Groupe de travail Réseau	D. Mills
Request for Comments : 4330	University of Delaware
RFC rendues obsolètes : 2030, 1769	janvier 2006
Catégorie : Information	Traduction Claude Brière de L'Isle

Version 4 du protocole simple de l'heure du réseau (SNTP) pour IPv4, IPv6 et OSI

Résumé
Ce mémoire décrit la version 4 du protocole simple de l'heure du réseau (SNTPv4, *Simple Network Time Protocol Version 4*), qui est un sous-ensemble du protocole de l'heure du réseau (NTP, *Network Time Protocol*) utilisé pour synchroniser les horloges des ordinateurs dans l'Internet. SNTPv4 peut être utilisé lorsque les performances extrêmes d'une mise en œuvre complète fondée sur la RFC 1305 ne sont ni nécessaires ni justifiées. Lorsque il fonctionne avec les versions courante et précédente de NTP et de SNTP, SNTPv4 ne requiert aucun changement des spécifications ou des mises en œuvre connues, mais précise plutôt certaines caractéristiques de conception qui permettent un fonctionnement dans un mode d'appel de procédure à distance (RPC) simple, sans état, avec des attentes de précision et de fiabilité similaires à celles du protocole UDP/TIME décrit dans la RFC 868.

Le présent mémoire rend obsolète la RFC 1769, qui décrit SNTP version 3 (SNTPv3), et la RFC 2030, qui décrit SNTPv4. Son objet est de corriger certaines incohérences des documents précédents et de préciser les formats d'en-tête et les opérations de protocole pour NTPv3 (IPv4) et SNTPv4 (IPv4, IPv6, et OSI), qui sont aussi utilisées pour SNTP. Il a aussi pour objet de fournir des lignes directrices pour les mises en œuvre de client domestique et d'affaires pour les routeurs et autres appareils d'utilisateurs pour protéger la population des serveurs contre les abus. Il n'est pas nécessaire de connaître le fonctionnement de la spécification NTPv3, la RFC 1305, pour la mise en œuvre de SNTP.

Table des matières

1. Introduction

Le protocole de l'heure du réseau version 3 (NTPv3), spécifié dans la RFC 1305 [MIL92], est largement utilisé pour synchroniser les horloges d'ordinateurs dans l'Internet du monde entier. Il fournit des mécanismes exhaustifs pour accéder aux services nationaux de l'heure et de la répartition des fréquences, il organise le sous-réseau NTP de serveurs et de clients, et ajuste le système d'horloge de chaque participant. Dans la plupart des lieux de l'Internet d'aujourd'hui, NTP fournit une précision de 1 à 50 ms, selon les caractéristiques de la source de synchronisation et les chemins du réseau.

La RFC 1305 spécifie la machine du protocole NTP en termes d'événements, d'états, de fonctions et d'actions de transition,

et d'algorithmes d'ingénierie pour améliorer la qualité de la conservation de l'heure et pour mixer plusieurs sources de synchronisation dont certaines peuvent être erronées. Pour réaliser des précisions de quelques millisecondes sur des chemins qui s'étendent sur des portions majeures de l'Internet, ces algorithmes compliqués, ou leurs équivalents fonctionnels, sont nécessaires. Dans de nombreuses applications, des précisions de l'ordre de fractions significatives de la seconde sont acceptables. Dans des applications de simple routeur domestique, des précisions jusqu'à une minute peuvent suffire. Dans de tels cas, des protocoles plus simples, tels que le protocole de l'heure spécifié dans la RFC 868 [POS83], ont été utilisés à cette fin. Ces protocoles impliquent un commutateur RPC auquel le client demande l'heure et le serveur la retourne sous forme de secondes écoulées depuis une époque de référence connue.

NTP est conçu pour être utilisé par une large gamme de capacités de clients et serveurs et sur une large gamme de caractéristiques de gigue du réseau et d'excursion de fréquence d'horloge. De nombreux utilisateurs de NTP dans l'Internet d'aujourd'hui utilisent un logiciel dont la distribution est disponible auprès de www.ntp.org. La distribution, qui comporte la suite complète des options de NTP, des algorithmes de mixage, et des schémas de sécurité, est une application relativement complexe, en temps réel. Bien que le logiciel ait été installé sur une grande variété de plates-formes matérielles allant du micro-ordinateur au super calculateur, sa taille et sa complexité ne sont pas appropriées pour de nombreuses applications. En conséquence, il est utile d'explorer des stratégies de remplacement en utilisant un logiciel plus simple approprié à des attentes de précision moins strictes.
Le présent mémoire décrit la version 4 du protocole simple de l'heure du réseau (SNTPv4), qui est un paradigme d'accès simplifié pour les serveurs et clients qui utilisent les versions actuelles et précédentes de NTP et SNTP. Le paradigme d'accès est identique au protocole UDP/TIME, et en fait, il devrait être aisé d'adapter une mise en œuvre de client UDP/TIME, disons pour un micro-ordinateur, pour qu'elle fonctionne en utilisant SNTP. De plus, SNTP est aussi conçu pour fonctionner dans une configuration de serveur dédié y compris une horloge radio intégrée. Avec une conception soigneuse et le contrôle des diverses latences dans le système, ce qui est praticable dans une conception dédiée, il est possible de délivrer une précision horaire de l'ordre de la microseconde.

Le seul changement significatif de protocole dans SNTPv4 par rapport aux précédentes versions de SNTP est l'interprétation d'un en-tête modifié pour s'accommoder de l'adressage de la version 6 du protocole Internet (IPv6) (RFC 2460) et de l'OSI (RFC 1629). Cependant, SNTPv4 comporte un certain nombre d'extensions facultatives au modèle de la version 3 de NTP (NTPv3), y compris un modèle de multi envoi *(manycast)* et un schéma d'authentification fondé sur la clé publique conçu spécifiquement pour les applications de diffusion et de multi envoi. Bien que le mode de multi envoi soit décrit dans le présent mémoire, le schéma d'authentification est décrit dans une autre RFC qui sera proposée ultérieurement. Jusqu'à ce qu'une spécification définitive de NTPv4 soit publiée, les caractéristiques de multi envoi et d'authentification devraient être considérées comme provisoires. De plus, le présent mémoire introduit le message du baiser de la mort *(kiss-o'-death)* qui peut être utilisé par les serveurs pour supprimer les demandes du client lorsque les circonstances l'exigent.

Lorsqu'il fonctionne avec les versions actuelle et précédentes de NTP et de SNTP, SNTPv4 n'exige pas de changement au protocole ou des mises en œuvre qui fonctionnent actuellement ou qui seront vraisemblablement mises en œuvre spécifiquement pour les versions futures de NTP ou SNTP. Les formats de paquet NTP et SNTP sont les mêmes, et les opérations arithmétiques pour calculer l'heure du client, le décalage d'horloge et les délais d'aller-retour sont les mêmes. Pour un serveur NTP ou SNTP, les clients NTP et SNTP sont indistinguables ; pour un client NTP ou SNTP, les serveurs NTP et SNTP sont indistinguables. Comme les serveurs NTP qui fonctionnent dans des modes non symétriques, les serveurs SNTP sont sans état et peuvent prendre en charge un grand nombres de clients ; cependant, à la différence de la plupart des clients NTP, les clients SNTP fonctionnent normalement avec un seul serveur à la fois.

La pleine mesure de la fiabilité normalement attendue des serveurs NTP n'est possible qu'en utilisant des sources redondantes, des chemins variés, et les algorithmes habiles d'une pleine mise en œuvre de NTP. Il est vivement recommandé que les clients SNTP ne soient utilisés qu'aux extrémités d'un sous-réseau de synchronisation. Les clients SNTP ne devraient fonctionner qu'avec les derniers embranchements (la plus haute strate) du sous-réseau et dans des configurations où aucun client NTP ou SNTP n'est dépendant d'un autre client SNTP pour la synchronisation. Les serveurs SNTP ne devraient fonctionner qu'à la racine (strate 1) du sous-réseau, et alors seulement dans les configurations où aucune autre source de synchronisation qu'une horloge radio fiable ou un modem téléphonique n'est disponible.

