

Configuration des protocoles IP/PPP pour l'accès téléphonique des serveurs d'accès avec PPP V.120 dédié

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Comment V.120 affecte les performances du routeur](#)

[Pourquoi implémenter PPP sur V.120 ?](#)

[Configuration](#)

[Interfaces virtuelles-asynchrones \(vty-async\)](#)

[Modèles virtuels](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Vérification de la connexion V.120](#)

[Vérifier V.120 en mode non PPP](#)

[Dépannage](#)

[Commandes de dépannage \(facultatif\)](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration pour l'accès IP/PPP commuté du serveur avec PPP V.120 dédié

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Logiciel Cisco IOS® Version 11.2 ou ultérieure, pour V.120 avec interfaces asynchrones virtuelles.
- Logiciel Cisco IOS Version 11.3 ou ultérieure, pour V.120 avec modèles virtuels.
- Image d'entreprise Cisco IOS pour la configuration de plus de cinq lignes VTY.

Utilisez l'[outil Software Advisor](#) (clients [enregistrés](#) uniquement) pour déterminer quels jeux de fonctions du logiciel Cisco IOS prennent en charge la fonctionnalité V.120. Dans l'outil, sélectionnez les fonctions suivantes : Support V.120, traduction de protocole et modèles virtuels pour la traduction de protocole. Si vous avez besoin de fonctions supplémentaires, sélectionnez-les selon les besoins.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

[Informations générales](#)

La Recommandation V.120 de l'UIT (International Telecommunication Union Telecommunication Standardization Sector) permet un transport fiable de données synchrones, asynchrones ou transparentes sur les canaux de transmission RNIS.

Une connexion V.120 peut être en mode PPP ou non PPP. En effet, de nombreuses cartes de terminal V.120 sont similaires aux modems et prennent en charge certains jeux de commandes AT. Le mode non PPP peut être utilisé pour vérifier si la configuration V.120 est correcte sur le client et le routeur. PPP peut ensuite être configuré sur cette liaison. Pour plus d'informations, reportez-vous à la section [Verify V.120 in non-PPP mode](#).

Il existe deux méthodes principales pour implémenter V.120 :

- **Interfaces virtuelles-asynchrones** Grâce au logiciel Cisco IOS, vous pouvez configurer des fonctions de protocole asynchrones, telles que PPP et SLIP, sur des lignes VTY. Les protocoles PPP et SLIP fonctionnent normalement uniquement sur des interfaces asynchrones et non sur des lignes VTY. Lorsque vous configurez une ligne VTY pour prendre en charge les fonctions de protocole asynchrone, vous créez des interfaces Virtual-Asynchronous sur les lignes VTY. Une interface virtuelle-asynchrone (également appelée vty-async) est créée pour prendre en charge les appels qui entrent dans le routeur via une interface non physique. Par exemple, les appels de flux de caractères asynchrones se terminent ou se posent sur des interfaces non physiques. Les interfaces virtuelles-asynchrones ne sont pas configurables par l'utilisateur ; elles sont plutôt créées dynamiquement et détruites à la demande.
- **Modèles virtuels** La mise en oeuvre Virtual-Template prend en charge la transmission tunnel du protocole PPP, en utilisant une traduction de protocole en deux étapes. Lorsqu'un utilisateur V.120 compose un numéro à l'aide d'une ligne de terminal virtuel, le routeur crée

une interface d'accès virtuelle. L'interface d'accès virtuel est une interface temporaire qui prend en charge la configuration de protocole asynchrone spécifiée dans le modèle d'interface virtuelle. Cette interface est créée dynamiquement en clonant l'interface Virtual-Template dans la configuration. Cette interface d'accès virtuel est libérée dès que la connexion est interrompue. Le modèle virtuel est plus flexible, car il offre plus d'options de configuration que la mise en oeuvre Virtual-Asynchronous limitée.

