

# Le serveur DHCP ne fonctionne pas sur un routeur qui exécute Cisco IOS-XE SD-WAN avec DIA

## Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

## Introduction

Ce document décrit les problèmes typiques auxquels on peut s'attendre lorsque la stratégie de données centralisée pour l'accès direct à Internet (DIA) et le serveur DHCP sont configurés sur un VPN côté service du même routeur exécutant le logiciel SDWAN IOS®-XE. Des problèmes similaires peuvent être observés avec tout autre trafic entrant sur le périphérique à partir du VPN côté service et destiné au traitement local du routeur.

## Problème

Le serveur DHCP ne fonctionne pas sur le routeur avec le logiciel SDWAN Cisco IOS®-XE. DIA est configuré avec une politique de données centralisée comme indiqué ici :

```
policy
data-policy _LAN_DIA
  vpn-list LAN
  sequence 1
  match
  destination-data-prefix-list EXCLUDE_SUBNET
  !
  action accept
  set
  local-tloc-list
  color biz-internet lte
  encaps ipsec
  !
  !
  !
  sequence 11
  action accept
  nat use-vpn 0
  !
  !
  default-action accept
!
lists
data-prefix-list EXCLUDE_SUBNET
ip-prefix 10.0.0.0/8
!
```

```

site-list DIA_BRANCHES
  site-id 7
  site-id 6
!
vpn-list LAN
  vpn 10
!
!
!
apply-policy
site-list DIA_BRANCHES
  data-policy _LAN_DIA_EXCLUDE from-service
!
!

```

## Solution

Pour que cela fonctionne, les paquets DHCP doivent être exclus de la stratégie de données, car il est clairement indiqué dans les débogages de suivi des paquets que les paquets vers les adresses de diffusion ne peuvent pas être routés (DROP 72 Ipv4RoutingErr) et qu'ils sont NAT (Action : REDIRECT\_NAT) selon la stratégie SDWAN (Fonction : Stratégie de données SDWAN IN) :

```

B2#show platform packet-trace summary
<skipped>
28  V190          V190          DROP    72  (Ipv4RoutingErr)
29  Gi0/1/0       Gi0/0/0       FWD
30  V190          V190          DROP    72  (Ipv4RoutingErr)

```

```

B2#show platform packet-trace packet 28
Packet: 28          CBUG ID: 28
Summary
  Input      : Vlan90
  Output     : Vlan90
  State      : DROP 72  (Ipv4RoutingErr)
Timestamp
  Start     : 14482257476440 ns (12/17/2018 13:56:58.524691 UTC)
  Stop      : 14482257534440 ns (12/17/2018 13:56:58.524749 UTC)

```

```

Path Trace
Feature: IPV4(Input)
  Input      : Vlan90
  Output     : <unknown>
  Source     : 0.0.0.0
  Destination : 255.255.255.255
  Protocol   : 17 (UDP)
  SrcPort    : 68
  DstPort    : 67
Feature: DEBUG_COND_INPUT_PKT
  Entry      : Input - 0x10e44b40
  Input      : Vlan90
  Output     : <unknown>
  Lapsed time : 106 ns
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
  Entry      : Input - 0x10e5ca94
  Input      : Vlan90
  Output     : <unknown>
  Lapsed time : 253 ns
Feature: IPV4_INPUT_FOR_US_MARTIAN
  Entry      : Input - 0x10e5cb24