Une disposition importante du présent mémoire est l'interprétation de certains champs d'en-tête NTP qui fournissent l'adressage IPv6 [DEE98] et OSI [COL94]. La seule différence significative entre les formats d'en-tête NTP et SNTPv4 est le champ d'identifiant de référence de quatre octets, qui est principalement utilisé pour détecter et éviter les boucles de synchronisation. Dans toutes les versions de NTP et de SNTP qui fournissent l'adressage IPv4, les serveurs principaux utilisent un identifiant d'horloge de référence ASCII de quatre caractères dans ce champ, tandis que les serveurs secondaires utilisent l'adresse IPv4 de 32 bits de la source de synchronisation. Dans SNTPv4 qui fournit l'adressage IPv6 et OSI, les serveurs primaires utilisent le même identifiant d'horloge, mais les serveurs secondaires utilisent les 32 premiers bits du hachage MD5 de l'adresse IPv6 ou NSAP de la source de synchronisation. Un autre usage de ce champ est lorsque le serveur envoie un message de baiser de la mort, documenté plus loin dans ce mémoire.

NTP version 4 (NTPv4), qui est maintenant en cours de développement, mais qui n'est pas encore l'objet d'un document de normalisation, utilise le même champ d'identifiant de Référence que SNTPv4.

Dans le cas de OSI, le service de transport sans connexion (CLTS, *Connectionless Transport Service*) est utilisé comme dans [ISO86]. Chaque paquet SNTP est transmis comme le paramètre TS-Userdata d'une primitive de demande T-UNITDATA. Autrement, l'en-tête peut être encapsulé dans une unité de données de protocole de transport (TPDU, *Transport Protocol Data Unit*), qui est elle-même transportée en utilisant UDP, comme décrit dans la RFC 1240 [DOB91]. Il n'est pas conseillé de faire fonctionner NTP aux couches supérieures de la pile de protocoles OSI, comme on pourrait le comprendre d'après la RFC 1698 [FUR94], car cela pourrait dégrader sérieusement la précision. Avec les formats d'en-tête définis dans le présent mémoire, il est en principe possible d'interfonctionner entre serveurs et clients d'une famille de protocoles et l'autre, bien que les difficultés pratiques puissent le faire déconseiller.

Dans ce qui suit, les paragraphes en retrait comme celui-ci contiennent des informations qui ne sont pas exigées par la spécification formelle du protocole, mais sont considérées comme de bonne pratique dans ses mises en œuvre.

Le présent mémoire est organisé comme suit. La Section 2 décrit le fonctionnement du protocole, ses différents modes, et comment sont utilisées les adresses IP et les accès UDP. La Section 3 décrit le format d'horodatage NTP, et la Section 4 le format de message NTP. La Section 5 résume les opérations du client SNTP, et la Section 6 résume les opérations du serveur SNTP. La Section 7 décrit les questions de fonctionnement et de gestion. La Section 8 décrit le message du baiser de la mort, nouvellement forgé avec des fonctions similaires à celles des messages ICMP Extinction de source et Destination injoignable. La Section 9 présente les questions de conception importantes pour un comportement citoyen et présente un exemple d'algorithme conçu pour donner une bonne fiabilité tout en minimisant la demande de ressources de réseau et de serveur.

1.1 Spécification des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT" et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la RFC 2119 [BRA97].

2. Modes de fonctionnement et adressage

Sauf exception mentionnée dans le contexte, une référence à une adresse de diffusion signifie une adresse de diffusion IPv4, une adresse de diffusion groupée IPv4, ou une adresse IPv6 de portée appropriée. On trouvera d'autres informations sur le modèle de diffusion/diffusion groupée dans la RFC 1112 [DEE89]. Les détails sur le format d'adresse, les règles de domaine d'application, etc., sortent du domaine d'application du pèsent mémoire. SNTPv4 peut fonctionner dans les modes d'adressage d'envoi individuel (point à point), de diffusion (point à multipoint), ou de multi envoi (multipoint à point). Un client en envoi individuel envoie une demande à un serveur désigné à son adresse d'envoi individuel et attend une réponse d'après laquelle il peut déterminer l'heure et, facultativement, le délai d'aller-retour et le décalage d'horloge par rapport au serveur. Un serveur de diffusion envoie périodiquement un message non sollicité à une adresse de diffusion désignée. Un client de diffusion écoute à cette adresse et n'envoie ordinairement pas de demandes.

Le multi envoi *(manycast)* est une extension du paradigme de l'envoi individuel décrit dans la RFC 1546 [PAR93]. Il est conçu pour être utilisé avec un ensemble de serveurs en coopération dont les adresses ne sont pas connues à l'avance. Le client de multi envoi envoie une demande ordinaire de client NTP à une adresse de diffusion désignée. Un ou plusieurs serveurs de multi envoi écoutent à cette adresse. À réception d'une demande, un serveur de multi envoi envoie une réponse NTP ordinaire au client. Le client mobilise alors une association pour chaque serveur trouvé et continue l'opération avec chacun d'eux. Ensuite, l'algorithme NTP de mixage fonctionne pour ne garder que les trois meilleurs.

Les serveurs de diffusion devraient répondre aux demandes d'envoi individuel du client, ainsi qu'aux messages en diffusion non sollicités. Les clients de diffusion peuvent envoyer des demandes en envoi individuel afin de mesurer les délais de propagation du réseau entre le serveur et le client puis continuer de fonctionner en mode d'écoute seule. Cependant, les serveurs de diffusion peuvent choisir de ne pas répondre aux demandes en envoi individuel, de sorte que les clients d'envoi individuel devraient être prêts à abandonner la mesure et à supposer une valeur par défaut pour le délai.

Les adresses de client et de serveur sont allouées selon les conventions IPv4, IPv6 ou OSI usuelles. Pour le multi envoi NTP, l'IANA a réservé le groupe d'adresses IPv4 224.0.1.1 et la terminaison d'adresse IPv6 :101 avec le domaine d'application approprié. L'adresse de diffusion NTP pour OSI a déjà été déterminée. Bien que des adresses aient été réservées par l'IANA, d'autres adresses de diffusion groupée peuvent être utilisées à condition qu'elles n'entrent pas en conflit avec les autres domaines d'application alloués. Les procédures de définition de portée et d'adhésion au groupe sont

déterminées par des considérations qui sortent du domaine d'application du présent mémoire.

Il est important de régler le champ Durée de vie (TTL, *time-to-live*) dans l'en-tête IP des messages de diffusion groupée à une valeur raisonnable afin de limiter les ressources réseau utilisées par ce service de diffusion groupée (et tous les autres). Seuls les clients dont le domaine d'application est la diffusion groupée vont recevoir les messages du serveur de diffusion groupée. Seuls les serveurs dont le domaine d'application est le multi envoi coopératif vont répondre à une demande du client. Les principes d'ingénierie qui déterminent les valeurs appropriées à utiliser sortent du domaine d'application du présent mémoire.

Dans le cas de SNTP tel que spécifié ici, le fait que les clients de diffusion de SNTP puissent être perturbés par des serveurs de diffusion SNTP ou NTP hostiles ou au mauvais comportement ailleurs dans l'Internet est une très réelle faiblesse. Il est vivement recommandé que des moyens de contrôle d'accès et/ou d'authentification cryptographique soient fournis pour une meilleure sécurité dans de tels cas.

Il est prévu que les adresses de diffusion IP soient principalement utilisées dans les sous-réseaux IP et les segments de LAN qui comportent un serveur NTP pleinement fonctionnel avec un certain nombre de clients SNTP qui en dépendent sur le même sous-réseau, et que les adresses de groupe de diffusion groupée IP soient utilisées seulement dans les cas où le TTL est mis en œuvre de façon spécifique pour chaque domaine de service. Cependant, ces utilisations ne sont pas intégrées à la spécification SNTP.