[Comment V.120 affecte les performances du routeur](#)

Cisco ne vous recommande pas d'exécuter PPP sur V.120 sur Micamodem, car le traitement V.120 nécessite énormément de CPU. Un Cisco AS5200 ne peut pas gérer de nombreuses connexions PPP V.120 actives simultanément. Les autres routeurs AS5xxx peuvent gérer des connexions PPP V.120 plus actives simultanément. Cisco recommande également de configurer l'adaptateur de terminal RNIS (TA) client pour effectuer une conversion PPP synchrone-asynchrone afin que la connexion entre dans le serveur d'accès au réseau (NAS) en tant que protocole PPP synchrone normal au lieu de V.120.

Cependant, avec les modems Nextport, une nouvelle fonctionnalité a été ajoutée pour décharger les appels V.120 vers le processeur de signal numérique (DSP) du modem. Si vous utilisez le logiciel Cisco IOS Version 12.2 XB (et 12.2(11)T et ultérieure), il est possible de terminer les appels V.120 sur le DSP NextPort au lieu du CPU. Pour plus d'informations, consultez [Terminating V.120 Sessions on the NextPort DSP](#).

[Pourquoi implémenter PPP sur V.120 ?](#)

Le protocole PPP sur V.120 consomme beaucoup de CPU. Par conséquent, Cisco décourage une mise en oeuvre étendue. Cependant, vous pouvez exécuter PPP sur V.120 pour les raisons suivantes :

- Vous utilisez une carte de terminal (TA) connectée à un équipement terminal de données asynchrone (ETTD) et ne peut pas effectuer de conversion PPP synchrone-asynchrone. Dans ce cas, vous devez utiliser V.120.
- La configuration par défaut de votre adaptateur de terminal est V.120 et vous ne pouvez pas reconfigurer votre adaptateur de terminal sans l'aide de votre fournisseur d'accès Internet (FAI).
- L'application souhaite que la session PPP démarre avec une boîte de dialogue de terminal à cellules de caractères (par exemple, un défi de mot de passe et une réponse uniques), de sorte que vous ne voulez pas d'une session PPP de synchronisation pure.

[Configuration](#)

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

Cette section décrit également la mise en oeuvre des modèles VTY-async et Virtual-Templates.

Remarque : ces étapes supposent que le NAS est correctement configuré pour l'accès RNIS ou Async Dialin de base et que le client est correctement configuré pour PPP sur V.120.

Interfaces virtuelles-asynchrones (vty-async)

Pour implémenter vty-async, procédez comme suit :

1. Créez des interfaces virtuelles-asynchrones à l'aide de la commande de configuration globale **vty-async**.
2. Configurez l'authentification pour la connexion vty-async. Utilisez l'autorité **ppp vty-async {chap | pap}**.
3. Configurez d'autres paramètres vty-async, tels que les compteurs keepalive, la taille mtu, la compression d'en-tête, etc., si nécessaire, pour votre configuration. Référez-vous à [Traduction de protocole et commandes de périphérique asynchrone virtuel](#) pour plus d'informations.
4. Configurez la détection automatique de l'encapsulation V.120 à l'aide de la commande **autodetect encapsulation v120 ppp**. Cette commande doit être appliquée à l'interface physique de l'appel entrant (par exemple, interface BRI 0, interface Serial 1:23). Cependant, si le V.120 TA appelant signale correctement V.120 dans le champ de compatibilité de bas niveau Q.931 SETUP, l'encapsulation de détection automatique n'est pas nécessaire. Malheureusement, de nombreux assistants sociaux ne parviennent pas à le faire.
5. Désactivez l'invite Nom d'utilisateur et Mot de passe sous la configuration de ligne VTY. Pour ce faire, vous pouvez configurer **no login** et **no password** en mode de configuration de ligne VTY. Si vous utilisez AAA, définissez une liste dont la méthode n'est pas définie, puis appliquez-la à l'interface VTY. Exemple :

```
maui-soho-01(config)#aaa new-model
maui-soho-01(config)#aaa authentication login NO_AUTHEN none
maui-soho-01(config)#line vty 0 4
maui-soho-01(config-line)#login authentication NO_AUTHEN
```
6. Configurez la commande **autocommand ppp default** en mode de configuration de ligne VTY. Sans authentification de connexion et **autocommand ppp**, le VTY lance PPP dès qu'une connexion V.120 arrive. Cela permet à l'homologue V.120 de commencer immédiatement les négociations PPP, sans avoir à exécuter un script, ou d'entrer un nom d'utilisateur et un mot de passe dans une fenêtre de terminal. La commande **autoselect** n'est pas prise en charge sur les VTY.**Remarque** : Puisque les VTY commencent à exécuter PPP dès que la connexion est établie, vous ne pourrez pas émettre la commande **telnet** sur le NAS à des fins administratives. Pour contourner cette restriction, appliquez la commande **transport input v120** sur les VTY utilisés pour les connexions PPP V.120, et appliquez la commande **transport input telnet** sur celles utilisées pour le telnet administratif.

