients de leurs commutateurs de distribution directement connectés. Quatre commutateurs d'accès (en haut à gauche) sont représentés comme des clients de diffusion avec des flèches en pointillés, tandis que toutes les autres relations client-serveur et homologue-homologue ne sont pas de diffusion.

---

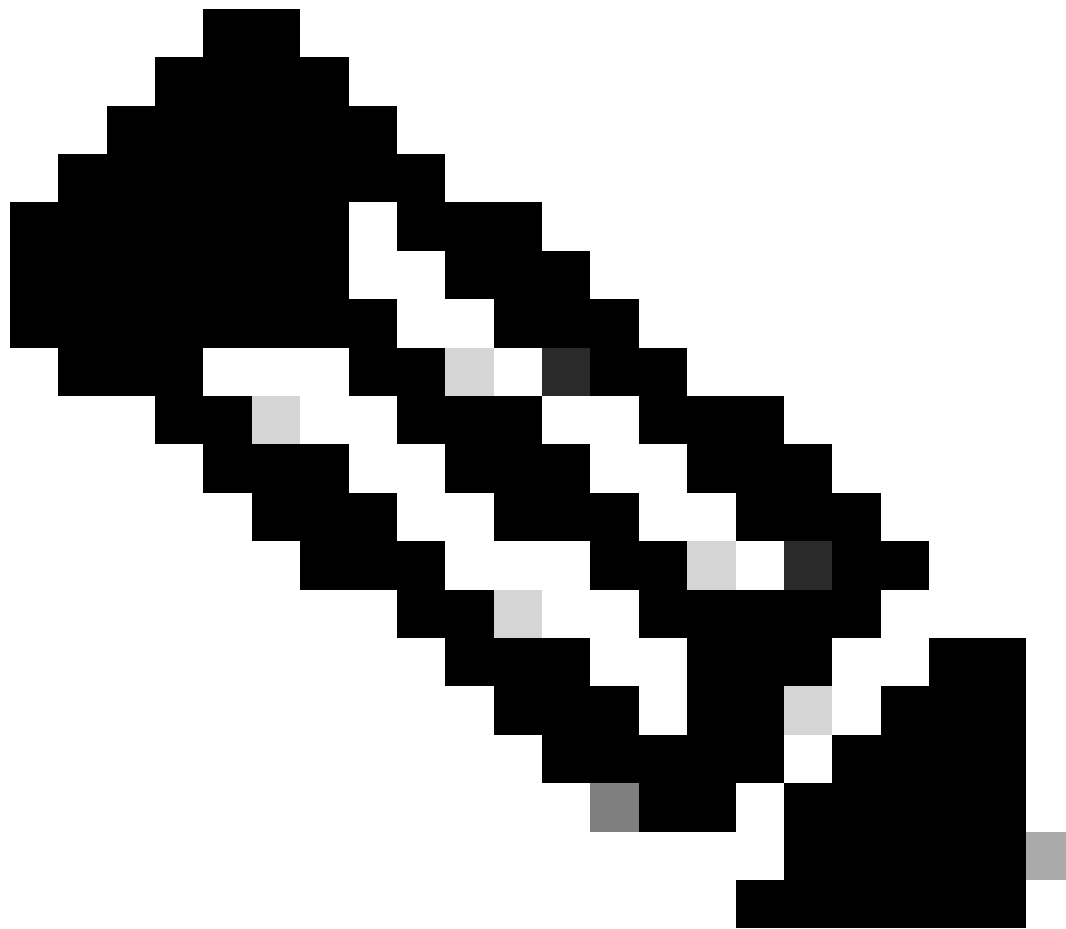
## Définitions de processus

Une définition de processus est une série d'actions, d'activités et de modifications liées effectuées par des agents qui ont l'intention de répondre à un objectif ou d'atteindre un objectif. Le contrôle

de processus est le processus de planification et de régulation, dont l'objectif est d'exécuter un processus de manière efficace et efficiente. Ceci est illustré dans le schéma suivant.