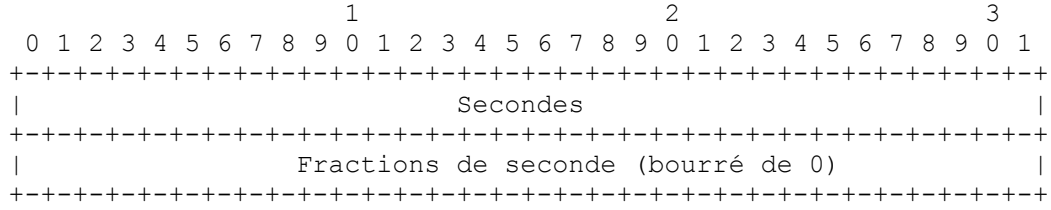
3. Format de l'horodatage NTP

SNTP utilise le format d'horodatage NTP standard décrit dans la RFC 1305 et dans les versions précédentes de ce document. Conformément aux pratiques standard de l'Internet, les données NTP sont spécifiées comme des quantités d'entier ou à virgule fixe, avec les bits numérotés en mode gros boutien à partir de 0 en commençant pas la gauche ou l'extrémité de poids fort. Sauf spécification contraire, toutes les quantités sont non signées et peuvent occuper la pleine largeur du champ avec un 0 implicite précédant le bit 0.

Comme les horodatages NTP sont des données chouchoutée qui, en fait, représentent le principal produit du protocole, un format d'horodatage particulier a été établi. Les horodatages NTP sont représentés comme un nombre à virgule fixe non signé de 64 bits, en secondes par rapport à 0 h le 1er janvier 1900. La partie entière dans les 32 premiers bits, et la partie fraction dans les 32 derniers bits. Dans la partie fraction, les bits de poids faible non significatifs ne sont pas spécifiés et sont ordinairement mis à 0.

Il est conseillé de remplir les bits non significatifs de poids faible de l'horodatage avec une chaîne binaire aléatoire non biaisée, à la fois pour éviter les erreurs d'arrondi systématiques et pour fournir un moyen de détection de boucle et de répétition (voir ci-dessous). Il est important que la chaîne binaire soit imprévisible par un intrus. Une façon d'y arriver est de générer uns chaîne binaire aléatoire de 128 bits au démarrage. Après cela, chaque fois que l'horloge système est lue, la chaîne comportant l'horodatage et la chaîne binaire est hachée avec l'algorithme MD5, puis les bits non significatifs de l'horodatage sont copiés à partir du résultat.

Le format NTP permet une arithmétique à précision multiple pratique et la conversion en message UDP/TIME (secondes), mais complique la conversion en message d'horodatage ICMP (millisecondes) et en valeurs de temps Unix (secondes et microsecondes ou secondes et nanosecondes). Le nombre maximum qui peut être représenté est 4 294 967 295 secondes avec une précision d'environ 232 picosecondes, qui devrait être adéquate pour les exigences les plus exotiques.



Noter que depuis une certaine heure en 1968 (la seconde 2 147 483 648), le bit de poids fort (le bit 0 de la partie entière) a été mis à 1 et que le champ de 64 bits va déborder à un moment de 2036 (à la seconde 4 294 967 296). Il existera un intervalle de 232-picosecondes, qui sera donc ignoré, tous les 136 ans lorsque le champ de 64 bits sera à 0, ce qui par convention est interprété comme un horodatage invalide ou indisponible.

Comme le format d'horodatage NTP a été utilisé pendant plus de 20 ans, il est possible qu'il soit encore utilisé dans 32 ans, quand le champ des secondes va déborder. Comme il est probablement inapproprié d'archiver les horodatages NTP

avant la mise à 1 du bit 0 en 1968, une façon pratique d'étendre la vie utile des horodatages NTP est la convention suivante : si le bit 0 est mis à 1, le temps UTC est dans la gamme 1968-2036, et le temps UTC est pris en compte à partir du 1er janvier 1900 à 0 h 0 min 0 s UTC. Si le bit 0 n'est pas mis à 1, l'heure est dans la gamme 2036-2104 et le temps UTC est calculé à partir du 7 février 2036 à 6 h 28 min 16 s UTC. Noter qu'en calculant la correspondance, 2000 est une année à saut, et les secondes sautées ne sont pas incluses dans le calcul.

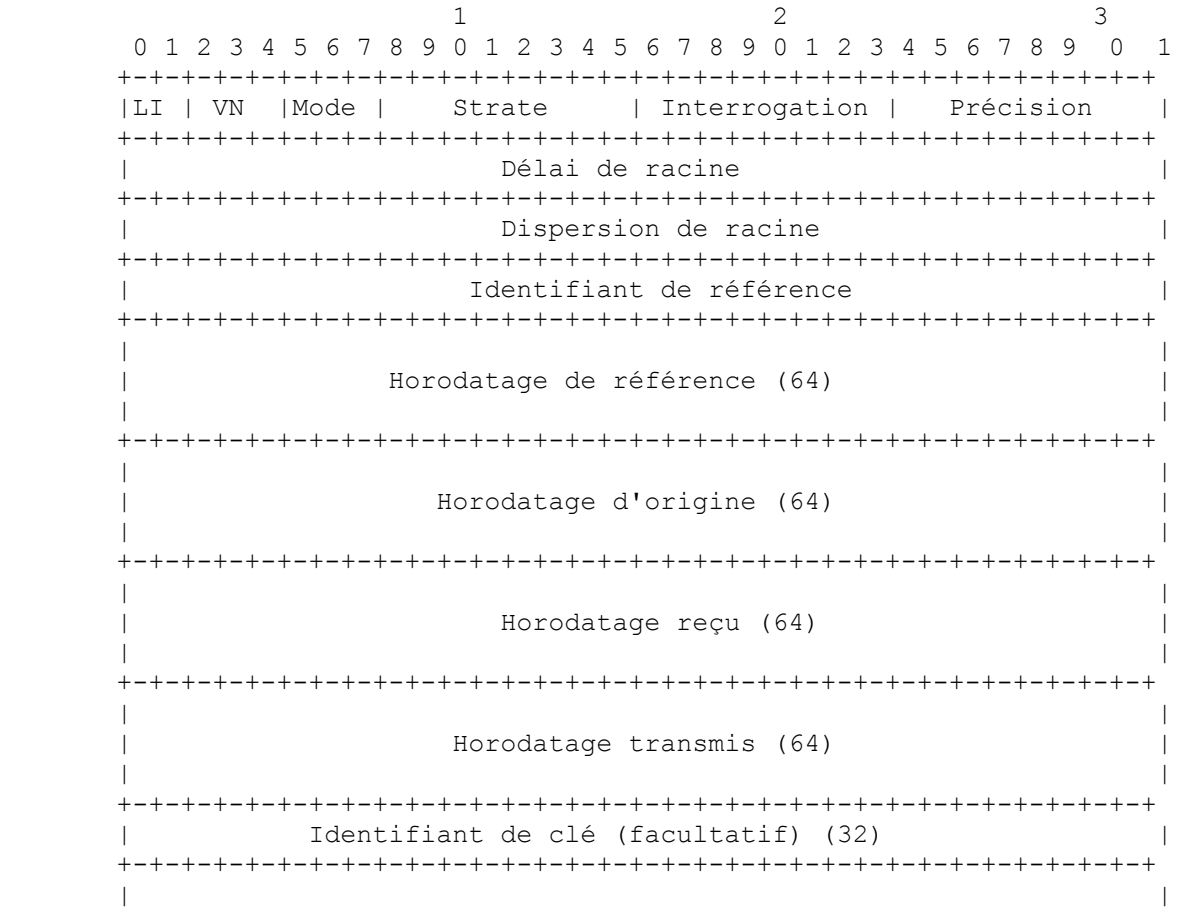
Les calculs arithmétiques utilisés par NTP pour déterminer le décalage d'horloge et le délai d'aller-retour exigent que l'heure du client soit dans les 34 années de l'heure du serveur avant que le client ne soit lancé. Comme l'heure depuis la base 1970 d'Unix est maintenant de plus de 34 ans, des moyens doivent être disponibles pour initialiser l'horloge à une date plus proche du présent, soit avec une puce de l'heure de l'année (TOY, *time-of-year*) soit à partir d'un logiciel particulier.

