*BULLETIN OFFICIEL DES ARMEES*

**Edition Chronologique n°17 du 13 avril 2012**

PARTIE PERMANENTE
Administration Centrale

Texte n°4

**DIRECTIVE N° 24/DEF/DGSIC**
portant sur le service de synchronisation horaire au standard internet protocol.

Du *9 mars 2012*

D I R E C T I O N G É N É R A L E D E S S Y S T È M E S D ' I N F O R M A T I O N E T D E COMMUNICATION : *sous-direction de l'ingénierie des systèmes d'information.*

**DIRECTIVE N° 24/DEF/DGSIC portant sur le service de synchronisation horaire au standard internet protocol.**

*Du 9 mars 2012*

NOR D E F E 1 2 5 0 3 4 6 X

---

*Pièce(s) Jointe(s) :*

Une annexe.

*Classement dans l'édition méthodique :* BOEM 160.1

*Référence de publication :* BOC N°17 du 13 avril 2012, texte 4.

---

SOMMAIRE

## 1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

### 1.1. **Présentation.**

La présente directive définit les règles d'usage et de mise en œuvre de la synchronisation horaire des réseaux intranets au standard internet protocol (IP) du ministère de la défense.

Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

Cette directive s'inspire du référentiel général d'intéropérabilité (RGI) et du référentiel général de sécurité (RGS) prescrits par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

1.2. **Niveaux de préconisation.**

Les règles présentées dans ce document ont différents niveaux de préconisation et sont conformes au RGI et à la *request for comments* (RFC) 2119 :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Gestion du document.**

Ce document est maintenu et mis à jour par le sous-comité architecture et services du comité directeur des intranets. Les modifications sont soumises pour approbation au directeur général des systèmes d'information et de communication.

Ce document est disponible sur le site DGSIC.

1.4. **Modalités d'application.**

La présente directive s'applique à l'ensemble des intranets utilisés par le ministère de la défense, quel que soit leur niveau de classification. Elle concerne la fourniture du service de synchronisation horaire à l'ensemble des composants des intranets (équipements réseaux, équipements de sécurité, serveurs, postes clients), ainsi qu'aux applications de services communs et métiers.

Ces règles définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure concernant les intranets au standard IP du ministère de la défense.

Les directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics des systèmes fournissant ou utilisant le service de synchronisation horaire.

1.5. **Gestion des dérogations pour les projets.**

Les dérogations sont présentées par un expert de haut niveau ou un directeur de projet au sous-comité architecture et services (SC2) qui statue sur la demande.

La commission ministérielle technique des systèmes d'information et de communication (CMTSIC) peut également être saisie en dernier ressort. Ces dérogations font l'objet d'une approbation par le directeur général des systèmes d'information et de communication. Elles concernent :

- les circonstances et justifications du non respect d'une règle recommandée ;

- les circonstances et justifications du non respect d'une règle déconseillée ;

- les justifications des exceptions à toute règle absolue (obligatoire ou interdit). Dans ce dernier cas, une instruction préalable des services de la DGSIC est nécessaire.

## 2. CADRE DOCUMENTAIRE.

### 2.1. **Documents applicables.**

RGI : référentiel général d'interopérabilité version 1.0 du 12 mai 2009.

RGS : référentiel général de sécurité version 1.0 du 6 mai 2010.

### 2.2. **Normes et standards applicables.**

RFC 867 : *day time protocol* (*standard may 1983*).

RFC 868 : *time protocol* (*standard may 1983*).

RFC 1129 : *internet time synchronisation, the network time protocol* (*informational october 1989*).

RFC 2119 : *key words for use in RFCs to indicate requirement levels* (*best current practice march 1997*).

RFC 5905 : *network time protocol* (NTP) *version 4, protocol and algorithms specification* (*proposed standard june 2010*).

RFC 5906 : NTP *version 4, autokey specifications* (*informational june 2010*).

RFC 5907 : *definition of managed objects for network time protocol version 4* (*proposed standard june 2010*).

RFC 5908 : NTP *server option for dynamic host configuration protocol version 6* (DHCPv6) (*proposed standard june 2010*).