Série de processus



Remarque : Diagramme qui spécifie la signification d'un processus utilisé par ce document. Il y a cinq régions. La région gauche présente une bordure pleine. Il contient les entrées, SNMP et Syslog. Il y a une flèche à sens unique entre la région de gauche et la région centrale. La région de droite a également une frontière solide. Il contient les sorties, les rapports et la métrique. Il y a une flèche à sens unique entre la région centrale et la région droite. La région supérieure comporte une bordure en pointillés. Il contient le propriétaire, les objectifs et les indicateurs de performance. Il y a des cercles avec des bordures pleines autour des trois. Il existe des flèches bidirectionnelles entre (a) le propriétaire et les indicateurs de performance (b) les objectifs et les indicateurs de performance et (c) la région supérieure et la région centrale. La région inférieure présente également une bordure en pointillés. Il contient des ressources et des rôles. Il y a des cercles avec des bordures solides autour des deux. Il existe des flèches bidirectionnelles qui semblent relier les ressources et les rôles à la région centrale, mais elles s'arrêtent à la limite de la région inférieure. La zone centrale comporte une bordure pleine et un en-tête indiquant Processus. Il contient également une tâche et une sous-tâche. Chacune possède une bordure circulaire solide. Les tâches comportent plus d'espace vide à l'intérieur du cercle que tout autre élément du graphique.

---

Le résultat du processus doit être conforme aux normes opérationnelles définies par une organisation et basées sur des objectifs commerciaux. Si le processus est conforme à l'ensemble de normes, il est considéré comme efficace, car il peut être répété, mesuré, géré et contribue à la réalisation des objectifs de l'entreprise. Si les activités sont réalisées avec un minimum d'effort, le processus est également considéré comme efficace.

## Propriétaire du processus

Les processus s'étendent sur plusieurs frontières organisationnelles. Par conséquent, il est important d'avoir un seul propriétaire de processus qui est responsable de la définition du processus. Le propriétaire est le point central qui détermine et signale si le processus est efficace et efficient. Si le processus n'est pas efficace, le propriétaire du processus entraîne la modification du processus. La modification du processus est régie par des processus de contrôle des modifications et de révision.

## Objectifs du processus

Les objectifs du processus sont établis pour définir l'orientation et la portée de la définition du processus. Les objectifs sont également utilisés pour définir les mesures utilisées pour mesurer l'efficacité d'un processus.

L'objectif de ce processus est de fournir des critères à documenter pendant la phase de conception NTP, et de fournir une capacité d'audit pour une architecture NTP déployée afin de garantir la conformité à long terme avec la conception prévue.

## Indicateurs de performance des processus

Les indicateurs de performance des processus sont utilisés pour évaluer l'efficacité de la définition de processus. Les indicateurs de performance doivent être mesurables et quantifiables. Par exemple, les indicateurs de performance suivants sont soit numériques, soit mesurés dans le temps.

- Durée nécessaire pour effectuer un cycle de l'ensemble du processus.
- Fréquence d'exécution requise pour détecter de manière proactive les problèmes NTP avant qu'ils n'affectent les utilisateurs.
- Charge réseau associée à l'exécution du processus.
- Nombre de mesures correctives recommandées par le processus.
- Nombre de mesures correctives mises en oeuvre à la suite du processus.
- La durée nécessaire à la mise en oeuvre des actions correctives.
- L'arriéré des mesures correctives.
- Les erreurs de dépannage ou de diagnostic des problèmes attribuées aux problèmes liés au

protocole NTP.

- Nombre d'éléments ajoutés, supprimés ou modifiés dans le fichier de départ. Ceci est une indication de la précision et de la stabilité.

## Entrées de processus

Les entrées de processus permettent de définir les critères et les conditions préalables d'un processus. Souvent, l'identification des entrées de processus fournit des informations sur les dépendances externes. Une liste des entrées relatives à la gestion NTP est fournie ci-dessous.

- Documentation de conception NTP
- Données MIB NTP collectées par interrogation SNMP

## Sorties du processus

Les sorties de processus sont définies comme suit :

- Rapports de configuration NTP définis dans la section [Présentation des données](#) de ce document
- Actions correctives NTP

## Définitions des tâches

Les sections suivantes définissent les tâches d'initialisation et itératives associées à la gestion NTP.

### Tâches d'initialisation

Les tâches d'initialisation sont exécutées une seule fois au cours de l'implémentation du processus et ne doivent pas être exécutées à chaque itération du processus.

#### Création de la conception NTP

Lorsque vous vérifiez des tâches préalables, s'il est déterminé que l'une des tâches n'est pas implémentée ou ne fournit pas suffisamment d'informations pour répondre efficacement aux besoins de cette procédure, ce fait doit être documenté par le propriétaire du processus et soumis à la direction. Le tableau suivant présente les tâches d'initialisation requises.

Tâche prérequis	Description
Objectifs des tâches	Créez un document de conception détaillé pour l'architecture NTP qui répond aux exigences de conception et aux objectifs de coût.