4. Format de message

NTP et SNTP sont tous deux des clients du protocole de datagramme d'utilisateur (UDP, *User Datagram Protocol*) spécifié dans la RFC 768 [POS80]. Les structures des en-têtes IP et UDP sont décrites dans les documents de spécification cités et ne seront pas détaillés plus avant ici. Le numéro d'accès UDP alloué par l'IANA à NTP est 123. Le client SNTP devrait utiliser cette valeur dans le champ Accès de destination UDP pour les messages de demande clients. Le champ Accès de source de ces messages peut être toute valeur non zéro choisie pour les besoins d'identification ou de multiplexage. Le serveur échange ces champs pour les messages de réponse correspondants.

Ceci diffère des spécifications de la RFC 2030, qui exigeait que les accès de source et de destination soient tous deux 123. L'intention de ce changement est de permettre l'identification de mises en œuvre client particulières (à qui il est maintenant permis d'utiliser des numéros d'accès non réservés, y compris ceux de leur choix) et d'atteindre la compatibilité avec la traduction d'accès d'adresse réseau (NAPT, *Network Address Port Translation*) décrite dans la RFC 2663 [SRI99] et la RFC 3022 [SRI01].

La Figure 1 est une description du format de message NTP et SNTP, qui suit les en-têtes IP et UDP dans le message. Ce format est identique au format de message NTP décrit dans la RFC 1305, à l'exception du champ d'Identifiant de référence décrit ci-dessous. Pour les messages de client SNTP, la plupart de ces champs sont à zéro ou sont initialisés avec des données pré spécifiées. Pour être complet, la fonction de chaque champ est brièvement résumée ci-dessous.



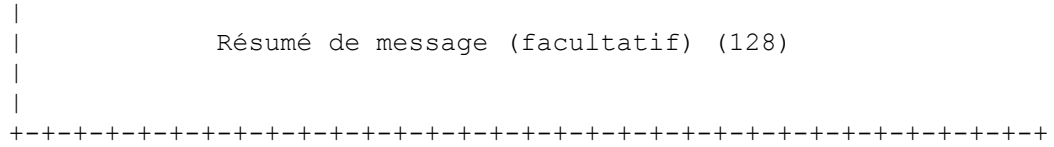


Figure 1 ; En-tête de paquet NTP

Indicateur de saut (LI, *Leap Indicator*) : C'est un code de deux bits avertissant du saut imminent d'une seconde à insérer/supprimer dans la dernière minute du jour en cours. Ce champ n'est significatif que dans les messages de serveur, et les valeurs sont définies comme suit :

LI	**Signification**
0	pas d'avertissement
1	la dernière minute a 61 secondes
2	la dernière minute a 59 secondes
3	condition d'alarme (horloge non synchronisée)

Au démarrage, les serveurs règlent de champ à 3 (horloge non synchronisée), et règlent ce champ à une autre valeur lorsqu'ils sont synchronisés à l'horloge de référence principale. Une fois réglé à une valeur autre que 3, le champ n'est jamais réglé à cette valeur à nouveau, même si toutes les sources de synchronisation deviennent injoignables ou défectueuses.

Numéro de version (VN, *Version Number*) : C'est un entier de trois bits qui indique le numéro de version NTP/SNTP, actuellement 4. Si il est nécessaire de distinguer entre IPv4, IPv6, et OSI, le contexte de l'encapsulation doit être inspecté.

Mode : C'est un nombre de trois bits qui indique le mode du protocole. Les valeurs sont définies comme suit :

Mode	**Signification**
0	réservé
1	actif symétrique
2	passif symétrique
3	client
4	serveur
5	diffusion
6	réservé pour le message de contrôle NTP
7	réservé pour utilisation privée

En mode d'envoi individuel et de multi envoi, le client règle ce champ à 3 (client) dans la demande, et le serveur le règle à 4 (serveur) dans la réponse. En mode diffusion, le serveur règle ce champ à 5 (diffusion). Les autres modes ne sont pas utilisés par les serveurs et clients SNTP.

Strate : C'est un entier non signé de huit bits qui indique la strate. Ce champ n'est significatif que dans les messages de serveur SNTP, et ses valeurs sont définies comme suit :

Strate	**Signification**
0	message de baiser de la mort (voir plus loin)
1	référence principale (par exemple, synchronisée par horloge radio)
2 à 15	référence secondaire (synchronisée par NTP ou SNTP)
16 à 255	réservé

Intervalle d'interrogation : C'est u entier non signé de huit bits utilisé comme puissance de deux, où la valeur résultante est l'intervalle maximum entre les messages successifs en secondes. Ce champ n'est significatif que dans les messages de serveur SNTP, et ses valeurs sont dans la gamme de 4 (16 s) à 17 (131 072 s -- environ 36 h).

Précision : C'est un entier signé de huit bits utilisé comme puissance de deux, où la valeur résultante est la précision de l'horloge système en secondes. Ce champ n'est significatif que dans les messages de serveur, et ses valeurs sont dans la gamme de -6 pour les horloges à la fréquence du réseau d'alimentation électrique à -20 pour les horloges à la microseconde qui se rencontrent dans certaines stations de travail.

Délai de racine : C'est un nombre signé de 32 bits à virgule fixe qui indique le délai d'aller-retour total de la source de référence principale, en secondes, avec la virgule de fraction entre les bits 15 et 16. Noter que cette variable peut prendre des valeurs positives et négatives, selon l'heure relative et les décalages de fréquence. Ce champ n'est significatif que dans les messages de serveur, et ses valeurs sont dans la gamme des valeurs négatives de quelques millisecondes à des valeurs positives de plusieurs centaines de millisecondes.

Code	**Source de référence externe**
LOCL	horloge locale non calibrée
CESM	horloge calibrée au césium
RBDM	horloge calibrée au rubidium
PPS	horloge à quartz calibrée ou autre source à impulsion par seconde
IRIG	Inter-Range Instrumentation Group
ACTS	service de modem téléphonique du NIST
USNO	service de modem téléphonique de USNO
PTB	service de modem téléphonique de PTB (DE)
TDF	Radio Allouis (France) 164 kHz
DCF	Radio Mainflingen (DE) 77,5 kHz
MSF	Radio Rugby (UK) Radio 60 kHz
WWV	Radio Ft. Collins (US) Radio 2,5, 5, 10, 15, 20 MHz
WWVB	Radio Boulder (US) Radio 60 kHz
WWVH	Radio Kauai Hawaii (US) Radio 2,5, 5, 10, 15 MHz
CHU	Radio Ottawa (Canada) 3330, 7335, 14670 kHz
LORC	système de radionavigation LORAN-C
OMEG	système de radionavigation OMEGA
GPS	Service de positionnement mondial

Figure 2 : Codes des identifiants de référence

Dispersion de racine : C'est un nombre signé de 32 bits à virgule fixe qui indique l'erreur maximale due à la tolérance de fréquence de l'horloge, en secondes avec la virgule de fraction entre les bits 15 et 16. Ce champ n'est significatif que dans les messages du serveur, et ses valeurs vont de zéro à plusieurs centaines de millisecondes.

Identifiant de référence : C'est une chaîne binaire de 32 bits qui identifie la source de référence particulière. Ce champ n'est significatif que dans les messages du serveur, où pour la strate 0 (message de baiser de la mort) et 1 (serveur principal), la valeur est une chaîne ASCII de quatre caractères, justifiée à gauche et bourrée de zéros jusqu'à 32 bits. Pour les serveurs secondaires IPv4, la valeur est l'adresse IPv4 de 32 bits de la source de synchronisation. Pour les serveurs secondaires IPv6 et OSI, la valeur est les 32 premiers bits du hachage MD5 de l'adresse IPv6 ou NSAP de la source de synchronisation.

Les serveurs principaux (strate 1) règlent ce champ à un code qui identifie la source de référence externe conformément à la Figure 2. Si la référence externe est une de celles figurant sur la liste, le code associé devrait être utilisé. Les codes pour les sources qui ne figurent pas sur la liste peuvent être forcés, selon le cas.

> Dans les serveurs et clients secondaires NTP et SNTP précédents, ce champ était souvent utilisé pour ramener le sous-réseau de synchronisation à la racine (serveur principal) pour des besoins de gestion. Dans SNTPv4 avec IPv6 ou OSI, cette caractéristique n'est pas disponible, parce que les adresses font plus de 32 bits, et seul un hachage est disponible. Cependant, un retour peut être effectué en utilisant le message de contrôle NTP et le champ d'identifiant de référence décrit dans la RFC 1305.

