

# Xconnect sur VRF Aware L2TPv3 dans ASR1K

## Contenu

–

[Introduction](#)

[Informations générales](#)

[Cas d'essai I : L2TPv3 Xconnect sur réseau IP avec terminaux dans VRF](#)

[Cas d'essai II : L2TPv3 Xconnect sur le réseau MPLS avec des terminaux dans VRF](#)

## Introduction

Ce document décrit comment le VRF (Virtual Routing and Forwarding) peut être utilisé lorsque vous configurez le réseau MPLS (Layer 2 Tunneling Protocol)v3 Xconnect over IP et Multiprotocol Label Switching.

## Informations générales

L2TP est le protocole de tunnellation utilisé par les fournisseurs d'accès Internet (FAI) afin de fournir un réseau privé virtuel (VPN) dans l'espace d'accès commuté sur Internet.

Il combine le meilleur du protocole L2F (Layer 2 Forwarding) de Cisco et le protocole PPTP (Point-to-Point Tunneling Protocol) de Microsoft. Les composants principaux de L2TP sont LAC (L2TP Access Controller) et LNS (L2TP Network Server).

Contrôleur d'accès L2TP : LAC est un serveur d'accès connecté au réseau téléphonique public commuté (RTPC). Le LAC est l'initiateur des appels entrants et le destinataire des appels sortants. Il est connecté à LNS sur LAN ou WAN.

Serveur réseau L2TP : LNS est le serveur réseau du protocole L2TP où les sessions PPP se terminent et sont authentifiées. Le LNS est l'initiateur des appels sortants et le destinataire des appels entrants.

L2TPv2 a été conçu pour transporter le trafic PPP sur des réseaux IP. Les équipements d'accès réseau (DSL, modem câble ou interfaces d'accès à distance) ont accepté les connexions PPP des abonnés et ont tunnelisé les sessions PPP vers le FAI via L2TP. La nouvelle version L2TPv3 est conçue pour transporter toute charge utile de couche 2 en plus de PPP qui était la seule charge utile prise en charge par la version 2. Plus précisément, L2TPv3 définit le protocole L2TP pour la transmission tunnel des charges utiles de couche 2 sur un réseau IP principal avec l'utilisation de VPN de couche 2. Cette fonctionnalité présente les avantages suivants :

- L2TPv3 simplifie le déploiement des VPN
- L2TPv3 ne nécessite pas de MPLS
- L2TPv3 prend en charge le tunneling de couche 2 sur IP pour toute charge utile

Voici un exemple de configuration de pseudowire L2TPv3 :