### 2.3. **Autres documents et sites de référence.**

Site DGSIC : site intranet défense DGSIC (www.dgsic.defense.gouv.fr).

NTP référence : www.ntp.org.

NTP référence Windows : www.meinberg.de.

## 3. DOMAINE COUVERT ET EMPLOI.

### 3.1. **Services attendus du système.**

Le système de synchronisation horaire a pour objectif de fournir une heure de référence, robuste fiable et universelle à l'ensemble des composants constituant les intranets (équipements réseaux, serveurs, postes de travail, chiffreurs, garde-barrières, sondes, etc.), ainsi qu'aux applications de services communs et métiers.

### 3.2. **Principes généraux.**

Cette directive s'applique indifféremment aux systèmes d'information d'administration et de gestion (SIAG), systèmes d'information opérationnel et de commandement (SIOC) et systèmes d'information scientifique et technique (SIST) et à tous les éléments constituant un intranet.

Un système de synchronisation horaire doit être déployé par intranet de niveau de confidentialité différent et doit prendre ses références sur les mêmes serveurs de temps de strate 0 s'ils ne sont pas confondus avec les serveurs de strate 1 (horloges atomiques mutualisées).

L'architecture de référence se limite à quatre strates logiques ; chacune des strates ayant un rôle bien défini. Les règles de la directive sont établies dans la logique de ces quatre strates et des rôles qui leurs sont dévolus :

- la strate 4 correspond aux postes terminaux ;

- la strate 3 correspond à la couche de distribution de l'heure aux postes terminaux. Elle peut-être constituée d'équipements réseaux (routeurs et commutateurs niveaux trois), *firewall*, sonde de détection d'intrusion, serveur *ActiveDirectory* (AD), boitier ntp, etc. ;

- les strates 1 et 2 constituent le noyau de confiance de l'heure, cette couche dispose d'un haut niveau de sécurité. C'est sur ce noyau que l'ensemble des éléments constituant l'architecture de l'intranet (équipements réseaux, serveurs communs, serveurs d'application métier, chiffreurs, pare-feux, sondes, etc.) hors postes terminaux doivent se synchroniser.

L'implémentation physique peut éventuellement être adaptée en fonction du contexte et de la charge ; ainsi la strate de niveau 2 peut évoluer :

- à la hausse pour des raisons de segmentations réseau, et être étoffée de strates complémentaires 2', 2", etc. qui doivent respecter les règles de la strate 2 ;

- à la baisse, dans la mesure ou le nombre de dispositifs à synchroniser est faible, la suppression de la strate 2 peut alors être envisagée sous réserve que les serveurs de la strate 1 puissent tenir la charge.

Le nombre de serveurs de strate 1, 2 et 3 sera adapté à la volumétrie des éléments constituant l'intranet.

Les systèmes autonomes ne bénéficiant pas d'un accès réseau permanent et/ou de débit suffisant sont exclus du périmètre de la directive.

Le schéma de principe suivant illustre ces différents points.