Horodatage de référence : Ce champ est l'heure à laquelle l'horloge système a été réglée ou corrigée pour la dernière fois, en format d'horodatage à 64 bits.

Horodatage d'origine : C'est l'heure à laquelle la demande est partie de chez le client pour le serveur, en format d'horodatage à 64 bits.

Horodatage reçu : C'est l'heure à laquelle la demande est arrivée chez le serveur ou à laquelle la réponse est arrivée chez le client, en format d'horodatage à 64 bits.

Horodatage transmis : C'est l'heure à laquelle la demande est partie du client ou à laquelle la réponse est partie du serveur, en format d'horodatage à 64 bits.

Authentificateur (facultatif) : Lorsque le schéma d'authentification NTP est mis en œuvre, les champs Identifiant de clé et Résumé de message contiennent les informations de code d'authentification de message (MAC, *Message Authentication Code*) définies dans l'Appendice C de la RFC 1305.

5. Opérations du client SNTP

Un client SNTP peut fonctionner en modes d'envoi individuel, en diffusion ou en multi envoi. En mode d'envoi individuel, le client envoie une demande (mode NTP 3) à un serveur d'envoi individuel désigné et attend une réponse (mode NTP 4) de ce serveur. En mode client de diffusion, il n'envoie pas de demande et attend une diffusion (mode NTP 5) de la part d'un ou plusieurs serveurs de diffusion. En mode multi envoi, le client envoie une demande (mode NTP 3) à une adresse de diffusion désignée et attend une réponse (mode NTP 4) de la part d'un ou plusieurs serveurs de multi envoi. Le client utilise la première réponse reçue pour établir le serveur particulier pour des opérations ultérieures d'envoi individuel. Les réponses ultérieures de ce serveur (duplicata) ou de tout autre serveur sont ignorées. À part la sélection d'adresse dans la demande, les opérations de clients de multi envoi et d'envoi individuel sont identiques.

> Les demandes du client sont normalement envoyées à des intervalles qui dépendent de la tolérance de fréquence de l'horloge du client et de la précision requise. Cependant, en aucun cas;, les demandes ne devraient être envoyées à des intervalles inférieurs à une minute. Un exposé complémentaire sur ce point figure à la Section 9.

Un client d'envoi individuel ou multiple initialise l'en-tête de message NTP, envoie la demande au serveur, et recueille l'heure dans le champ Horodatage transmis de la réponse. À cette fin, tous les champs d'en-tête NTP montrés ci-dessus sont réglés à 0, excepté les champs Mode, VN, et Horodatage transmis facultatif.

Les clients NTP et SNTP règlent le champ mode à 3 (client) pour les demandes en envoi individuel et en multi envoi. Ils règlent le champ VN à tout numéro de version pris en charge par le serveur, choisi par configuration ou découverte, et qui peut interopérer avec tous les serveurs NTP et SNTP de version précédente. Les serveurs répondent avec la même version que la demande, de sorte que le champ VN de la demande spécifie aussi le champ VN de la réponse. Un client SNTP prudent peut spécifier la plus ancienne version acceptable en espérant que tout serveur de cette version ou d'une plus récente va répondre. Les serveurs NTP de version 3 (RFC 1305) et de version 2 (RFC 1119) acceptent toutes les versions précédentes, y compris la version 1 (RFC 1059). Noter que la version 0 (RFC 959) n'est plus acceptée par les serveurs NTP et SNTP actuels et futurs.

Bien qu'il ne soit pas nécessaire de régler le champ Horodatage transmis dans la demande à l'heure qui figure dans le format d'horodatage NTP de l'horloge du client dans une mise en œuvre de client conforme, il est vivement recommandé de le faire dans les modes d'envoi individuel et de multi envoi. Cela permet de déterminer par un simple calcul le délai de propagation entre le serveur et le client et d'aligner l'horloge système dans un écart généralement inférieur à quelques dixièmes de millisecondes par rapport au serveur. De plus, cela fournit une méthode simple pour vérifier que la réponse du serveur est en fait une réponse légitime à la demande spécifique du client ce qui évité donc des répétitions. En mode diffusion, le client n'a pas d'information pour calculer le délai de propagation ou pour déterminer la validité du serveur, sauf à utiliser un des schémas d'authentification NTP.

Pour calculer le délai d'aller-retour d et le décalage d'horloge du système t par rapport au serveur, le client règle le champ Horodatage transmis de la demande à l'heure conforme à l'horloge du client dans le format d'horodatage NTP. À cette fin, l'horloge n'a pas besoin d'être synchronisée. Le serveur copie dans la réponse ce champ Horodatage d'origine et règle les champs Horodatage reçu et Horodatage transmis à l'heure conforme à celle de l'horloge du serveur dans le format d'horodatage NTP.

Lorsque la réponse du serveur est reçue, le client détermine une variable Horodatage de destination comme heure d'arrivée conformément à son horloge en format d'horodatage NTP. Le tableau suivant résume les quatre horodatages.

Nom de l'horodatage	ID	quand il est généré
Horodatage d'origine	T1	heure de la demande envoyée par le client
Horodatage reçu	T2	heure de la demande reçue par le serveur
Horodatage transmis	T3	heure de la réponse envoyée par le serveur
Horodatage de destination	T4	heure de la réponse reçue par le client

Le délai d'aller-retour d et le décalage d'horloge du système t sont définis par :

$$d = (T4 - T1) - (T3 - T2) \qquad t = ((T2 - T1) + (T3 - T4)) / 2.$$

Noter qu'en général aussi bien le délai que le décalage sont des quantités signées qui peuvent être négatives ; cependant, un délai négatif n'est possible que dans des modes symétriques, que les clients SNTP n'ont pas le droit d'utiliser. Le tableau suivant résume les opérations exigées du client SNTP dans les modes d'envoi individuel, de multi envoi, et de diffusion. Les vérifications d'erreur recommandées sont indiquées dans les colonnes Réponse et Diffusion du tableau. Le message

devrait n'être considéré comme valide que si tous les champs indiqués contiennent des valeurs dans les gammes respectives. Savoir s'il faut croire le message si un ou plusieurs champs marqués "ignorer" contiennent des valeurs invalides est à la discrétion de la mise en œuvre.

Nom du champ	Demande en envoi individuel/multiple	Réponse en envoi individuel/multiple	Diffusion
LI	0	0 à 3	0 à 3
VN	1-4	copié d'après la demande	1 à 4
Mode	3	4	5
Strate	ignorer	0-15	0-15
Interrogation	ignorer	ignorer	ignorer
Précision	ignorer	ignorer	ignorer
Délai de racine	ignorer	ignorer	ignorer
Dispersion de racine	ignorer	ignorer	ignorer
Identifiant de référence	ignorer	ignorer	ignorer
Horodatage de référence	ignorer	ignorer	ignorer
Horodatage d'origine	ignorer	voir le texte	ignorer
Horodatage reçu	0	voir le texte	ignorer
Horodatage transmis	(voir le texte)	différent de zéro	différent de zéro
Authentificateur	facultatif	facultatif	facultatif

Bien que ce ne soit pas exigé d'une mise en œuvre de client SNTP conforme, il est avisé de prendre en compte une série de vérifications de bonne santé conçue pour éviter diverses sortes de désagréments qui pourraient survenir par suite d'erreurs de mise en œuvre du serveur ou d'attaques malveillantes. Voici une liste des vérifications suggérées.

1. Lorsque les adresses IP de source et de destination sont disponibles pour la demande du client, elles devraient correspondre aux adresses interchangées dans la réponse du serveur.

2. Lorsque les accès UDP de source et de destination sont disponibles pour la demande du client, ils devraient correspondre aux accès interchangés dans la réponse du serveur.

3. L'horodatage d'origine dans la réponse du serveur devrait correspondre à l'horodatage transmis utilisé dans la demande du client.

4. La réponse du serveur devrait être éliminée si un des champs LI, Strate, ou Horodatage transmis est à 0 ou si le champ Mode n'est pas à 4 (envoi individuel) ou 5 (diffusion).