Entrées de tâche	<ul style="list-style-type: none"> <li>• Exigences techniques et économiques de conception</li> <li>• Documentation de conception de réseau actuelle</li> <li>• Critères définissant les aspects requis à enregistrer dans la conception pour activer les fonctions de gestion</li> <li>• Informations de déploiement des applications informatiques</li> <li>• Exigences de surveillance des performances</li> </ul>
Sortie de tâche	Documentation de conception NTP.
Ressources de tâche	Architecte ingénieur réseau Architecte des opérations réseau.
Rôles des tâches	Approbation technique de la conception du réseau par les examinateurs de l'ingénierie et des opérations Coûts de conception du réseau approuvés par le responsable du budget.

### Créer un fichier d'amorçage

Le processus de gestion NTP nécessite l'utilisation d'un fichier d'amorçage pour supprimer le besoin d'une fonction de découverte de réseau. Le fichier d'amorçage enregistre l'ensemble des routeurs qui sont régis par le processus NTP et est également utilisé comme point central pour la coordination avec les processus de gestion du changement dans une organisation. Par exemple, si de nouveaux noeuds sont entrés dans le réseau, ils doivent être ajoutés au fichier de départ NTP. Si des modifications sont apportées aux noms de communauté SNMP en raison des exigences de sécurité, elles doivent être reflétées dans le fichier d'amorce. Le tableau suivant indique comment créer un fichier d'amorce.

Tâche prérequis	Description
Objectifs des tâches	<p>Créez un fichier d'amorçage qui identifie trois catégories de périphériques réseau :</p> <ol style="list-style-type: none"> <li>1. Périphériques critiques : interrogés fréquemment pour obtenir des informations sur la configuration</li> <li>2. Périphériques intéressants : interrogés moins fréquemment</li> <li>3. Tous les périphériques compatibles NTP : interrogés le moins possible</li> </ol>

Entrées de tâche	Documentation de conception NTP Documentation de topologie de réseau.
Sortie de tâche	Fichier d'amorçage.
Ressources de tâche	Critères de conception pouvant être utilisés pour identifier et hiérarchiser les noeuds impliqués dans l'architecture NTP.

### Paramètres de performances NTP de référence

Plusieurs des paramètres disponibles pour la surveillance du réseau NTP présentent des variations normales attendues. Le processus de planification initiale est utilisé pour caractériser les variations normales attendues et pour définir des seuils définissant des conditions inattendues ou anormales. Cette tâche permet de planifier l'ensemble variable de paramètres pour l'architecture NTP.

Process	Description
Objectifs des tâches	Paramètres de variable de ligne de base.
Entrées de tâche	Identifiez les paramètres variables cntpSysRootDelay cntpSysRootDispersion cntpPeersRootDelay cntpPeersRootDispersion cntpPeersOffset cntpPeersDelay cntpPeersDispersion.
Sorties des tâches	Valeurs et seuils de référence.
Ressources de tâche	Outils qui collectent les données SNMP et calculent les lignes de base.
Rôle de tâche	Ingénieur réseau Ingénieur NMS.

### Tâches itératives

Des tâches itératives sont exécutées au cours de chaque itération du processus et leur fréquence est déterminée et modifiée afin d'améliorer les indicateurs de performance.

#### Tenir à jour le fichier de démarrage

Le fichier de départ est essentiel à la mise en oeuvre efficace du processus de gestion NTP. Par conséquent, l'état actuel du fichier de départ doit être géré activement. Les modifications

apportées au réseau qui ont un impact sur le contenu du fichier de départ doivent être suivies par le propriétaire du processus de gestion NTP.

Process	Description
Objectifs des tâches	Maintenir l'exactitude du fichier de départ
Entrées de tâche	Informations sur les modifications du réseau
Sorties des tâches	Fichier d'amorçage
Ressources de tâche	Rapports, notifications, réunions concernant des modifications
Rôle de tâche	Ingénieur réseau Ingénieur NMS

#### Exécuter l'analyse du noeud NTP

Collecter des informations sur les analyses critiques, intéressantes et de configuration définies par cette procédure. Exécutez ces trois balayages à différentes fréquences.