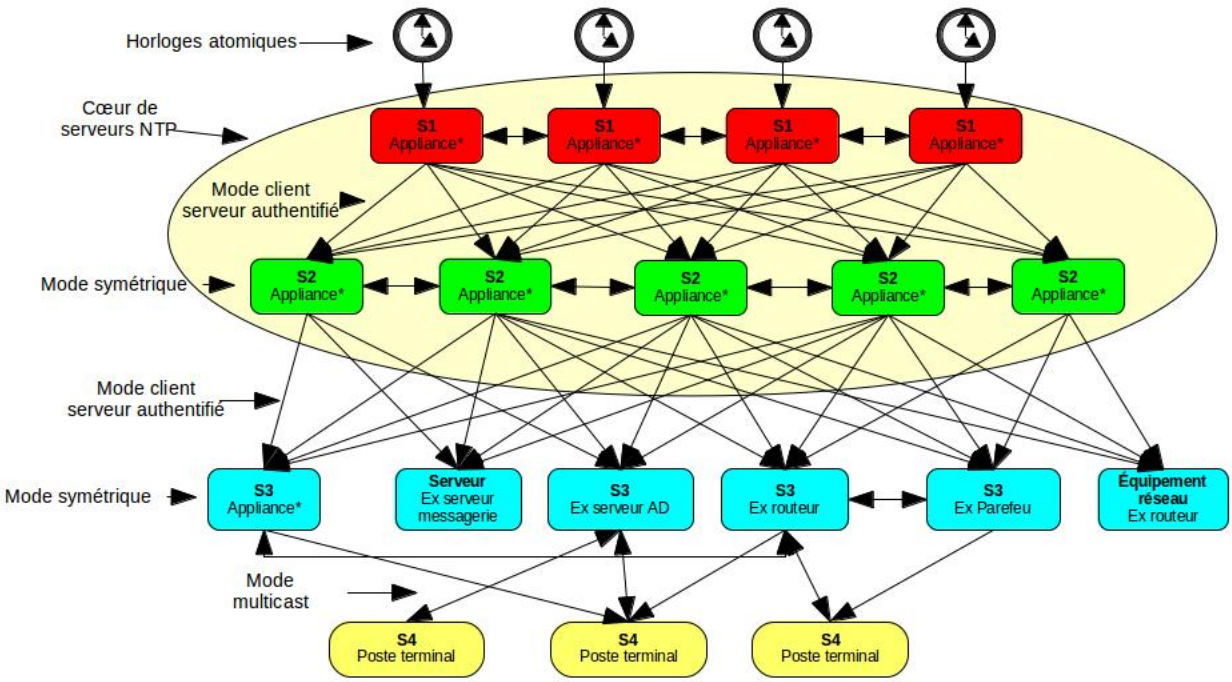


Schéma de principe de l'architecture de synchronisation horaire.

4. LES RÈGLES.

4.1. **Règles techniques.**

*4.1.1.* ***Généralités.***

RT 01 : il est obligatoire d'utiliser le protocole NTP dans sa version supérieure ou égale à trois pour synchroniser les intranets au standard IP du ministère de la défense.

RT 02 : il est recommandé d'utiliser le protocole NTP dans sa version 4 pour synchroniser les intranets au standard IP du ministère de la défense.

RT 03 : il est obligatoire que les serveurs de temps utilisent le protocole NTP.

RT 04 : il est obligatoire d'utiliser le protocole *user datagram protocol* (UDP) pour synchroniser les serveurs NTP entre eux.

RT 05 : il est obligatoire d'utiliser le temps universel coordonné (UTC ou TUC).

*4.1.2.* ***D'architecture.***

*4.1.2.1. Généralités.*

RTA 01 : il est recommandé que l'architecture de distribution horaire ne dépasse pas quatre niveaux (S1 à S4).

RTA 02 : il est obligatoire que les serveurs de strates 1 et 2 soient des serveurs dédiés au protocole NTP.

RTA 03 : il est interdit d'utiliser l'horloge virtualisée d'un serveur pour le service NTP.

RTA 04 : il est obligatoire que tous les équipements composant l'intranet, hors postes terminaux, supportent la synchronisation avec un serveur NTP en mode client/serveur.

RTA 05 : il est recommandé que le logiciel client/serveur NTP utilisé par les postes terminaux et les serveurs soit celui fournit par NTP référence.

*4.1.2.2. Strate 0 (horloge atomique).*

RTA 11 : il est obligatoire que la strate 0 soit un équipement dont la précision est garantie par une horloge atomique.

RTA 12 : il est obligatoire que les équipements de strate 0 disposent d'une sortie horaire au protocole *inter-range instrumentation group time codes* (IRIG) B.

RTA 13 : il est recommandé que les équipements de strate 0 disposent d'une sortie horaire au protocole *standardization agreements* (STANAG) 4430.

*4.1.2.3. Strate 1 (noyau network time protocol fournit l'heure à la strate 2 ou assure son rôle).*

RTA 21 : il est obligatoire que les équipements de strate 1 supportent le protocole IRIG B comme référence de synchronisation de strate 0.

RTA 22 : il est recommandé que les équipements de strate 1 supportent le STANAG 4430 comme référence de synchronisation de strate 0.

RTA 23 : il est obligatoire qu'un serveur de strate 1 soit asservi à un équipement de strate 0.