Modèles virtuels

Pour mettre en oeuvre des modèles virtuels, procédez comme suit :

1. Créez et configurez un modèle d'interface virtuelle à l'aide de la commande **interface virtual-template**. Configurez cette interface virtuelle de la même manière que vous configureriez une interface série asynchrone régulière. Pour ce faire, affectez au modèle d'interface virtuelle l'adresse IP d'une interface active (à l'aide de la commande **ip unnumbered interface**) et

configurez l'adressage, comme vous le feriez sur une interface asynchrone. Vous pouvez également entrer des commandes en mode de configuration d'interface qui compressent les en-têtes TCP ou configurent l'authentification CHAP (Challenge Handshake Authentication Protocol) pour PPP. Exemple :

```
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPaddressPool
 ppp authentication chap
```

2. Créez des interfaces virtuelles-asynchrones à l'aide de la commande de configuration globale **vty-async**.
3. Configurez des lignes de terminal virtuel pour prendre en charge des fonctions de protocole asynchrones, en fonction de la définition d'un modèle d'interface virtuelle. Pour ce faire, utilisez la commande **vty-async virtual-template number** en mode de configuration globale.

Exemple :

```
vty-async
vty-async Virtual-Template 1
```

4. Configurez la détection automatique de l'encapsulation V.120 à l'aide de la commande **autodetect encapsulation v120 ppp**. Appliquez cette commande à l'interface physique de l'appel entrant (par exemple, interface BRI 0, interface Serial 1:23). Cependant, si le V.120 TA appelant signale correctement V.120 dans le champ de compatibilité de bas niveau Q.931 SETUP, l'**encapsulation de détection automatique** n'est pas requise. Malheureusement, de nombreux assistants sociaux ne parviennent pas à le faire.
5. Désactivez l'invite Nom d'utilisateur et Mot de passe sous la configuration de la ligne vty. Pour ce faire, configurez **no login** et **no password** en mode de configuration de ligne vty. Si vous utilisez AAA, définissez une liste qui a la méthode none et appliquez-la à l'interface vty.

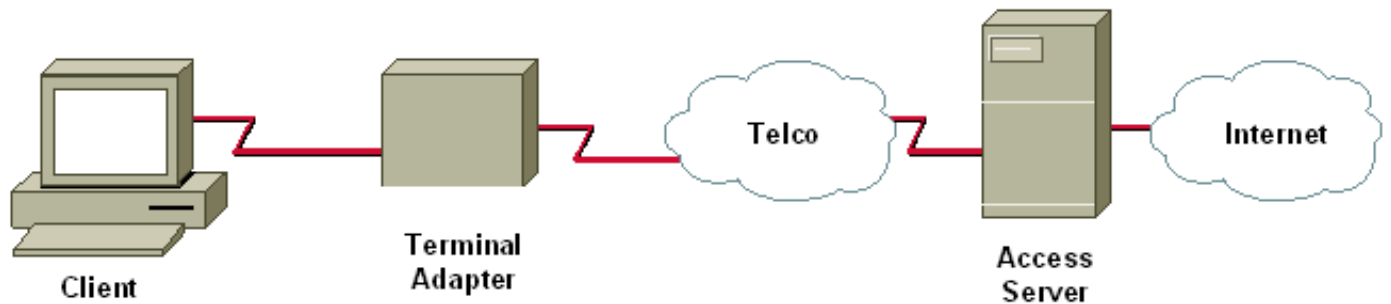
Exemple :

```
maui-soho-01(config)#aaa new-model
maui-soho-01(config)#aaa authentication login NO_AUTHEN none
maui-soho-01(config)#line vty 0 4
maui-soho-01(config-line)#login authentication NO_AUTHEN
```