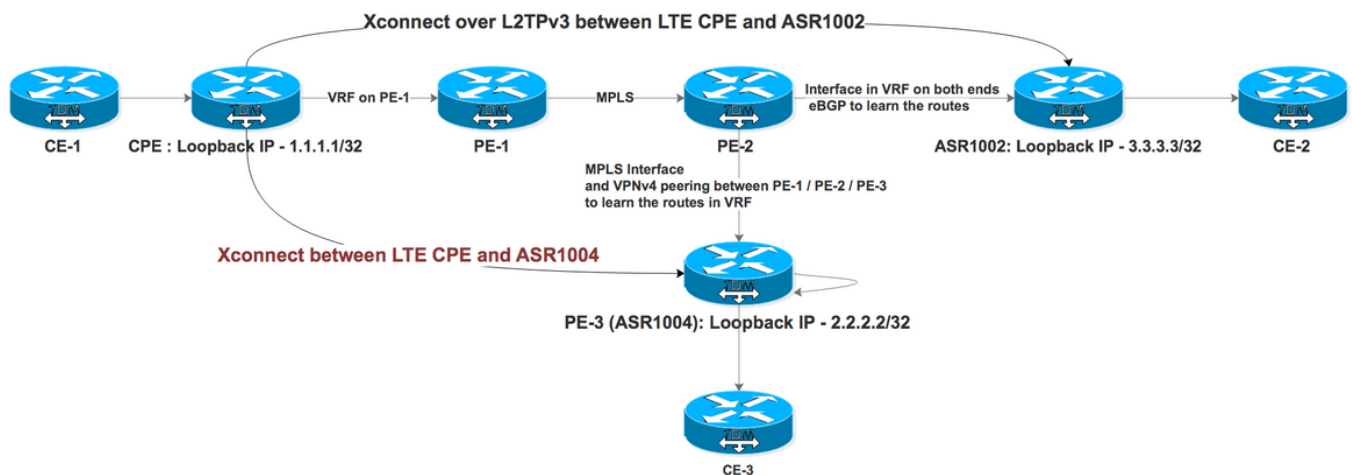
1.enable

2.configureterminal

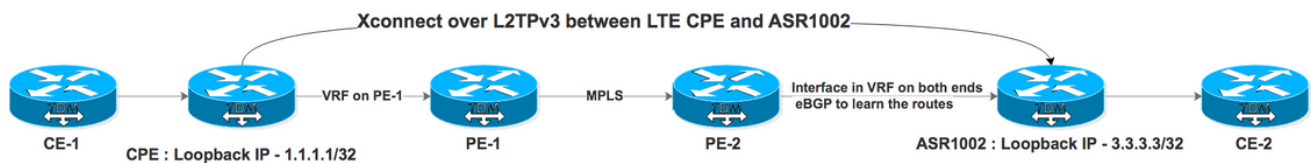
3.interface logement/port de type

4.xconnectpeer-ip-address vcidencapsulation l2tpv3 pw-classpw-class-name

Examinons maintenant le comportement de L2TPv3 Xconnect lors de l'utilisation de VRF. Voici la topologie utilisée pour la démonstration dans laquelle nous Xconnect est configuré entre CPE et ASR1002 (IP) et ASR1004 (MPLS) avec des points de terminaison à ASR1000 dans VRF (VRF Aware L2TPv3 n'est pas pris en charge sur la plate-forme ASR100000).



## Cas d'essai I : L2TPv3 Xconnect sur réseau IP avec terminaux dans VRF



PE-1 et PE-2 créent le réseau MPLS pour ISP. Le CPE est connecté à PE-1 sur VRF et ASR1002 est connecté à PE-2 sur VRF. L'ASR1002 dispose également de VRF sur l'interface connectée à PE-2. L'accessibilité du bouclage CPE à partir de l'ASR1002 est via l'interface VRF sur IP.

Configuration sur CPE pour Xconnect vers ASR1002 :

```
interface FastEthernet4.2381
```

```
encapsulation dot1Q 2381
```

```
xconnect 3.3.3.3 2381 encapsulation l2tpv3 pw-class PSEUDO_CLASS >>>>>>>>>> Xconnect with ASR1002
```



```
pseudowire-class PSEUDO_CLASS
encapsulation l2tpv3
interworking vlan
protocol l2tpv3 L2TP_CLASS
ip local interface Loopback11
```

```
l2tp-class L2TP_CLASS
authentication
password cisco
```

```
interface Loopback11
ip vrf forwarding L2TP_VRF -----> Source is in VRF
ip address 3.3.3.3 255.255.255.255
```

```
router bgp 1
```

```
address-family ipv4 vrf L2TP_VRF
redistribute connected
neighbor 10.1.1.2 remote-as 2 -----> eBGP with PE-2 in VRF
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 soft-reconfiguration inbound
```

```
exit-address-family
```

```
VRF L2TP_VRF :
```

```
B      1.1.1.1/32 [20/0] via 10.1.1.2, 1d -----> Xconnect end point learned via eBGP in VRF
```

