

# El servidor DHCP no funciona en un router que ejecuta Cisco IOS-XE SD-WAN con DIA

## Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

## Introducción

Este documento describe los problemas típicos que podrían esperarse cuando la política de datos centralizada para el acceso directo a Internet (DIA) y el servidor DHCP se configuran en la VPN del lado del servicio del mismo router que ejecuta el software IOS®-XE SDWAN. Se pueden ver problemas similares con cualquier otro tráfico que ingresa al dispositivo desde la VPN del lado del servicio y está destinado al procesamiento local del router.

## Problema

El servidor DHCP no funciona en el router con el software SDWAN Cisco IOS®-XE. DIA se configura con una política de datos centralizada como se muestra aquí:

```
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
!
!

```

## Solución

Para que esto funcione, los paquetes DHCP deben excluirse de la política de datos, ya que se ve claramente en las depuraciones de seguimiento de paquetes que los paquetes a las direcciones de difusión no se pueden rutear (DROP 72 Ipv4RoutingErr) y son NATed (Acción: REDIRECT\_NAT) según la política de SDWAN (Función: Política de datos de 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 política de datos se modifica para excluir los paquetes DHCP (puertos UDP 67,68) de NAT, como se muestra aquí:

```
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
```

La depuración de Packet-Trace mostrará una imagen diferente para los paquetes DHCP y serán impulsados a la CPU RP para mayor procesamiento local (Estado: PUNT 60), como deben ser:

```
B2#show platform packet-trace summary
Pkt  Input          Output          State  Reason
<skipped>
88   V190            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   V190            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
```

Se trata de un comportamiento esperado y se pueden detectar problemas similares con cualquier otro tráfico destinado al procesamiento de CPU de procesador de routing de dispositivo local (RP)

(por ejemplo, la sincronización del protocolo de tiempo de red (NTP) si el router actúa como origen NTP) si la política de datos centralizada no excluye adecuadamente el tipo de tráfico concreto.

**Nota:** Para obtener más información sobre Datapath Packet Trace, consulte:  
<https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html>