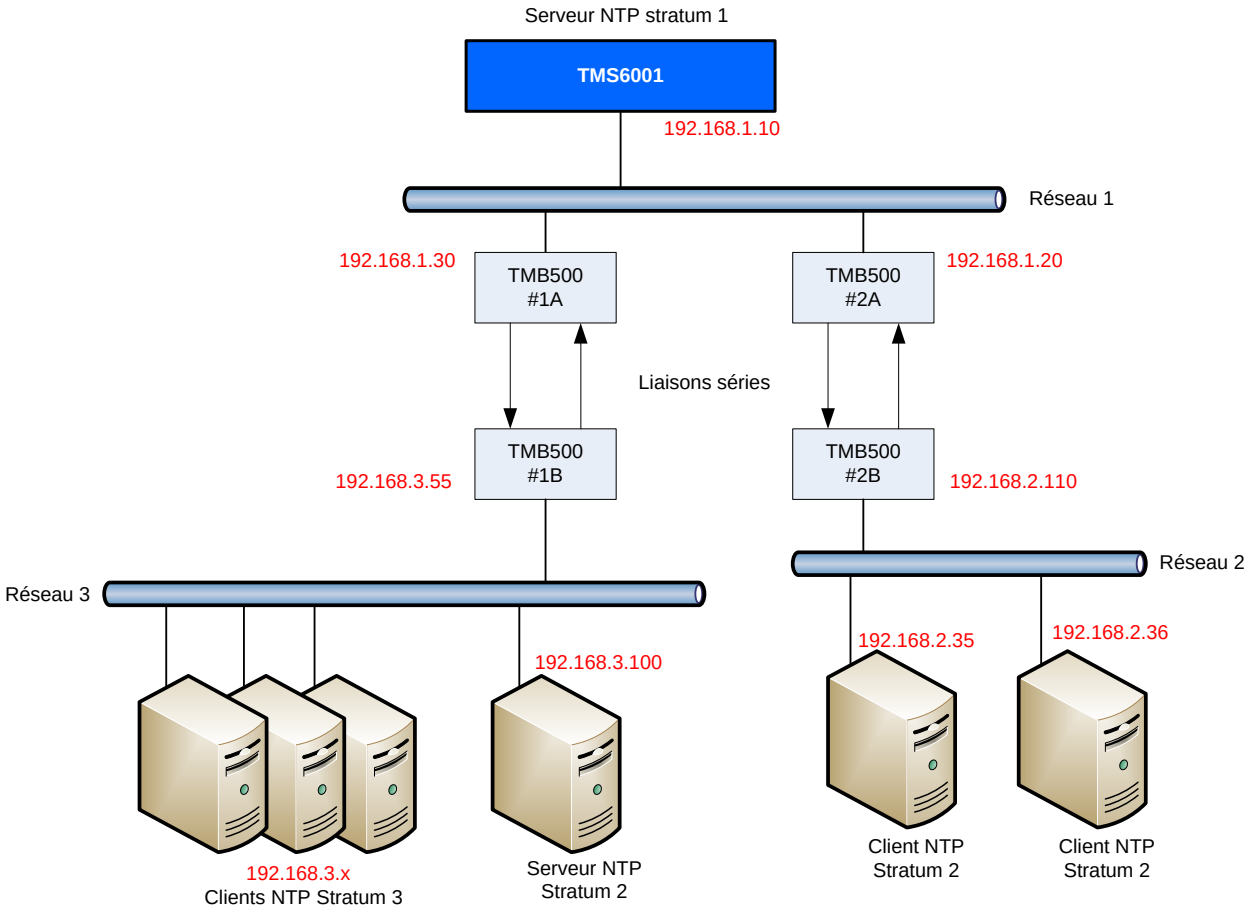
Ligne de produits sécurisés
Note d'application TMB500

Mise en œuvre d'un serveur NTP dans un environnement sécurisé

Cette note d'application montre la mise en œuvre d'un serveur NTP primaire sur un réseau recevant des requêtes NTP de clients situés sur deux autres réseaux totalement isolés.
Les équipements TMB500 permettent de réaliser des passerelles entre ces réseaux avec une rupture de protocole garantissant l'étanchéité totale entre eux.



Les PC clients NTP sur le réseau 2 émettent directement leurs requêtes vers le serveur NTP primaire TMS6001. Les PC clients NTP sur le réseau 3 émettent leurs requêtes vers le serveur NTP secondaire du réseau 3, ce dernier se synchronise sur le serveur NTP primaire TMS6001.

Le tableau ci-dessous donne la configuration du service ntp (fichier ntp.conf pour les PC sous linux) pour chacun des équipements.

Réseau	Equipement	Configuration NTP
Réseau 2	Clients NTP	Server 192.168.2.110 (*)
Réseau 3	Serveur NTP stratum 2	Server 192.168.3.55 (*)
Réseau 3	Clients NTP	Server 192.168.3.100

(*) On constate que l'adresse IP du serveur TMS6001 n'est pas connue des réseaux 2 et 3, le serveur y est représenté par le TMB500 relié au réseau correspondant

.

Au niveau de chaque TMB500, les routes sont définies comme indiqué dans le tableau suivant.

Equipement	Route	IP autorisée	Port source	Port de destination
TMB500 #1A	1	192.168.1.10	123	123
TMB500 #1B	1	192.168.3.100	123	123
TMB500 #2A	1	192.168.1.10	Random 1	123
	2	192.168.1.10	Random 2	123
TMB500 #2B	1	192.168.2.35	123	123
	2	192.168.2.36	123	123

Note : Pour différencier les requêtes venant des deux clients NTP du réseau 2, le TMB500 #2A émet les requêtes vers le TMS6001 avec des numéros de port source aléatoires, le port par défaut 123 n'est pas utilisable dans ce cas.

En régime établi, un client NTP linux émet des requêtes avec des intervalles de temps croissants au fur et à mesure que la précision de la synchronisation s'améliore. Ces intervalles sont successivement de 64, 126, 256, 512 et 1024 secondes. La limitation de la bande passante introduite par la rupture de protocole (maximum 100 échanges NTP / seconde) n'est donc pas un problème pour ce genre d'architecture.
Généralement, lorsqu'il y a un nombre important de clients NTP, ces derniers se synchronisent sur une machine locale au réseau, elle-même synchronisée sur le serveur primaire.