**Contrôlons maintenant l'état de Xconnect sur CPE :**

```
CPE #sh xconnect all de
```

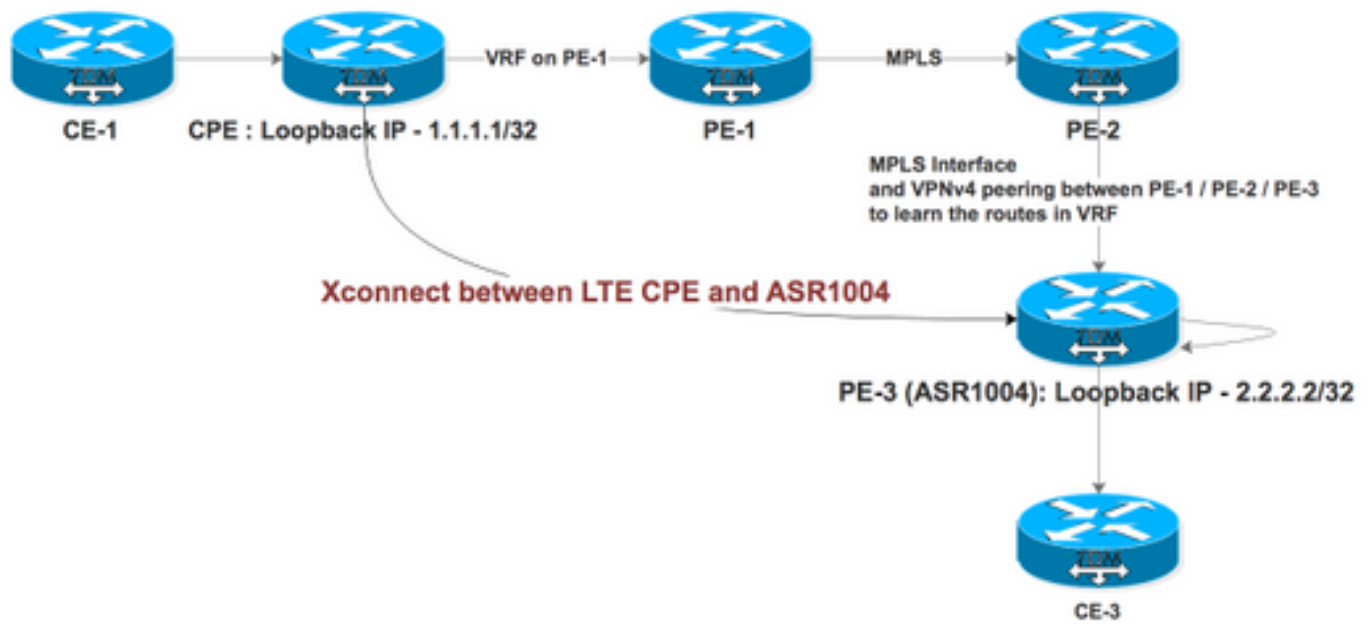
```
Legend:   XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
```

```
UP=Up      DN=Down      AD=Admin Down  IA=Inactive
```

```
SB=Standby HS=Hot Standby  RV=Recovering  NH=No Hardware
```







PE-1, PE-2 et PE-3 font du réseau MPLS pour ISP avec PE-2 agissant comme réflecteur de route (RR). Le CPE est connecté à PE-1 sur VRF et ASR1004 est connecté à PE-2 avec MPLS activé sur l'interface. L'ASR1004 dispose également d'un VRF dans lequel il est supposé recevoir les routes VPNv4 de PE-1 via RR. L'accessibilité de la boucle CPE à partir de l'ASR1004 est via l'interface VRF sur MPLS.

Configuration sur CPE pour Xconnect vers ASR1004 :

```
interface FastEthernet4.2380

encapsulation dot1Q 2380

xconnect 2.2.2.2 2380 encapsulation l2tpv3 pw-class PSEUDO_CLASS >>>>>>>>>Xconnect with
ASR1004

interface FastEthernet4.2381

encapsulation dot1Q 2381

xconnect 3.3.3.3 2381 encapsulation l2tpv3 pw-class PSEUDO_CLASS >>>>>>>>> Xconnect with
ASR1002

pseudowire-class PSEUDO_CLASS

encapsulation l2tpv3

interworking vlan

protocol l2tpv3 L2TP_CLASS

ip local interface Loopback0
```





```
interworking vlan
protocol l2tpv3 L2TP_CLASS
ip local interface Loopback11
```

```
l2tp-class L2TP_CLASS
authentication
password cisco
```

```
router bgp 2
address-family ipv4 vrf L2TP_VRF
redistribute connected
redistribute static
default-information originate
exit-address-family
```

### Entrée de route pour le point d'extrémité Xconnect :

```
ASR1004#sh ip rou vrf L2TP_VRF 1.1.1.1 . -----> Xconnect End Point also learned
via VRF
```

```
Routing Table: L2TP_VRF
Routing entry for 1.1.1.1/32
Known via "bgp 2", distance 200, metric 0, type internal
Last update from 11.11.11.11 6d17h ago
Routing Descriptor Blocks:
* 11.11.11.11 (default), from 22.22.22.22, 6d17h ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: 18
MPLS Flags: MPLS Required
```

We observed that Segment 2 was continuously flapping on both ends.

```
ASR1004#sh xc all de
```

```
Legend:   XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
UP=Up     DN=Down                 AD=Admin Down     IA=Inactive
SB=Standby HS=Hot Standby       RV=Recovering     NH=No Hardware
```



Tunnel ID: 1760690853

Protocol State: DOWN

Remote Circuit State: DOWN

pw-class: PSEUDO\_CLASS

UP pri ac Fa4.2381:2381(Eth VLAN) UP l2tp 3.3.3.3:2381 UP -----  
---à Stable with ASR1002