Les noeuds critiques sont des périphériques considérés comme très importants pour les points de données de collecte des performances. L'analyse du noeud critique est exécutée souvent, par exemple, toutes les heures ou à la demande, avant et après les modifications. Les noeuds intéressants sont des périphériques jugés importants pour l'intégrité globale de l'architecture NTP, mais qui ne peuvent pas figurer dans l'arborescence de synchronisation temporelle pour la collecte de données de performances critiques. Ce rapport est exécuté périodiquement, par exemple, quotidiennement ou mensuellement. Le rapport de configuration est un rapport complet et riche en ressources qui est utilisé pour caractériser la configuration de déploiement NTP globale par rapport aux enregistrements de conception. Ce rapport est exécuté moins fréquemment, par exemple, mensuellement ou trimestriellement. Il est important de tenir compte du fait que la fréquence de collecte des rapports peut être ajustée en fonction de la stabilité observée de l'architecture NTP et des besoins de l'entreprise.

Process	Description
Objectif de tâche	Surveiller l'architecture NTP
Entrée de tâche	Données des périphériques réseau
Sortie de tâche	Rapports
Ressources de tâche	Applications logicielles pour collecter des données et produire des rapports
Rôle de tâche	Ingénieur réseau

#### Examiner les rapports de noeud NTP

Cette tâche nécessite que les rapports critiques, intéressants et de configuration soient examinés et analysés. Si des problèmes sont détectés, des actions correctives doivent être entreprises.

Process	Description
Entrées de tâche	Analyser les rapports
Sorties des tâches	Analyse de stabilité Mesures correctives
Ressources de tâche	Accès aux périphériques réseau pour une étude et une vérification plus poussées



Rôle de tâche	Ingénieur réseau
---------------	------------------

## Identification des données

### Caractéristiques générales des données

Le tableau suivant décrit les données considérées comme importantes lors de l'analyse de l'architecture NTP.

Données	Description
ID de noeud	Périphérique dont le protocole NTP est configuré
Pairs	Les homologues configurés pour le périphérique
Source de synchronisation	Homologue sélectionné pour la synchronisation
Données de configuration NTP	Paramètres utilisés pour évaluer la cohérence de la conception NTP
Données de qualité NTP	Paramètres utilisés pour caractériser la qualité des associations NTP

### Identification des données SNMP

#### Groupe de systèmes Cisco NTP MIB

Les données SNMP NTP sont définies par la base de données MIB Cisco-NTP. Pour obtenir des informations à jour sur les versions qui prennent en charge cette base de données MIB, utilisez l'outil de navigation des fonctions CCO et sélectionnez l'option de localisation MIB. Cet outil est accessible via la page TAC Tools for Voice, Telephony and Messaging Technologies.

Le groupe système de la [MIB Cisco NTP](#) fournit des informations pour le noeud cible qui exécute NTP. Le noeud cible est la destination des requêtes SNMP.

Nom d'objet	Description d'objet
cntpSysStratum	La strate de l'horloge locale. Si la valeur est définie sur 1, une référence principale, alors la procédure d'horloge principale décrite dans Section 3.4.6, dans <a href="#">RFC-1305</a> est appelé. ::= { cntpSystem 2 } object identifier = .1.3.6.1.4.1.9.9.168.1.1.2
cntpSysPrecision	Entier signé qui indique la précision de l'horloge système, en secondes, à la puissance deux la plus proche. La valeur doit être arrondie à la puissance supérieure de deux suivante. Par exemple, une horloge de fréquence de puissance de 50 Hz (20 ms) ou 60 Hz (16,67 ms) reçoit la valeur -5 (31,25 ms), tandis qu'une horloge commandée par quartz de 1000 Hz (1 ms) reçoit la valeur -9 (1,95 ms). ::= { cntpSystem 3 } object identifier = .1.3.6.1.4.1.9.9.168.1.1.3
cntpSysRootDelay	Nombre à virgule fixe signé qui indique le délai d'aller-retour total en secondes à la source de référence principale à la racine du sous-réseau de synchronisation. ::= { cntpSystem 4 } object identifier =