6. Configurez la commande **autocommand ppp default** en mode de configuration de ligne vty. Sans authentification de connexion et **autocommand ppp**, le VTY lance PPP dès qu'une connexion V.120 arrive. Cela permettra à l'homologue V.120 de commencer immédiatement les négociations PPP, sans avoir à exécuter un script ou à entrer un nom d'utilisateur et un mot de passe dans une fenêtre de terminal. Notez que la commande **autoselect** n'est pas prise en charge sur les VTY. **Remarque** : Puisque les VTY commencent à exécuter PPP dès que la connexion est établie, vous ne pourrez pas émettre la commande **telnet** sur le NAS à des fins administratives. Pour contourner cette restriction, appliquez la commande **transport input v120** sur les VTY utilisés pour les connexions PPP V.120, et appliquez la commande **transport input telnet** sur celles utilisées pour le telnet administratif.

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise la configuration suivante :

- Cisco AS5200 qui prend en charge les clients IP ou PPP commutés pour le protocole PPP RNIS synchrone (non multilaision), le protocole PPP asynchrone et le protocole PPP V.120. Cette configuration utilise la méthode VTY-asynchrone (Virtual-Asynchronous interfaces) décrite ci-dessus.

V.120 (PPP) avec interfaces asynchrones virtuelles

```

aaa new-model
aaa authentication login default local
aaa authentication login NOAUTH none
!--- The aaa list NOAUTH has no authentication. !---
! This list will be applied to the vty interface. !
username fred password FLINTSTONE ! ip local pool
default 10.1.1.2 10.1.1.47 !--- Define local IP address
pool. vty-async !--- Configures all virtual terminal
lines on a router to !--- support asynchronous protocol
features. !--- The vty-async parameters are required for
Async V.120. vty-async keepalive 0 !--- Disable PPP
keepalives. vty-async ppp authen chap pap !--- Async
V.120 PPP authentication methods. ! interface Ethernet0
ip address 10.1.1.1 255.255.255.0 ! interface serial0:23
!--- ISDN D-channel configuration for T1 0. no ip
address encapsulation ppp isdn incoming-voice modem !---
Analog calls are forwarded to the internal digital
modem. ppp authentication chap pap dialer rotary-group 1
!--- Member of rotary group 1. !--- The rotary group
configuration is interface Dialer 1. autodetect
encapsulation v120 ppp !--- Automatic detection of
encapsulation type on the specified interface. !--- This
interface will automatically detect whether the call is
normal PPP or V.120 !--- If the calling V.120 TA
correctly signals V.120 in the Q.931 !--- SETUP low-
level compatibility field, autodetect encapsulation is
!--- not needed. Unfortunately, many TAs fail to do
this. ! interface Dialer1 !--- Rotary group 1 logical
interface. description Dialer interface for sync ISDN
calls ip unnumbered Ethernet0 encapsulation ppp peer
default ip address pool dialer-group 1 dialer idle-
timeout 300 no cdp enable ppp authentication chap pap !
interface Group-Async1 description Interface for async
modem calls async mode dedicated !--- PPP only, no exec
dial-ins (or Teminal window after dial). ip unnumbered
Ethernet0 encapsulation ppp ip tcp header-compression