Interworking: vlan

Session ID: 1906980494

Tunnel ID: 2886222725

Protocol State: UP

Remote Circuit State: UP

pw-class: PSEUDO\_CLASS

CPE#sh l2tp session

L2TP Session Information Total tunnels 2 sessions 2

LocID	RemID	TunID	Username, Intf/ Vcid, Circuit	State	Last Chg	Uniq ID	
2714490989	3697021268	1760690853	2380, Fa4.2380:2380	est	00:00:03 0		-----> Flapping with ASR1004
1906980494	2361475239	2886222725	2381, Fa4.2381:2381	est	15:37:06 0		-----> Stable with ASR1002

Vous ne pouvez pas configurer une route statique dans ce cas, car l'interface de sortie est activée par MPLS. Comme solution de contournement, deux interfaces sont bouclées l'une vers l'autre et configurées l'une dans VRF avec l'autre dans global. Ensuite configuré une route statique dans global pointant vers l'interface VRF, avec ce Xconnect est devenu stable.

ASR1004#sh run int gi0/0/2

Building configuration...

Current configuration : 95 bytes

!

interface GigabitEthernet0/0/2 -----> Looped to Gi0/0/3

ip address 20.20.20.2 255.255.255.252

negotiation auto

end

```
#sh run int gi0/0/3
```

Building configuration...

Current configuration : 126 bytes

!

```
interface GigabitEthernet0/0/3
```

```
ip vrf forwarding L2TP_VRF
```

```
ip address 20.20.20.1 255.255.255.252
```

```
negotiation auto
```

end

ip route 10.246.131.62 255.255.255.255 20.20.20.1 ———> Static route pointing towards an IP interface in Global

```
CPE#sh xconnect all de
```

Legend: XC ST=Xconnect State S1=Segment1 State S2=Segment2 State

UP=Up DN=Down AD=Admin Down IA=Inactive

SB=Standby HS=Hot Standby RV=Recovering NH=No Hardware

XC	ST	Segment 1	S1	Segment 2	S2
----	----	-----------	----	-----------	----

DN	pri	ac Fa4.2380:2380(Eth VLAN)	UP	l2tp 2.2.2.2:2380	UP
----	-----	----------------------------	----	-------------------	----

Interworking: vlan

Session ID: 3434660693

Tunnel ID: 1760690853

Protocol State: DOWN

Remote Circuit State: DOWN

pw-class: PSEUDO\_CLASS

UP	pri	ac Fa4.2381:2381(Eth VLAN)	UP	l2tp 3.3.3.3:2381	UP
----	-----	----------------------------	----	-------------------	----

Interworking: vlan

Session ID: 1906980494

Tunnel ID: 2886222725

Protocol State: UP

Remote Circuit State: UP

pw-class: PSEUDO\_CLASS

CPE#sh l2tp session

Informations de session L2TP Total tunnels 2 sessions 2 :

LocID	RemID	TunID	Username, Intf/ Vcid, Circuit	State	Last Chg	Uniq ID
2714490989	3697021268	1760690853	2380, Fa4.2380:2380	est	00:20:03	0

1906980494	2361475239	2886222725	2381, Fa4.2381:2381	est	15:37:06	0
------------	------------	------------	---------------------	-----	----------	---

Le flux de trafic est considéré comme dans le cas de l'ASR1004 :

- Lorsque le trafic provient de CPE sur ASR1004, il provient de l'interface MPLS Gi0/0/1 et est commuté directement au port d'accès Gi0/0/0.
- Lorsque le trafic provient du port d'accès Gi0/0/0, il emprunte le chemin bouclé de Gi0/0/0 -> Gi0/0/2 -> Gi0/0/3 -> Gi0/0/1.

Le principal problème de cette solution de contournement est l'utilisation de QFP sur la plateforme ASR1000, car le traitement des paquets est effectué deux fois :

ASR1004# show platform packet-trace summary

Pkt	Input	Output	State	Reason
0	Gi0/0/3	Gi0/0/1	FWD	
1	Gi0/0/3	Gi0/0/1	FWD	
2	Gi0/0/3	Gi0/0/1	FWD	
3	Gi0/0/0	Gi0/0/2	FWD	
4	Gi0/0/0	Gi0/0/2	FWD	
5	Gi0/0/0	Gi0/0/2	FWD	
6	Gi0/0/0	Gi0/0/2	FWD	
7	Gi0/0/0	Gi0/0/2	FWD	

Ce comportement est documenté dans Doc Bug : [CSCvi42964](#)