```

Input : Vlan90  
Output : <unknown>  
Lapsed time : 4853 ns  
Feature: IPV4\_INPUT\_FNF\_FIRST\_EXT  
Entry : Input - 0x10e48968  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 600 ns  
Feature: SDWAN Data Policy IN  
VRF : 1  
Seq : 1  
DNS Flags : (0x0) NONE  
Policy Flags : 0x10  
Action : REDIRECT\_NAT  
Feature: SDWAN\_DATA\_POLICY\_IN\_EXT  
Entry : Input - 0x10eb9d7c  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 5360 ns  
Feature: IPV4\_INPUT\_DST\_LOOKUP\_ISSUE  
Entry : Input - 0x10e5c9d8  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 200 ns  
Feature: IPV4\_INPUT\_ARL  
Entry : Input - 0x10e46158  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 200 ns  
Feature: IPV4\_INTERNAL\_DST\_LOOKUP\_CONSUME  
Entry : Input - 0x10e5cac4  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 253 ns  
Feature: STILE\_LEGACY\_DROP  
Entry : Input - 0x10eb294c  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 306 ns  
Feature: INGRESS\_MMA\_LOOKUP\_DROP  
Entry : Input - 0x10eae2a4  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 213 ns  
Feature: INPUT\_DROP\_FNF\_AOR  
Entry : Input - 0x10e5b864  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 386 ns  
Feature: INPUT\_FNF\_DROP  
Entry : Input - 0x10e48cf8  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 493 ns  
Feature: INPUT\_DROP\_FNF\_AOR\_RELEASE  
Entry : Input - 0x10e5b234  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 213 ns  
Feature: INPUT\_DROP  
Entry : Input - 0x10e439d4  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 106 ns

```

Feature: IPV4_INTERNAL_FOR_US
Entry      : Input - 0x10e5cb54
Input      : Vlan90
Output     : <unknown>
Lapsed time : 4640 ns

```

La stratégie de données est modifiée pour exclure les paquets DHCP (ports UDP 67,68) de la NAT, comme indiqué ici :

```

B2# show sdwan policy from-vsmart
from-vsmart data-policy _LAN_DIA
direction from-service
vpn-list LAN
sequence 1
match
destination-data-prefix-list EXCLUDE_SUBNET
action accept
set
local-tloc-list
color biz-internet lte
encap ipsec
sequence 11
match
destination-port 67-68
protocol 17
action accept
sequence 21
match
source-port 67-68
protocol 17
action accept
sequence 31
action accept
nat use-vpn 0
no nat fallback
default-action accept
from-vsmart lists vpn-list LAN
vpn 10
from-vsmart lists data-prefix-list EXCLUDE_SUBNET
ip-prefix 10.0.0.0/8

```

Le débogage de Packet-trace affiche une image différente pour les paquets DHCP et ils seront punis au processeur RP pour un traitement local ultérieur (État : PUNT 60) comme ils devraient être :

```

B2#show platform packet-trace summary

```

Pkt	Input	Output	State	Reason
<skipped>				
88	Vl90	internal0/0/rp:0	PUNT	60 (IP subnet or broadcast pac
89	INJ.7	Gi0/1/0.MOD0	FWD	
90	Gi0/1/0	internal0/0/rp:0	PUNT	60 (IP subnet or broadcast pac
91	INJ.7	Gi0/1/0.MOD0	FWD	
92	Gi0/0/0	internal0/0/rp:0	PUNT	60 (IP subnet or broadcast pac
93	Gi0/1/1	Ce0/2/0	FWD	
94	Gi0/0/0	internal0/0/rp:0	PUNT	60 (IP subnet or broadcast pac
95	Vl90	internal0/0/rp:0	PUNT	60 (IP subnet or broadcast pac
96	INJ.7	Gi0/1/0.MOD0	FWD	
97	Gi0/1/1	internal0/0/rp:0	PUNT	60 (IP subnet or broadcast pac
98	INJ.7	Gi0/1/0.MOD0	FWD	

B2# show platform packet-trace packet 88

Packet: 88 CBUG ID: 88

Summary

Input : Vlan90  
Output : internal0/0/rp:0  
State : PUNT 60 (IP subnet or broadcast pac

Timestamp

Start : 16485953871600 ns (12/17/2018 14:30:22.221086 UTC)  
Stop : 16485953959680 ns (12/17/2018 14:30:22.221174 UTC)

Path Trace

Feature: IPV4(Input)