5. Un client vraiment paranoïaque peut vérifier que les champs Délai de racine et Dispersion de racine sont chacun supérieur ou égal à 0 et inférieurs à l'infini, où l'infini est en fait un nombre de l'ordre d'une seconde. Cette vérification évite d'utiliser un serveur dont la source de synchronisation a expiré depuis très longtemps.

6. Opérations du serveur SNTP

Un serveur SNTP qui fonctionne avec un client NTP ou SNTP de la même version ou d'une version antérieure ne conserve pas d'état persistant. Parce qu'un serveur SNTP ne met généralement pas en œuvre toute la série des algorithmes de soins et de mixage destinés à prendre en charge les serveurs redondants et la diversité des chemins du réseau, il ne devrait fonctionner qu'en conjonction avec une source de synchronisation externe, telle qu'une horloge radio fiable ou un modem téléphonique. Dans ce cas, il fonctionne comme serveur principal (strate 1).

Un serveur SNTP peut fonctionner avec toute adresse d'envoi individuel, de multi envoi, ou de diffusion, ou toute combinaison de ces adresses. Un serveur d'envoi individuel ou de multi envoi reçoit une demande (mode NTP 3), modifie certains champs dans l'en-tête NTP, et envoie une réponse (mode NTP 4), éventuellement en utilisant la même mémoire tampon de message que la demande. Un serveur en multi envoi écoute sur l'adresse de diffusion désignée, mais utilise sa propre adresse IP d'envoi individuel dans le champ Adresse de source de la réponse. À part le choix de l'adresse dans la réponse, les opérations des serveurs de multi envoi et d'envoi individuel sont identiques. Les messages en diffusion sont normalement envoyés à des intervalles de 64 s à 1024 s, selon la tolérance de fréquence espérée des horloges client et la précision exigée.

Les serveurs en envoi individuel et en multi envoi copient intacts les champs VN et Interrogation de la demande dans la réponse et règlent le champ Strate à 1.

Noter que les serveurs SNTP fonctionnent normalement comme serveurs principaux (strate 1). Bien que le fonctionnement à une strate supérieure (jusqu'à 15) tout en se synchronisant à une source externe telle qu'un receveur GPS ne soit pas interdit, c'est fortement déconseillé.

Si le champ Mode de la demande est 3 (client), la réponse est réglée à 4 (serveur). Si ce champ est mis à 1 (symétrique actif), la réponse est réglée à 2 (symétrique passif). Cela permet aux clients configurés en client (mode NTP 3) ou en symétrique actif (mode NTP 1) d'interopérer avec succès, même si ils sont configurés de façon éventuellement sous optimale. Pour toute autre valeur dans le champ Mode, la demande est éliminée. En mode diffusion (non sollicité), le champ VN est réglé à 4, le champ Mode est mis à 5 (diffusion), et le champ Interrogation est réglé au logarithme en base 2 entier le plus proche de l'intervalle d'interrogation.

Noter qu'il est très souhaitable qu'un serveur de diffusion prenne aussi en charge les clients d'envoi individuel. Ainsi un client de diffusion potentiel peut calculer le délai de propagation en utilisant un échange client/serveur avant de passer au mode de client de diffusion (en écoute seule). Par nature, un serveur de multi envoi est aussi un serveur d'envoi individuel. Il ne semble pas y avoir grand avantage qu'un serveur fonctionne à la fois en diffusion et en multi envoi en même temps, bien que la spécification du protocole ne l'interdise pas.

Un serveur de diffusion ou de multi envoi n'envoie pas de paquets si il n'est pas synchronisé à une source de référence qui fonctionne correctement. Il peut ou non répondre à une demande de client si il n'est pas synchronisé, mais l'option préférée est qu'il réponde parce que cela permet de déterminer l'accessibilité sans considération de l'état de synchronisation. Si le serveur n'a jamais été synchronisé à une source de référence, le champ LI est réglé à 3 (non synchronisé). Une fois synchronisé à une source de référence, le champ LI est réglé à une des trois autres valeurs et reste à la dernière valeur établie même si la source de référence devient injoignable ou devient fautive.

Si le serveur est synchronisé à une source de référence, le champ Strate est réglé à 1, et le champ Identifiant de référence est mis à l'identifiant de source ASCII montré à la Figure 2. Si le serveur n'est pas synchronisé, le champ Strate est réglé à zéro, et le champ Identifiant de référence est mis à un identifiant d'erreur ASCII décrit plus loin.

Le champ Précision est réglé de façon à refléter l'erreur de lecture maximum de l'horloge système. Pour tous les cas pratiques il est calculé comme le logarithme négative de base 2 du nombre de bits significatifs à droite de la virgule dans le format d'horodatage NTP. Les champs Délai de racine et Dispersion de racine sont mis à 0 pour un serveur primaire.

Les champs d'horodatage dans le message de serveur sont réglés comme suit. Si le serveur n'est pas synchronisé ou vient d'être mis sous tension, tous les champs d'horodatage sont mis à zéro, à une exception près. Si le message est une réponse à une demande client reçue précédemment, le champ Horodatage transmis de la demande est copié inchangé dans le champ Horodatage d'origine de la réponse. Il est important que ce champ soit copié intact, car un client NTP ou SNTP l'utilise pour éviter les messages erronés.

Si le serveur est synchronisé, l'horodatage de référence est réglé à l'heure de la réception de la dernière mise à jour de la part de la source de référence. Le champ Horodatage d'origine est réglé comme dans le cas de non synchronisation ci-dessus. Le champ horodatage transmis est mis à l'heure à laquelle le message a été envoyé. Dans les messages en diffusion, le champ Horodatage reçu est réglé à zéro et recopié du champ Horodatage transmis dans les autres messages. Le tableau suivant résume ces actions.

Nom du champ	Demande en envoi individuel/multiple	Réponse en envoi individuel/multiple	Diffusion
LI	ignorer	comme nécessaire	comme nécessaire
VN	1-4	copié de la demande	4
Mode	3	4	5
Strate	ignorer	1	1
Interrogation	ignorer	copié de la demande	log2 de l'intervalle d'interrogation
Précision	ignorer	-log2 des bits significatifs du serveur	-log2 des bits significatifs du serveur
Délai de racine	ignorer	0	0
Dispersion de racine	ignorer	0	0
Identifiant de référence	ignorer	identifiant de la source	identifiant de la source
Horodatage de référence	ignorer	heure de la dernière mise à jour de la source	heure de la dernière mise à jour de la source
Horodatage d'origine	ignorer	copié de l'horodatage transmis	0
Horodatage reçu	ignorer	heure du jour	0
Horodatage transmis	(voir le texte)	heure du jour	heure du jour
Authentificateur	facultatif	facultatif	facultatif

La plupart des clients ont une certaine latitude pour pardonner les horodatages invalides, comme il peut en survenir lorsque le serveur vient d'être mis sous tension ou durant les périodes où la source de référence est inopérante. Le plus important indicateur d'un serveur en mauvaise santé est le champ Strate, dans lequel une valeur de 0 indique un état de non synchronisation. Lorsque cette valeur est affichée, les clients devraient éliminer le message du serveur, sans considération du contenu des autres champs.

7. Configuration et gestion

L'établissement initial des serveurs et clients SNTP peut être fait en utilisant un client sur la Toile, s'if en est de disponible, ou sinon, un accès en série. Certains espéraient que la gestion de service des serveurs et clients NTP et SNTPv4 pourrait être effectuée en utilisant SNMP et une MIB convenable à publier, et ceci est arrivé dans certains serveurs SNTP commerciaux. Mais les moyens qui ont été utilisés pendant les vingt dernières années et seront probablement utilisés dans les vingt prochaines est le protocole de contrôle et de surveillance de NTP défini dans la RFC 1305. Normalement, les serveurs et clients SNTP sont supposés fonctionner avec peu ou pas du tout de configuration spécifique du site, autre que de spécifier l'adresse IP du client, le gabarit de sous-réseau, et le routeur.