```

```

peer default ip address pool default dialer-group 1
dialer idle-timeout 300 no cdp enable ppp authentication
chap pap ! dialer-list 1 protocol ip permit ! line con 0
login authentication NOAUTH line 1 48 !--- Modems used
for normal async calls. no exec modem inout ! line vty 0
45 !--- V.120 call will be terminated on vty 0 45. !---
If your router does not support more than five vtys
refer !--- to the Components Used section. login
authentication NOAUTH !--- Use the AAA list NOAUTH
(which specified no authentication) !--- configured
previously with this method. There will be no !---
Username/password exec prompt. Use the no login command
!--- if this NAS does not do AAA.

autocommand ppp default
!--- This command is ONLY required for V.120 with PPP.
session-timeout 5 output !--- Timeout of 5 minutes.
transport input v120 !--- Allow only V.120 connections
into these VTYS. line vty 46 50 !--- These vtys will be
used for normal telnets into the router. login
authentication default !--- Use AAA list "default" for
vty 46-50. !--- This method uses local authentication
(configured previously). exec-timeout 30 transport input
telnet !--- Permit only incoming telnet connections to
use vty 46-50.

```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show ip route** : affiche les entrées de la table de routage IP.
- **show users** : affiche des informations sur les lignes actives du serveur réseau, y compris le numéro de ligne, les noms de connexion et l'emplacement du terminal.

Vérification de la connexion V.120

Pour vérifier la connexion V.120, procédez comme suit :

1. Utilisez **debug v120** et générez un appel V.120 entrant. Vous devriez voir cette sortie de débogage sur le NAS :

```

19:25:16: V120: Autodetect trying to detect V120 mode on Se0:18
19:25:16: V120 sampled pkt: 3 bytes: 8 1 7F
19:25:16: Se0:18-v120 started - Setting default V.120 parameters
19:25:16: V120established handle = 4

```

Si ce message n'apparaît pas, l'appel entrant n'était probablement pas V.120 et le routeur ne l'a donc pas détecté en tant que tel.

2. Vérifiez si l'interface vty-async s'active. Si votre configuration utilise V.120 avec des modèles virtuels, vérifiez si une interface d'accès virtuel est créée. Dans le journal de console suivant, l'interface vty-async 32 est active :

```

19:25:17: %LINK-3-UPDOWN: Interface VTY-Async32,
changed state to up

```

- Utilisez **debug ppp negotiation** et **debug ppp authentication**. pour garantir que les paramètres PPP sont négociés correctement. Pour plus d'informations sur le débogage PPP, consultez [Technologie commutée : Techniques de dépannage](#).
- Exécutez une **commande show ip route** et **show users** pour vérifier que l'appel V.120 est correctement établi.

Les exemples suivants sont des sorties d'une configuration où nous n'avons pas de modèles virtuels V.120 :

```
DSL4-5300A#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```

172.68.0.0/32 is subnetted, 1 subnets
S    172.68.186.41 [1/0] via 172.18.120.1
172.18.0.0/24 is subnetted, 1 subnets
S    172.18.120.0 [1/0] via 10.92.1.1
10.0.0.0/24 is subnetted, 1 subnets
C    10.92.1.0 is directly connected, FastEthernet0
C    192.168.1.0/24 is directly connected, Loopback0
172.0.0.0/32 is subnetted, 1 subnets
C    172.22.53.1 is directly connected, VTY-Async32
```

Remarque : l'appel est connecté à l'interface VTY-Async 32 et il existe une route vers le client.

Remarque : L'adresse IP du côté NAS de la liaison sera celle de l'interface Ethernet ou Fast-Ethernet sur le NAS, lors de l'utilisation de l'option de configuration non Virtual-Template. Par conséquent, vérifiez si l'interface Ethernet ou Fast-Ethernet est activée et peut être envoyée par ping.

```
DSL4-5300A#show users
```

Line	User	Host(s)	Idle	Location
*0 con 0		idle	00:00:00	
32 vty 0	wan-2520-5	VTY-Async32	00:01:37	Serial0:18
Interface	User	Mode	Idle	Peer Address
VT32	wan-2520-5	Async PPP	00:01:14	172.22.53.1

Remarque : l'appel est connecté à l'interface VTY-Async 32 et l'adresse IP de l'homologue est spécifiée.