Input : Vlan90  
Output : <unknown>  
Source : 0.0.0.0  
Destination : 255.255.255.255  
Protocol : 17 (UDP)  
SrcPort : 68  
DstPort : 67

Feature: DEBUG\_COND\_INPUT\_PKT

Entry : Input - 0x10e44b40  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 93 ns

Feature: IPV4\_INPUT\_DST\_LOOKUP\_CONSUME

Entry : Input - 0x10e5ca94  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 320 ns

Feature: IPV4\_INPUT\_FOR\_US\_MARTIAN

Entry : Input - 0x10e5cb24  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 8053 ns

Feature: IPV4\_INPUT\_FNF\_FIRST\_EXT

Entry : Input - 0x10e48968  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 533 ns

Feature: SDWAN Data Policy IN

VRF : 1  
Seq : 1  
DNS Flags : (0x0) NONE  
Policy Flags : 0x0  
Action : NONE

Feature: SDWAN\_DATA\_POLICY\_IN\_EXT

Entry : Input - 0x10eb9d7c  
Input : Vlan90  
Output : <unknown>  
Lapsed time : 5626 ns

Feature: IPV4\_INPUT\_LOOKUP\_PROCESS\_EXT

Entry : Input - 0x10e5cc70  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 1600 ns

Feature: IPV4\_INPUT\_FNF\_FINAL\_EXT

Entry : Input - 0x10e489c8  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 386 ns

Feature: IPV4\_INPUT\_IPOPTIONS\_PROCESS\_EXT

Entry : Input - 0x10e5ce10  
Input : Vlan90  
Output : internal0/0/rp:0

Lapsed time : 186 ns  
Feature: IPV4\_INPUT\_GOTO\_OUTPUT\_FEATURE\_EXT  
Entry : Input - 0x10e46278  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 493 ns  
Feature: CBUG\_OUTPUT\_FIA\_EXT  
Entry : Output - 0x10e44c00  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 560 ns  
Feature: IPV4\_INTERNAL\_ARL\_SANITY\_EXT  
Entry : Output - 0x10e46128  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 253 ns  
Feature: IPV4\_OUTPUT\_THREAT\_DEFENSE\_EXT  
Entry : Output - 0x10eb5cc4  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 266 ns  
Feature: IPV4\_VFR\_REFRAG\_EXT  
Entry : Output - 0x10e5cf10  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 66 ns  
Feature: IPV4\_OUTPUT\_DROP\_POLICY\_EXT  
Entry : Output - 0x10e5e900  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 2586 ns  
Feature: DEBUG\_COND\_OUTPUT\_PKT\_EXT  
Entry : Output - 0x10e44ba0  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 133 ns  
Feature: INTERNAL\_TRANSMIT\_PKT\_EXT  
Entry : Output - 0x10e45420  
Input : Vlan90  
Output : internal0/0/rp:0  
Lapsed time : 5066 ns

IOSd Path Flow: Packet: 88 CBUG ID: 88

Feature: INFRA  
Pkt Direction: IN  
Packet Rcvd From DATAPLANE

Feature: IP  
Pkt Direction: IN  
Source : 0.0.0.0  
Destination : 255.255.255.255

Feature: IP  
Pkt Direction: IN  
Packet Enqueued in IP layer  
Source : 0.0.0.0  
Destination : 255.255.255.255  
Interface : Vlan90

Feature: UDP  
Pkt Direction: IN  
src : 0.0.0.0(68)  
dst : 255.255.255.255(67)  
length : 308

Ce comportement est attendu et des problèmes similaires peuvent être détectés avec tout autre trafic destiné à un traitement CPU du processeur RP (processeur de routage de périphérique local) (par exemple, synchronisation NTP (Network Time Protocol) si le routeur agit comme source NTP) si la politique de données centralisée n'exclut pas un type de trafic particulier de manière appropriée.

**Note:** Pour plus d'informations sur Datapath Packet Trace, reportez-vous à :  
<https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html>