

# STUN (Serial Tunneling) - FAQ

## Contenu

[Quelle adresse dois-je utiliser pour définir l'instruction STUN \(Serial Tunneling\) peer-name ?](#)

[Pourquoi mon nom d'homologue STUN \(Serial Tunneling\) est-il fermé ?](#)

[Pourquoi et quand différents groupes de tunnellation série \(STUN\) sont-ils utilisés ?](#)

[Après avoir configuré l'encapsulation STUN \(Serial Tunneling\) sur l'interface, comment supprimer cette fonctionnalité ? L'encapsulation ? ? ? no stun ? ? ne fonctionne pas.](#)

[Pourquoi devons-nous utiliser une boîte de dérivation pour lier RTS \(Request To Send\) et DTR \(Data Terminal Ready\) ensemble pour maintenir l'interface STUN \(Serial Tunneling\) active ?](#)

[Comment dois-je hiérarchiser le trafic STUN \(Serial Tunneling\) ?](#)

[La tunnellation série \(STUN\) peut-elle fonctionner sur un cloud SMDS \(Switched Multimegabit Data Service\), Frame Relay ou X.25 ?](#)

[Pourquoi la commutation lente entre des liaisons de 56 kbits/s est-elle recommandée par rapport à la commutation rapide ?](#)

[Dans la sortie d'une commande \*\*debug stun packet\*\*, que signifient SDI et NDI ?](#)

[Informations connexes](#)

**Q. Quelle adresse dois-je utiliser pour définir l'instruction STUN (Serial Tunneling) peer-name ?**

A. Vous pouvez utiliser n'importe quelle adresse IP d'une interface active dans le routeur. Cependant, vous devez utiliser l'adresse IP de l'interface la plus stable, qui est l'adresse de bouclage.

**Q. Pourquoi mon nom d'homologue STUN (Serial Tunneling) est-il fermé ?**

A. Votre nom d'homologue STUN est fermé car aucune donnée n'a été échangée.

- Si vous utilisez l'encapsulation directe, votre interface est désactivée.
- Si vous utilisez l'encapsulation IP, la connexion IP entre les deux homologues n'est pas active soit parce qu'il n'y a pas de connectivité IP, soit parce qu'aucun des deux périphériques n'a tenté d'envoyer des données sur le canal.

**Q. Pourquoi et quand différents groupes de tunnellation série (STUN) sont-ils utilisés ?**

A. Utilisez différents groupes STUN pour différencier le trafic des processeurs frontaux (FEP) qui ont des contrôleurs avec la même adresse.

**Q. Après avoir configuré l'encapsulation STUN (Serial Tunneling) sur l'interface, comment supprimer cette fonctionnalité ? L'encapsulation ? ? ? no stun ? ? ne**

fonctionne pas.

A. Émettez la commande `hdlc encapsulation`, qui rétablira l'encapsulation par défaut de l'interface.

**Q. Pourquoi devons-nous utiliser une boîte de dérivation pour lier RTS (Request To Send) et DTR (Data Terminal Ready) ensemble pour maintenir l'interface STUN (Serial Tunneling) active ?**

A. À moins que le nouveau mode bidirectionnel non retour à zéro inversé (NRZI) ne soit activé, STUN prend uniquement en charge le mode bidirectionnel simultané ; par cette convention ??? full duplex ??? signifie que RTS et CTS (Clear To Send) sont toujours élevés. Le fait de fixer les broches RTS et DTR ensemble permet de maintenir la hauteur RTS en permanence.

**Q. Comment dois-je hiérarchiser le trafic STUN (Serial Tunneling) ?**

A. Hiérarchisez le trafic STUN pour le logiciel Cisco IOS version 9.1 et ultérieure, comme indiqué ci-dessous.

- Suivez la procédure ci-dessous pour une encapsulation série simple. Utilisez la commande suivante:

```
priority-list x stun {high|medium|normal|low}
      address stun_group controller_address
!--- The above command is entered on one line.
```

Attribuez le groupe de priorités à l'interface de sortie.

- Pour l'encapsulation TCP, il existe maintenant quatre ports, répertoriés ci-dessous, au lieu d'un port, comme dans le logiciel précédent.

```
1994 : high priority
1990 : medium priority
1991 : normal priority
1992 : low priority
```

Ainsi, pour hiérarchiser le trafic, codez d'abord le port STUN, puis utilisez la commande **priority-list** pour assigner la hiérarchisation. Par exemple, configurez la liste de priorité pour STUN sur l'interface **série 1** avec l'adresse de contrôleur **C1** comme indiqué ci-dessous.

```
priority-list 1 protocol ip high tcp 1994
priority-list 1 protocol ip medium tcp 1990
priority-list 1 protocol ip normal tcp 1991
priority-list 1 protocol ip low tcp 1992
priority-list 1 stun high address 1 C1
interface s 1
encapsulation stun
stun group 1
stun route address C1 tcp 131.108.64.250
      local-ack priority
!--- The above command is entered on one line.
```

```
interface serial 2
priority-group 1
!--- Note: This is the WAN interface.
```

**Remarque :** L'instruction **priority-group** est appliquée à l'interface WAN sur laquelle le trafic STUN est tunnelisé, *pas* à l'interface STUN elle-même.

**Q. La tunnellation série (STUN) peut-elle fonctionner sur un cloud SMDS (Switched Multimegabit Data Service), Frame Relay ou X.25 ?**

A. Oui, si vous utilisez l'encapsulation TCP. Après l'encapsulation, le paquet sera comme un paquet IP ordinaire, et il sera routé sur X.25, Frame Relay ou SMDS comme trafic IP normal.

**Q. Pourquoi la commutation lente entre des liaisons de 56 kbits/s est-elle recommandée par rapport à la commutation rapide ?**

A. Dans la plupart des cas, la commutation rapide place les paquets dans la file d'attente de sortie trop rapidement pour la liaison de 56 kbits/s, et les paquets sont abandonnés si aucun tampon de sortie ne peut être alloué. Lorsqu'un paquet tombe en panne, le protocole TCP tente de retransmettre le paquet, qui utilise beaucoup de cycles CPU. Par conséquent, avec une liaison de 56 kbits/s ou plus lente, il est généralement recommandé d'arrêter la commutation rapide.

**Q. Dans la sortie d'une commande debug stun packet, que signifient SDI et NDI ?**

A. Reportez-vous à l'[explication de SDI et NDI à partir d'une commande debug stun packet](#) pour connaître la signification de SDI (Serial Data Input) et NDI (Network Data Input).

## [Informations connexes](#)

- [Support technique - Cisco Systems](#)