	.1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRootDispersion	Erreur maximale en secondes, relative à la source de référence principale à la racine du sous-réseau de synchronisation. Seules les valeurs positives supérieures à zéro sont possibles. ::= { cntpSystem 5 } object identifier = .1.3.6.1.4.1.9.9.168.1.1.4
cntpSysRefTime	Heure locale de la dernière mise à jour de l'horloge locale. Si l'horloge locale n'a jamais été synchronisée, la valeur est zéro. ::= { cntpSystem 7 } object identifier = .1.3.6.1.4.1.9.9.168.1.1.7
cntpSysPeer	Source de synchronisation actuelle qui contient l'identificateur d'association unique cntpPeersAssocId de l'entrée homologue correspondante dans la table cntpPeersVarTable de l'homologue agissant comme source de synchronisation. S'il n'y a pas d'homologue, la valeur est zéro. ::= { cntpSystem 9 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.1.9
cntpSysClock	Heure locale actuelle. L'heure locale est dérivée de l'horloge matérielle de la machine particulière et s'incrémente à intervalles réguliers en fonction de la conception utilisée. ::= { cntpSystem 10 } object identifier = .1.3.6.1.4.1.9.9.168.1.1.10

#### Groupe d'homologues Cisco NTP MIB - Tableau des variables d'homologues

Le groupe d'homologues de la base de données MIB Cisco NTP fournit des informations sur les homologues du noeud cible.

Nom d'objet	Description d'objet
cntpPeersTableVar	Ce tableau fournit des informations sur les homologues avec lesquels le serveur NTP local a des associations. Les homologues sont également des serveurs NTP qui s'exécutent sur différents hôtes. Voici une table de cntpPeersVarEntry ::= { cntpPeers 1 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1
cntpPeerVarEntry	Chaque entrée d'homologue fournit des informations NTP récupérées à partir d'un serveur NTP homologue particulier. Chaque homologue est identifié par un identificateur d'association unique. Les entrées sont automatiquement créées lorsque l'utilisateur configure le serveur NTP pour qu'il soit associé à des homologues distants. De même, les entrées sont supprimées lorsque l'utilisateur supprime l'association d'homologues du serveur NTP. Les entrées peuvent également être créées par la station de gestion en définissant des valeurs pour cntpPeersPeerAddress, cntpPeersHostAddress et cntpPeersMode et en définissant cntpPeersEntryStatus comme étant actif (1). Au minimum, la station de gestion doit définir une valeur pour cntpPeerPeerAddress pour rendre la ligne active. INDEX { cntpPeersAssocId } ::= { cntpPeersVarTable 1 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1

cntpPeersAssocId	Valeur entière supérieure à zéro qui identifie de manière unique un homologue auquel le serveur NTP local est associé. ::= { cntpPeersVarEntry 1 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.1
cntpHomologuesConfigurés	Il s'agit d'un bit qui indique que l'association a été créée à partir des informations de configuration et ne doit pas être dissociée même si l'homologue devient inaccessible. ::= { cntpPeersVarEntry 2 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.2
cntpPeerAddress	Adresse IP de l'homologue. Lorsqu'une nouvelle association est créée, une valeur pour cet objet doit être définie avant que la ligne soit activée. ::= { cntpPeersVarEntry 3 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.3
cntpPeersMode	SYNTAXE INTEGER { unspecified (0), symmetricActive (1), symmetricPassive (2), client (3), server (4), broadcast (5), reservedControl (6), reservedPrivate (7) } Lorsqu'une nouvelle association d'homologues est créée, si aucune valeur n'est spécifiée pour cet objet, elle prend par défaut la valeur symmetricActive (1). ::= { cntpPeersVarEntry 8 } object identifier = .1.3.6.1.4.1.9.9.168.1.2.1.1.8
cntpPeersStratum	La strate de l'horloge homologue. ::= { cntpPeersVarEntry 9 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.9
cntpHomologuesDélaiRacine	Nombre à virgule fixe signé qui indique le délai d'aller-retour total en secondes, de l'homologue à la source de référence principale à la racine du sous-réseau de synchronisation. ::= { cntpPeersVarEntry 13 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.13
cntpHomologuesDispersionRacine	Erreur maximale, en secondes, de l'horloge homologue par rapport à la source de référence principale à la racine du sous-réseau de synchronisation. Seules les valeurs positives supérieures à zéro sont possibles. ::= { cntpPeersVarEntry 14 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.14
cntpPeersRefTime	Heure locale de l'homologue lors de la dernière mise à jour de son horloge. Si l'horloge homologue n'a jamais été synchronisée, la valeur est zéro. ::= { cntpPeersVarEntry 16 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.16
cntpPeerReach	Registre à décalage utilisé pour déterminer l'état d'accessibilité de l'homologue, avec des bits qui entrent depuis l'extrémité la moins significative (la plus à droite). Un homologue est considéré comme accessible si au moins un bit de ce registre est défini sur un (l'objet est différent de zéro). Les données du registre à décalage sont renseignées par les procédures du protocole NTP. ::= { cntpPeersVarEntry 21 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpHomologuesDécalage	Décalage estimé de l'horloge homologue par rapport à l'horloge locale, en secondes. L'hôte détermine la valeur de