Les clients en envoi individuel doivent recevoir un ou plusieurs noms ou adresses IP de serveurs désignés. Si plus d'un serveur est fourni, l'un peut être utilisé pour le fonctionnement actif et un des autres pour la sauvegarde si celui qui est actif devait avoir une défaillance ou subir une condition d'erreur. Il n'est normalement pas utile d'utiliser plus d'un serveur à la fois, car avec les millions d'appareils à capacité SNTP prévus dans le proche futur, une telle utilisation représenterait une charge non nécessaire des ressources du réseau et des serveurs.

Les serveurs de diffusion et les clients de multi envoi doivent être approvisionnés avec le TTL et l'adresse de diffusion locale ou de groupe de diffusion groupée. Les serveurs d'envoi individuel et de multi envoi et les clients de diffusion peuvent être configurés avec une liste de paires adresse-gabarit pour le contrôle d'accès, de sorte que seuls les clients ou serveurs connus pour être de confiance soient acceptés. Les serveurs et clients de diffusion groupée doivent mettre en œuvre le protocole IGMP et recevoir aussi l'adresse de diffusion locale ou l'adresse de groupe de diffusion groupée. Les données de configuration pour l'authentification cryptographique sortent du domaine d'application du présent mémoire.

Plusieurs scénarios fournissent la découverte automatique et la sélection du serveur pour les clients SNTP sans configuration de serveur pré spécifiée. Par exemple, un serveur de rôle avec CNAME tel que pool.ntp.org retourne une liste aléatoire d'adresses de serveurs secondaires volontaires, et le client peut en choisir un ou plusieurs comme candidats. Pour un sous-réseau IP ou un segment de LAN qui comporte un serveur NTP ou SNTP, les clients SNTP peuvent être configurés comme clients de diffusion. La même approche peut être utilisée avec des serveurs et clients de diffusion groupée. Dans les deux cas, la fourniture d'une liste de contrôle d'accès est une bonne façon de s'assurer que seules des sources de confiance peuvent être utilisée pour régler l'horloge système.

Dans un autre scénario convenable pour un réseau étendu avec des délais de propagation réseau significatifs, les clients peuvent être configurés pour des adresses de multi envoi, à la fois pour le démarrage initial et après un certain temps lorsque la source de multi envoi actuellement choisie n'a plus été entendue. Suivant le protocole défini, le client se lie au serveur duquel la première réponse est reçue et continues à fonctionner en mode d'envoi individuel.

8. Le paquet du baiser de la mort

Dans l'Internet turbulent d'aujourd'hui, il est impératif que des moyens soient disponibles pour dire à un client d'arrêter de faire des demandes et d'aller voir ailleurs. Une expérience récente a impliqué un grand nombre de routeurs domestiques/d'affaires tous configurés pour utiliser un serveur d'heure d'une université particulière. Dans certaines conditions d'erreur, une fraction substantielle de ces routeurs envoyaient des paquets à des intervalles d'une seconde. La pointe de trafic résultante était spectaculaire, et des mesures extrêmes ont été nécessaires pour diagnostiquer le problème et le mettre sous contrôle. La conclusion est que les clients doivent respecter les moyens disponibles sur les serveurs cibles pour les empêcher d'envoyer des paquets.

Selon la spécification de NTP, la RFC 1305, si le champ Strate de l'en-tête NTP est 1, ce qui indique un serveur principal, le champ Identifiant de référence contient une chaîne ASCII qui identifie le type particulier d'horloge de référence. Cependant, rien dans la RFC 1305 n'est dit sur le champ Identifiant de référence si le champ Strate est à 0, qui est alors qualifié de "non spécifié". Cependant, si le champ Strate est à 0, le champ Identifiant de référence peut être utilisé pour convoyer des messages utiles pour les rapports d'état et le contrôle d'accès. Dans NTPv4 et SNTPv4, les paquets de cette sorte sont appelés paquets Baiser de la mort (KoD, *Kiss-o'-Death*), et les messages ASCII qu'ils portent sont appelés codes de baiser. Les paquets KoD tirent leur nom d'une ancienne utilisation pour dire aux clients d'arrêter d'envoyer des paquets qui violent les contrôles d'accès du serveur.

En général, un client SNTP devrait arrêter d'envoyer à un serveur particulier si ce serveur retourne une réponse avec un champ Strate de 0, sans considération du code de baiser, et qu'un serveur de remplacement est disponible. Si aucun serveur de remplacement n'est disponible, le client devrait retransmettre en utilisant un algorithme de retard exponentiel qui est décrit au paragraphe suivant.

Les codes de baiser peuvent fournir des informations utiles à un client intelligent. Ces codes sont codés dans des chaînes ASCII de quatre caractères justifiés à gauche et remplis de zéros. Les chaînes sont conçues pour l'affichage des caractères et les fichiers de connexion. Normalement, seuls quelques uns de ces codes peuvent survenir chez les clients SNTP, en particulier DENY, RSTR, et RATE. Les autres ne surviennent que plus rarement, en particulier INIT et STEP, lorsque le serveur est dans une condition temporaire particulière . La Figure 3 donne une liste des codes de baiser actuellement définis dans un simple but d'information ; cette liste pourra être modifiée ou étendue à l'avenir.

Code	Signification
ACST	L'association appartient à un serveur d'envoi individuel
AUTH	L'authentification du serveur a échoué
AUTO	La séquence d'auto codage a échoué
BCST	L'association appartient à un serveur de diffusion
CRYP	L'authentification cryptographique ou l'identification a échoué
DENY	Accès refusé par le serveur distant
DROP	Homologue perdu en mode symétrique
RSTR	Accès refusé à cause d'une politique locale
INIT	l'association n'a pas encore été synchronisée pour la première fois
MCST	L'association appartient à un serveur de multi envoi
NKEY	Pas de clé trouvée. Soit la clé n'a jamais été installée soit elle n'est pas de confiance
RATE	Débit dépassé. Le serveur a temporairement refusé l'accès parce que le client excède le seuil de débit
RMOT	Quelqu'un tripote l'association depuis un hôte distant avec ntpdc. Il n'y a pas à s'inquiéter sauf si un fripon a volé vos clés
STEP	Un changement de pas est survenus dans l'heure système, mais l'association n'a pas encore été resynchronisée

Figure 3 : Codes de baiser

9. Être un bon citoyen du réseau

SNTP et son grand frère NTP ont subi une croissance explosive ces dernières années, reflétant la croissance de l'Internet. Tout appareil Internet a une forme de prise en charge de NTP, que ce soit Windows XP, les routeurs de Cisco, les contrôleurs incorporés, et les systèmes de logiciels de toutes sortes. C'est la première édition de la RFC de SNTP où il est devenu nécessaire de poser des règles d'engagement sous forme de critère de conception pour les mises en œuvre de client SNTP. Ceci est nécessaire pour éduquer les développeurs de logiciels en ce qui concerne le bon usage des ressources de serveur horaire de l'Internet alors que l'Internet est en pleine expansion et que la demande sur les serveurs de l'heure augmente, pour empêcher que la sorte de problèmes mentionnés plus haut ne devienne récurrente.

10. Bonnes pratiques

Les clients NTP et SNTP peuvent consommer des ressources considérables de réseau et de serveur si ils ne sont pas de bons citoyens du réseau. Il y a maintenant des appareils consommateurs des commodités de l'Internet qui se comptent par millions et qui sont des consommateurs potentiels des serveurs public et privés NTP et SNTP. L'expérience récente suggère fortement que les concepteurs d'appareils prêtent une attention particulière à la minimisation de l'impact sur les ressources, en particulier si de grands nombres de ces appareils sont déployés. La plus importante considération de la conception est l'intervalle entre les demandes de client, appelé l'intervalle d'interrogation. Il est extrêmement important que le concepteur utilise l'intervalle d'interrogation maximum cohérent avec la précision acceptable.

1. Un client NE DOIT sous aucune condition utiliser un intervalle d'interrogation inférieur à 15 secondes.

2 Un client DEVRAIT augmenter l'intervalle d'interrogation en utilisant le retard exponentiel que permettent les performances et en particulier si le serveur ne répond pas dans un délai raisonnable.

3. Un client DEVRAIT utiliser les serveurs locaux chaque fois qu'ils sont disponibles pour éviter du trafic non nécessaire sur les cœurs de réseau.