Les équipements de strate 0 et 1 peuvent être confondus dans la mesure où les serveurs de strate 1 disposent d'une horloge atomique et d'au moins une référence extérieure précise comme le *global positioning system* (GPS) ou Galiléo. Dans ce cas, les règles RTA 12, 13, 21 et 22 ne s 'appliquent plus.

RTA 24 : il est obligatoire de disposer d'au moins 4 serveurs de strate 1.

2n + 1 serveurs de strate 1 permettent d'assurer de garantir la précision horaire même si n serveurs sont défaillants ou indisponibles. Cette règle n'est valable que pour n>= 2 ; il faut 4 serveurs pour résister à la perte d'un serveur tout en garantissant la précision horaire :

- 3 serveurs permettent d'assurer la précision horaire et aucune panne de serveur ;

- 4 serveurs autorisent la perte d'un serveur (panne, maintenance, etc.) ;

- 5 serveurs autorisent la perte de 2 serveurs ;

- 7 serveurs autorisent la perte de 3 serveurs, etc. ;

- 2n + 1 serveurs autorisent la perte de n serveurs.

*4.1.2.4. Strate 2 (noyau network time protocol distribution de l'heure aux équipements constituant l'intranet hors postes terminaux).*

RTA 31 : il est obligatoire que les serveurs NTP de strate 2 se synchronisent sur les serveurs NTP de strate 1 en mode client/serveur.

RTA 32 : il est obligatoire qu'un serveur de strate 2 se synchronise sur au moins quatre serveurs de strate 1.

RTA 33 : il est obligatoire que les serveurs NTP de strate 2 se synchronisent, entre eux, en mode symétrique.

RTA 34 : il est obligatoire que les serveurs NTP de strate 2 se synchronisent à un minimum de deux serveurs NTP de même niveau.

*4.1.2.5. Strate 3 (distribution de l'heure aux postes terminaux).*

RTA 41 : il est obligatoire que les serveurs NTP de strate 3 se synchronisent sur les serveurs NTP de strate 2 en mode client/serveur.

RTA 42 : il est obligatoire qu'un serveur de strate 3 se synchronise sur au moins quatre serveurs de strate 2.

RTA 43 : il est obligatoire que tous les équipements composant l'intranet, hors postes terminaux se synchronisent sur au moins un serveur NTP de strate 2 en mode client/serveur.

RTA 44 : il est recommandé que tous les équipements composant l'intranet, hors postes terminaux se synchronisent sur au moins quatre serveurs NTP de strate 2 en mode client/serveur.

RTA 45 : il est recommandé que les équipements composant l'intranet, hors postes terminaux, et compatibles NTP, soient configurés et utilisés comme serveurs NTP de strate 3.

RTA 46 : il est recommandé que les serveurs NTP de strate 3 se synchronisent, entre eux, en mode symétrique à un minimum de deux serveurs NTP de même niveau.

*4.1.2.6. Strate 4 (postes terminaux).*

RTA 51 : il est obligatoire que les postes terminaux se synchronisent sur au moins un serveur de strate 3.

RTA 52 : il est recommandé que les postes terminaux se synchronisent sur au moins quatre serveurs de strate 3.

RTA 53 : il est recommandé que les postes terminaux se synchronisent en utilisant le protocole NTP en mode multicast.

*4.1.3.* ***De sécurité.***

*4.1.3.1. Généralités.*

RTS 01 : il est obligatoire que tous les équipements composant l'intranet, hors postes terminaux, supportent la synchronisation avec un serveur NTP en mode authentifié *message digest* (MD) 5.

RTS 02 : il est recommandé que tous les équipements composant l'intranet, hors postes terminaux supportent la synchronisation avec un serveur NTP en mode authentifié protocole *autokey*.

RTS 03 : il est obligatoire que les serveurs de temps de strate 1 et 2 soient monitorés.

RTS 04 : il est obligatoire de se conformer au RGS pour la longueur des clefs utilisées en protocole *autokey* schéma *identification, friend or foe* (IFF).

*4.1.3.2. Strate 0 (horloge atomique).*

Sans objet.