	cet objet qui utilise l'algorithme de filtre d'horloge NTP. ::= { cntpPeersVarEntry 23 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.21
cntpPeersDelay	Délai d'aller-retour estimé de l'horloge homologue par rapport à l'horloge locale sur le chemin réseau entre elles, en secondes. L'hôte détermine la valeur de cet objet qui utilise l'algorithme de filtre d'horloge NTP. ::= { cntpPeersVarEntry 24 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.24
cntpPeerDispersion	Erreur maximale estimée de l'horloge homologue par rapport à l'horloge locale sur le chemin réseau entre elles, en secondes. L'hôte détermine la valeur de cet objet qui utilise l'algorithme de filtre d'horloge NTP. ::= { cntpPeersVarEntry 25 } identificateur d'objet = .1.3.6.1.4.1.9.9.168.1.2.1.1.25

## Collecte de données

### Collecte de données SNMP

Toutes les informations requises par cette procédure peuvent être collectées par le biais de requêtes SNMP. Afin d'analyser les données et de produire les rapports, des scripts personnalisés ou des programmes logiciels doivent être développés.

## Présentation des données

### Rapport de noeud critique NTP

Les noeuds critiques sont des périphériques importants dans l'arborescence de synchronisation des points de collecte de données de performances sélectionnés. Si un service VoIP à revenu élevé est surveillé et que des mesures de variation de délai unidirectionnel sont collectées, les noeuds source et de destination où les horodatages sont enregistrés sont considérés comme des noeuds critiques.

Dans cet exemple, la conception NTP a été établie à la suite d'un exemple de hiérarchie OSPF. Par conséquent, les rapports décrits ci-dessous sont formatés pour regrouper les périphériques NTP par la zone OSPF du périphérique. Dans les cas où un noeud possède des interfaces dans plusieurs zones, le logiciel de génération de rapports doit décider quelle zone le noeud peut être répertoriée à des fins de rapport. Comme mentionné précédemment, OSPF n'est pas une condition préalable pour NTP. Il n'est utilisé dans ce document qu'à titre d'exemple.

Zone	Périphérique	Données des périphériques	Valeur
ID zone #n	ID de périphérique #1	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysRefTime	
		cntpSysPeer	

		cntpSysClock	
	ID de périphérique #n	cntpSysStratum	
		cntpSysPrecision	
		cntpSysRootDelay	
		cntpSysRootDispersion	
		cntpSysRefTime	
		cntpSysPeer	
		cntpSysClock	

## Rapport NTP sur les noeuds intéressants

Le format du rapport de noeud intéressant est le même que celui du rapport de noeud critique. Les noeuds intéressants sont considérés comme importants pour l'architecture NTP globale, mais ne peuvent pas contribuer directement à la synchronisation temporelle des points critiques de surveillance des performances.

## Rapport de configuration NTP

Le rapport de configuration est un rapport complet qui collecte des informations sur l'architecture NTP globale. Ce rapport est utilisé pour enregistrer et vérifier le déploiement NTP par rapport aux enregistrements de conception.

Zone	Périphérique	Pair	Données homologues	Valeur
ID zone #n	ID de périphérique #n	PeerId #1	cntpPeersAssocId	
			cntpHomologuesConfigurés	
			cntpPeerAddress	
			cntpPeersMode	
			cntpPeersStratum	
			cntpHomologuesDélaiRacine	
			cntpHomologuesDispersionRacine	
			cntpPeersRefTime	
			cntpPeerReach	
			cntpHomologuesDécalage	
			cntpPeersDelay	
			cntpPeerDispersion	
		PeerId #n	cntpPeersAssocId	
			cntpHomologuesConfigurés	
			cntpPeerAddress	
			cntpPeersMode	
			cntpPeersStratum	
			cntpHomologuesDélaiRacine	
			cntpHomologuesDispersionRacine	
			cntpPeersRefTime	
cntpPeerReach				

			cntpHomologuesDécalage	
			cntpPeersDelay	
			cntpPeerDispersion	

## Informations connexes

- [Protocole RFC 1305 \(Network Time Protocol\)](#)
- [Cadre RFC 2330 pour les mesures de performances IP](#)
- [Fonctionnalités essentielles de Cisco IOS Chaque FAI doit prendre en compte la version 2.84](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.