4. Un client DOIT permettre à l'opérateur de configurer les noms ou adresses de serveur principal et/ou de remplacement

en plus ou à la place d'une adresse IP par défaut de microcode.

5. Si une adresse IP de serveur par défaut de microcode est fournie, elle DOIT être celle d'un serveur géré par le fabricant ou le vendeur de l'appareil ou un autre serveur, mais seulement avec la permission de l'opérateur.

6. Un client DEVRAIT utiliser le système des noms de domaines (DNS) pour résoudre les adresses IP de serveur, de sorte que l'opérateur puisse faire un équilibrage de charge efficace entre l'ensemble des serveurs et changer les liens d'adresse IP en noms canoniques.

7. Un client DEVRAIT recommencer la résolution d'adresse IP du serveur à intervalles périodiques, mais pas à des intervalles inférieurs à la valeur du champ Durée de vie de la réponse du DNS.

8. Un client DEVRAIT prendre en charge le mécanisme NTP d'accès-refus de telle sorte qu'une réplique de baiser de la mort d'un serveur en réponse à une demande d'un client cause la cessation de l'envoi de demandes du client à ce serveur et son passage à un serveur de remplacement, s'il en est de disponible.

L'algorithme qui suit peut être utilisé comme canevas pour des mises en œuvres spécifiques. Il utilise les variables suivantes :

Temporisateur : C'est un compteur qui se décrémente à un taux fixé. Lorsque il atteint zéro, un paquet est envoyé, et le temporisateur est initialisé avec la durée prévue pour le prochain paquet.

Temporisation maximum : C'est la durée de temporisation maximum déterminée d'après la tolérance de fréquence de l'oscillateur et la précision requise.

Nom de serveur : C'est le nom DNS du serveur. Il peut y en avoir plus d'un, à choisir selon un algorithme non examiné ici.

Adresse IP du serveur : C'est l'adresse IPv4, IPv6 ou OSI du serveur.

Si le microcode ou la documentation comporte des noms de serveur spécifiques, les noms devraient être ceux que le fabricant ou le vendeur utilise pour la commodité des utilisateurs ou ceux pour lesquels une permission spécifique a été obtenue de l'opérateur. Une demande au DNS sur un nom de serveur générique, tel que ntp.mytimeserver.com devrait résulter en un choix aléatoire des adresses IP de serveur disponibles à cette fin. Chaque fois qu'une demande est reçue au DNS, une nouvelle liste aléatoire est retournée. Le client utilise ordinairement la première adresse de la liste.

Lorsque les serveurs SNTP ou NTP candidats sont choisis, il est impératif de respecter les conditions d'accès de l'opérateur du serveur. Les listes de serveurs publics et leurs conditions d'accès sont disponibles à www.ntp.org. Un schéma semi-automatique de découverte de serveur utilisant le DNS est décrit sur ce site. Certains FAI gèrent des serveurs publics, bien que les trouver via leurs aide en ligne puisse être difficile.

Un client modèle fonctionne comme suit (noter que les étapes 2 à 4 constituent une boucle de synchronisation) :

1. Considérer la tolérance de fréquence spécifiée de l'oscillateur de l'horloge système. Définir la précision requise de l'horloge système, puis calculer la temporisation maximum. Par exemple, si la tolérance de fréquence est de 2 pour 10 000 et que la précision requise est d'une minute, la temporisation maximum est d'environ 3,5 jours. Utiliser la temporisation maximum la plus longue possible étant données les contraintes du système pour minimiser la charge agrégée du serveur de l'heure, mais ne la rendre jamais inférieure à 15 minutes.

2 Lorsque le client s'active pour la première fois, ou après une réinitialisation, rendre la temporisation aléatoire entre une et cinq minutes. Ceci est destiné à minimiser le choc lorsque 3000 PC sont réinitialisés au même moment quand le courant est rétabli après une coupure. Supposer à ce moment que l'adresse IP est inconnue et que l'horloge système n'est pas synchronisée. Autrement, utiliser la valeur de temporisation calculée dans les étapes précédentes de la boucle. Noter qu'il peut être nécessaire de se refreiner de mettre en œuvre le délai aléatoire susmentionné pour certaines classes de certification de l'association internationale de sécurité informatique (ICSA, *International Computer Security Association*).

3. Lorsque le temporisateur atteint zéro, si l'adresse IP n'est pas connue, envoyer un paquet d'interrogation du DNS ; autrement, envoyer un paquet de demande NTP à cette adresse. Si aucun paquet de réponse n'a été entendu depuis la dernière expiration de la temporisation, doubler la durée de la temporisation, mais ne pas la rendre supérieure à la temporisation maximum. Si les serveurs principaux et secondaires de l'heure ont été configurés, alterner les interrogations entre le serveur principale et les serveurs secondaires lorsque on ne réussit pas à recevoir de réponse.

4 Si un paquet de réponse du DNS est reçu, sauvegarder l'adresse IP et continuer à l'étape 2. Si un paquet KoD est reçu,

retirer ce serveur de l'heure de la liste, active le serveur secondaire de l'heure, et continuer à l'étape 2. Si un paquet reçu échoue aux vérifications de bonne santé, éliminer ce paquet et continuer à l'étape 2. Si un paquet NTP valide est reçu, mettre à jour l'horloge système, régler la temporisation au maximum, et continuer à l'étape 2.

11. Considérations pour la sécurité

Sans authentification cryptographique, le service SNTPv4 est vulnérable à la perturbation par des serveurs SNTP ou NTP hostiles ou qui se conduisent mal quelque part ailleurs dans l'Internet. Il est vivement recommandé que des moyens de contrôle d'accès et/ou d'authentification cryptographiques soient fournis pour une sécurité supplémentaire. Le présent document comporte des dispositions protocolaires pour ajouter de tels mécanismes de sécurité, mais il ne définit pas les mécanismes eux-mêmes. Un document distinct [MIL03] en préparation définira des mécanismes de sécurité cryptographiques pour SNTP.

12. Remerciements

Jeff Learman a aidé à développer le modèle OSI pour ce protocole. Ajit Thyagarajan a fourni des suggestions et des corrections précieuses.

13. Contributeurs

D. Plonka
J. Montgomery

14. Références informatives

[BRA97] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", RFC 2119, BCP 14, mars 1997.

[COL94] R. Colella, R. Callon, E. Gardner et Y. Rekhter, "Lignes directrices pour allocations de NSAP OSI dans l'Internet", RFC 1629, mai 1994. *(D.S.)*

[DEE89] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", RFC 1112, STD 5, août 1989.

[DEE98] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", RFC 2460, décembre 1998. *(MàJ par 5095, D.S)*

[DOB91] J. Shue et autres, "Services OSI de transport sans connexion par dessus UDP, version 1", RFC 1240, juin 1991. *(Historique)*

[FUR94] P. Furniss, "Séquences d'octets pour les couches supérieures OSI pour la prise en charge d'applications de communications de base", RFC 1698, octobre 1994. *(Information)*

[ISO86] Norme internationale 8602 – "Systèmes de traitement de l'information – OSI : Spécification du protocole de transport sans connexion". Organisation internationale de normalisation, décembre 1986.

[MIL92] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", RFC 1305, STD 12, mars 1992.

[MIL03] Mills, D., "The Autokey Security Architecture, Protocol and Algorithms", http://eecis.udel.edu/~mills/database/reports/stime/stime.pdf, August 2003.

[PAR93] C. Partridge, T. Mendez, W. Milliken, "Service d'envoi à la cantonade pour les hôtes", RFC 1546, novembre 1993. *(Information)*

[POS80] J. Postel, "Protocole de datagramme d'utilisateur", RFC 768, (STD 6), 28 août 1980.

[POS83] J. Postel et K. Harrenstien, "Protocole de l'heure", RFC 868, STD 26, mai 1983.

[SRI99] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", RFC 2663, août 1999. *(Information)*

[SRI01] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", RFC 3022, janvier 2001. *(Information)*

Adresse de l'auteur

David L. Mills
Electrical and Computer Engineering Department
University of Delaware
Newark, DE 19716
téléphone : (302) 831-8247
mél : mills@udel.edu

Déclaration de copyright

Propriété intellectuelle

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.