*4.1.3.3. Strate 1 (noyau network time protocol : fournit l'heure à la strate 2 ou assure son rôle).*

RTS 21 : il est obligatoire que les serveurs NTP de strate 1 supportent la synchronisation *via* le protocole *autokey*.

RTS 22 : il est obligatoire que l'accès aux serveurs NTP de strate 1 soit limité aux serveurs NTP de strate 2.

*4.1.3.4. Strate 2 (noyau network time protocol : distribution de l'heure aux équipements constituant l'intranet hors postes terminaux).*

RTS 31 : il est obligatoire que les serveurs NTP de strate 2 se synchronisent en mode authentifié protocole *autokey* schéma IFF.

RTS 32 : il est obligatoire que tous les équipements composant l'intranet, hors postes terminaux se synchronisent sur les serveur NTP de strate 2 en mode authentifié MD5 ou protocole *autokey*.

*4.1.3.5. Strate 3 (distribution de l'heure aux postes terminaux).*

RTS 41 : il est obligatoire que les serveurs NTP de strate 3 se synchronisent en mode authentifié protocole *autokey* schéma IFF, à défaut MD5.

*4.1.3.6. Strate 4 (postes terminaux).*

RTS 51 : il est recommandé que les postes terminaux se synchronisent en utilisant le protocole NTP en mode authentifié protocole *autokey* à défaut MD5.

4.2. **Cas de l'internet.**

RT 11 : il est obligatoire que les machines constituant le réseau internet utilisé au sein du ministère de la défense se synchronisent sur les serveurs mis à disposition par l'internet.

4.3. **Règles organisationnelles.**

Sans objet.

4.4. **Règles sémantiques.**

Sans objet.

Pour le ministre de la défense et des anciens combattants et par délégation :

*L'amiral,*
*directeur général des systèmes d'information et de communication,*

Christian PÉNILLARD.

ANNEXE.

## GLOSSAIRE ET ACRONYMES.

| ACRONYME. | DÉFINITION. |
|---|---|
| CMTSIC | Commission ministérielle technique des systèmes d'information et de communication. |
| CMSSI | Commission ministérielle de la sécurité des systèmes d'information. |
| CUT | *Coordinated universal time* voir UTC (temps universel coordonné). |
| DGSIC | Direction générale des systèmes d'information et de communication. |
| GPS | *Global positioning system*. |
| IETF | *Internet engineering task force*. |
| IP | *Internet protocol*. |
| IRIG | *Inter-range instrumentation group time codes*. |
| MD | *Message digest*. |
| NTP | *Network time protocol*. |
| RFC | *Request for comment*. |
| RGI | Référentiel général d'interopérabilité. |
| RGS | Référentiel général de sécurité. |
| SIAG | Système d'information d'administration et de gestion. |
| SIOC | Système d'information opérationnel et de commandement. |
| SIST | Système d'information scientifique et technique. |
| SNTP | *Simple network time protocol*. |
| TCP | *Transmission control protocol*. |
| UDP | *User datagram protocol*. |
| TUC | Temps universel coordonné. |

| TERME. | DÉFINITION. |
|---|---|
| Appliance. | Boitier spécialisé. |
| Galiléo. | Système de positionnement européen similaire au GPS. |
| IFF. | Voir mode authentifié protocole *autokey* schéma *identification, friend or foe* (IFF). |
| IRIG B. | Standard de format de codage de temps élaboré par *l'inter-range instrumentation group* et repris par l'AFNOR sous la référence NFS 87.500. |
| MD5. | *Message digest* 5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier. |
| Mode authentifié protocole *autokey*. | Mode de sécurisation du protocole NTP reposant sur la cryptographie à clef publique apparue avec la version 4 du protocole NTP. Seuls les serveurs de strate signent leurs réponses, les clients connaissant la clef publique des serveurs peuvent vérifier leurs réponses. Seuls les serveurs nécessitent l'installation d'une clef. |
| Mode authentifié protocole *autokey* schéma IFF. | Mise en œuvre du mode authentifié protocole *autokey* et de groupes (ensemble de clients et de serveurs NTP regroupés au sein d'un même espace cryptographique).<br><br>IFF : *identification, friend or foe* (identification ami ou ennemi). |
| Mode authentifié MD5. | Mode de sécurisation du protocole NTP reposant sur la cryptographie à secret partagé. Les paquets sont signés par un secret partagé et l'utilisation de l'algorithme MD5. |
| Monitorer un serveur NTP. | Opération qui consiste à :<br><br>- savoir si le programme résident « ntpd » est présent ou non en mémoire ; |