Si vous utilisez l'option Virtual-Template avec V.120, la sortie **show ip route** et **show user** apparaît comme suit :

```
DSL4-5300A#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
```



```
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.199.0/32 is subnetted, 1 subnets
C    192.168.199.5 is directly connected, Virtual-Access1
172.22.0.0/32 is subnetted, 1 subnets
S    172.22.186.41 [1/0] via 172.18.120.1
10.0.0.0/24 is subnetted, 1 subnets
C    10.20.20.0 is directly connected, Virtual-Access1
.....
```

Remarque : l'appel est connecté à l'interface Virtual-Access 1 et il existe une route vers le client.

```
DSL4-5300A#show users
```

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	
32 vty 0	wan-2520-5	Virtual-Access1	00:00:05	Serial0:18

Remarque : l'appel est connecté à l'interface Virtual-Access 1.

[Vérifier V.120 en mode non PPP](#)

De nombreuses cartes de terminal V.120 sont similaires aux modems et prennent en charge certains jeux de commandes AT. Par conséquent, vous pouvez utiliser le mode non PPP pour vérifier si la configuration V.120 sur le client et le routeur est correcte. Vous pouvez ensuite configurer PPP sur cette liaison. Le test de la V.120 en lui-même nous permet de résoudre des problèmes liés à la V.120 sans ajouter la complexité du protocole PPP.

Pour tester la connexion V.120 en mode non PPP, procédez comme suit :

1. Activez l'invite Nom d'utilisateur et Mot de passe sous la configuration de la ligne vty. Utilisez la commande **login** pour activer la connexion. Utilisez la commande **password password** pour définir le mot de passe de ligne. Si vous utilisez AAA, supprimez la commande **login authentication list** sous vty.
2. Supprimez la commande **autocommand ppp default** en mode de configuration de ligne vty.

Exemple :

```
maui-soho-01(config)#line vty 0 4
maui-soho-01(config-line)#login
maui-soho-01(config-line)#password letmein maui-soho-01(config-line)#no autocommand ppp
default
```

3. Activez **debug v120** et lancez un appel à partir du client. Le routeur doit afficher ce qui suit :
19:25:16: V120: Autodetect trying to detect V120 mode on Se0:18
19:25:16: V120 sampled pkt: 3 bytes: 8 1 7F
19:25:16: Se0:18-v120 started - Setting default V.120 parameters
19:25:16: V120established handle = 4
4. Continuez la configuration V.120. Suivez les étapes décrites dans la section [Configurer](#).

[Dépannage](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Commandes de dépannage (facultatif)

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque : Avant d'émettre des commandes **debug**, reportez-vous à [Informations importantes sur les commandes de débogage](#) pour plus d'informations.

- **debug v120** : indique quand le traitement V.120 est démarré ou terminé, et l'interface sur laquelle il est en cours d'exécution.
- **debug ppp negotiation** - affiche des informations sur le trafic et les échanges PPP, tout en négociant les composants PPP, notamment LCP (Link Control Protocol), Authentication et NCP. Une négociation PPP réussie ouvrira d'abord l'état LCP, puis s'authentifiera, puis négociera finalement NCP (généralement IPCP).
- **debug ppp authentication** - affiche les messages du protocole d'authentification PPP, y compris les échanges de paquets CHAP et les échanges PAP (Password Authentication Protocol).

Informations connexes

- [Configuration de l'accès V.120](#)
- [Commandes d'accès V.120](#)
- [Configuration du trafic asynchrone virtuel sur RNIS](#)
- [Commandes de traduction de protocole et de périphérique asynchrone virtuel](#)
- [Support et documentation techniques - Cisco Systems](#)