| | |
|---|---|
| | - prendre connaissance de l'état du serveur vis-à-vis du NTP et plus particulièrement des valeurs suivantes :<br><br>- *jitter* : correspond à une moyenne qui indique combien de pulsations (PPS) varient de seconde en seconde. Les bonnes valeurs sont de l'ordre de la micro secondes. Des valeurs de l'ordre de la millisecondes indiquant un manque de précision ;<br><br>- *offset* : différence entre 2 temps horaires, comparé à l'horloge de référence. Cela représente l'ajustement de l'horloge local et la référence horaire ;<br><br>- s*tability* : stabilité de l'horloge ;<br><br>- vérifier le taux de requêtes UDP/NTP pour connaître la stabilité des serveurs et quantifier la charge réseau induite. |
| NTP. | Protocole de temps réseaux définit par la RFC 1305 de mars 1992 : un protocole qui permet de synchroniser, *via* un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure. L'heure de référence fournie par NTP est UTC, à ce titre, il ne s'occupe pas :<br><br>- du changement de l'heure dû au fuseau horaire ;<br><br>- du passage à l'heure d'été et d'hiver. |
| Poste terminal. | Selon la directive n° 8/DEF/DGSIC du 29 juin 2009 modifiée, définissant les règles à appliquer aux systèmes de postes terminaux.<br><br>Quatre types de postes terminaux sont définis :<br><br>- type 1 : poste banalisé fixe non contraint en débit qui s'appuie sur un réseau fixe maîtrisé par le ministère de la défense ou sur un réseau civil non maîtrisé ;<br><br>- type 2 : poste banalisé mobile qui s'appuie sur un réseau fixe maîtrisé par le ministère de la défense ou sur un réseau civil non maîtrisé ;<br><br>- type 3 : poste banalisé permettant une autonomie complète qui s'appuie sur un réseau projetable contraint en débit, maîtrisé par le ministère de la défense ;<br><br>- type 4 : poste spécifique. |
| SNTP. | Sous ensemble du protocole NTP. La spécification *simple network time protocol* (SNTP) recommande de n'utiliser SNTP qu'aux extrémités d'un réseau NTP. Par rapport à NTP, cette version est simplifiée dans le sens où elle ne spécifie pas les algorithmes à mettre en place dans les machines ce qui entraîne une précision moindre et un risque de retour en arrière brutal de l'horloge. |
| STANAG 4430. | *Precise time and frequency interface and its management for military electronic systems*. |
| Strate. | Le réseau NTP est composé :<br><br>- de récepteurs récupérant l'heure de référence par radios, câbles, satellites ou directement depuis une horloge atomique ;<br><br>- de serveurs de temps récupérant l'heure de référence auprès des récepteurs ou bien auprès d'autres serveurs de temps ;<br><br>- de clients récupérant l'heure de référence auprès des serveurs de temps.<br><br>Tous ces systèmes sont organisés de façon hiérarchique, dont chaque couche ou niveau est appelé une strate. Chaque client NTP de strate N se synchronise avec d'autres serveurs, le plus souvent de la strate égale ou inférieure et peut également faire office de serveur NTP de strate N+1. La strate 0 |

| | |
|---|---|
| | comprend des horloges de référence (récepteurs GPS ou grandes ondes, horloges au césium ou au rubidium, oscillateur à quartz thermostaté, etc.) qui ne sont pas connectées aux serveurs de strate 1 *via* un réseau mais *via* une interface comme un port série. La norme prévoit jusqu'à 16 strates, mais la plupart des clients se situent dans les strates 3 ou 4. La redondance des serveurs et leur organisation permet une répartition de la charge et ainsi la fiabilité du réseau. |
| Stratum. | Voir strate. |
| TUC. | Échelle de temps adoptée comme base du temps civil international par la majorité des pays du globe. |