Configurer la fonctionnalité VXLAN sur les périphériques Cisco IOS XE

Table des matières

Introduction

Ce document décrit la configuration de base et le dépannage sur les périphériques Cisco IOS® XE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base des superpositions DCI et de la multidiffusion

Composants utilisés

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

- ASR1004 exécutant le logiciel 03.16.00.S
- CSR100v(VXE) exécutant le logiciel 3.16.03.S

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le réseau LAN virtuel extensible (VXLAN) est de plus en plus populaire en tant que solution d'interconnexion de data center (DCI). La fonctionnalité VXLAN est utilisée pour fournir une extension de couche 2 sur le domaine de routage public/couche 3. Ce document traite de la configuration de base et du dépannage sur les périphériques Cisco IOS XE.

Les sections Configurer et Vérifier de ce document couvrent deux scénarios :

- Le scénario A décrit une configuration VXLAN entre trois data centers en mode multidiffusion.
- Le scénario B décrit une configuration VXLAN entre deux data centers en mode

monodiffusion.

Configurer

Scénario A : configuration de VXLAN entre trois data centers en mode multidiffusion

Configuration de base

Le mode multidiffusion nécessite une connectivité de monodiffusion et de multidiffusion entre les sites. Ce guide de configuration utilise le protocole OSPF (Open Shortest Path First) pour fournir une connectivité monodiffusion et le protocole PIM (Protocol Independent Multicast) bidirectionnel pour fournir une connectivité multidiffusion.

Voici la configuration de base des trois data centers pour le mode multidiffusion :

<#root>

```
!
DC1#
```

show run | sec ospf

```
router ospf 1
network 10.1.1.1 0.0.0.0 area 0
network 10.10.10.4 0.0.0.3 area 0
!
```

Configuration bidirectionnelle PIM :

<#root>

```
!
DC1#
```

show run | sec pim

```
ip pim bidir-enable
ip pim send-rp-discovery scope 10
ip pim bsr-candidate Loopback1 0
ip pim rp-candidate Loopback1 group-list 10 bidir
!
access-list 10 permit 239.0.0.0 0.0.0.255
!
DC1#
!
```

En outre, le mode intermédiaire PIM est activé sous toutes les interfaces L3, y compris le bouclage :

<#root>

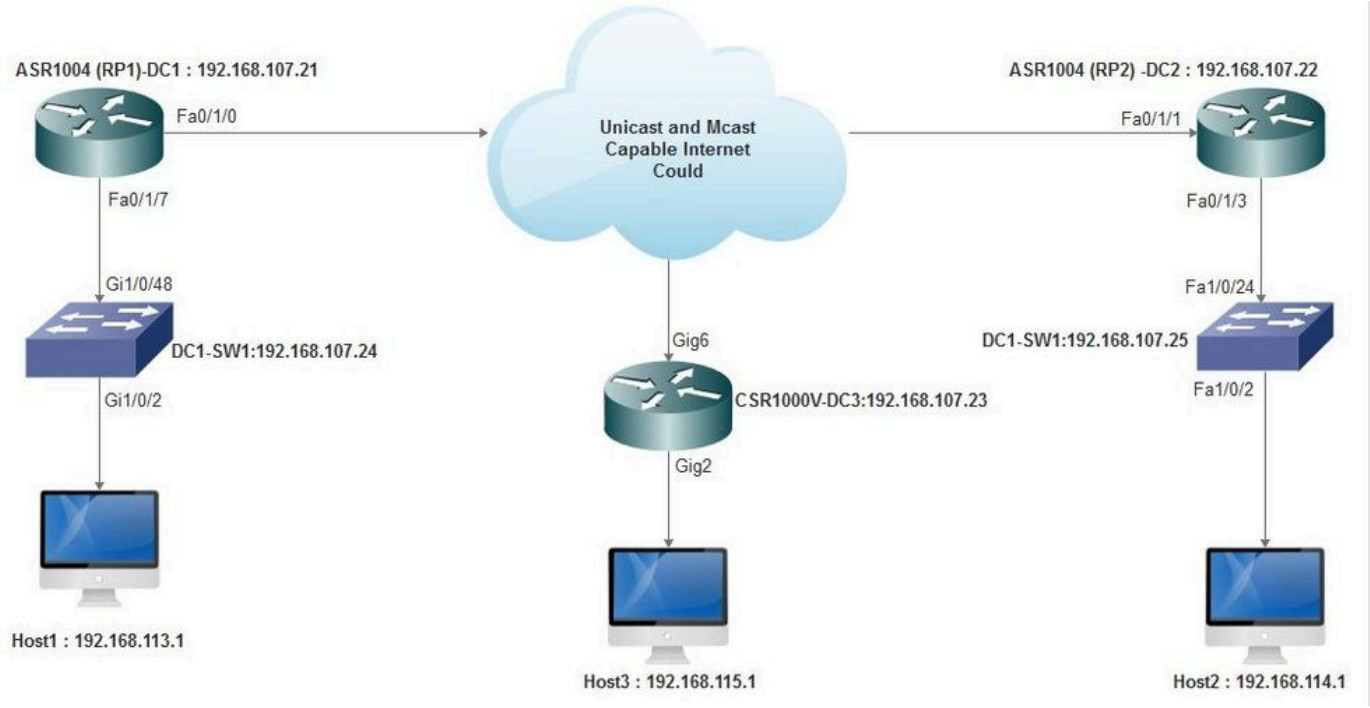
```
!
DC1#
```

show run interface lo1

```
Building configuration...
Current configuration : 83 bytes
!
interface Loopback1
ip address 10.1.1.1 255.255.255.255
ip pim sparse-mode
end
```

Assurez-vous également que le routage de multidiffusion est activé sur votre périphérique et que la table de multidiffusion mroute est remplie.

Diagramme du réseau



Internet compatible monodiffusion et multidiffusion

Configuration de DC1(VTEP1)

```
!
!
Vxlan udp port 1024
!
Interface Loopback1
ip address 10.1.1.1 255.255.255.255
ip pim sparse-mode
!
```

Définissez les membres VNI et l'interface membre dans la configuration de domaine de pont :

```
!
bridge-domain 1
member vni 6001
member FastEthernet0/1/7 service-instance 1
!
```

Créez l'interface réseau virtuelle (NVE) et définissez les membres VNI qui doivent être étendus sur le WAN à d'autres data centers :

```
!
interface nve1
no ip address
shut
member vni 6001 mcast-group 10.0.0.10
!
source-interface Loopback1
!
```

Créez des instances de service sur l'interface LAN (c'est-à-dire l'interface qui connecte le réseau LAN) pour superposer le VLAN particulier (trafic étiqueté 802.1q) - dans ce cas, VLAN 1 :

```
!
interface FastEthernet0/1/7
no ip address
negotiation auto
cdp enable
no shut
!
```

Supprimez l'étiquette VLAN avant d'envoyer le trafic à travers la superposition, et poussez-la après l'envoi du trafic de retour dans le VLAN :

```
!
service instance 1 ethernet
encapsulation unagged
!
```

Configuration de DC2 (VTEP2)

```
!
!
Vxlan udp port 1024
!
interface Loopback1
ip address 10.2.2.2 255.255.255.255
ip pim sparse-mode
!
!
bridge-domain 1
member vni 6001
member FastEthernet0/1/3 service-instance 1
!
!
interface nve1
no ip address
member vni 6001 mcast-group 10.0.0.10
!
source-interface Loopback1
shut
!
!
interface FastEthernet0/1/3
no ip address
negotiation auto
cdp enable
no shut
!
service instance 1 ethernet
encapsulation untagged
!
```

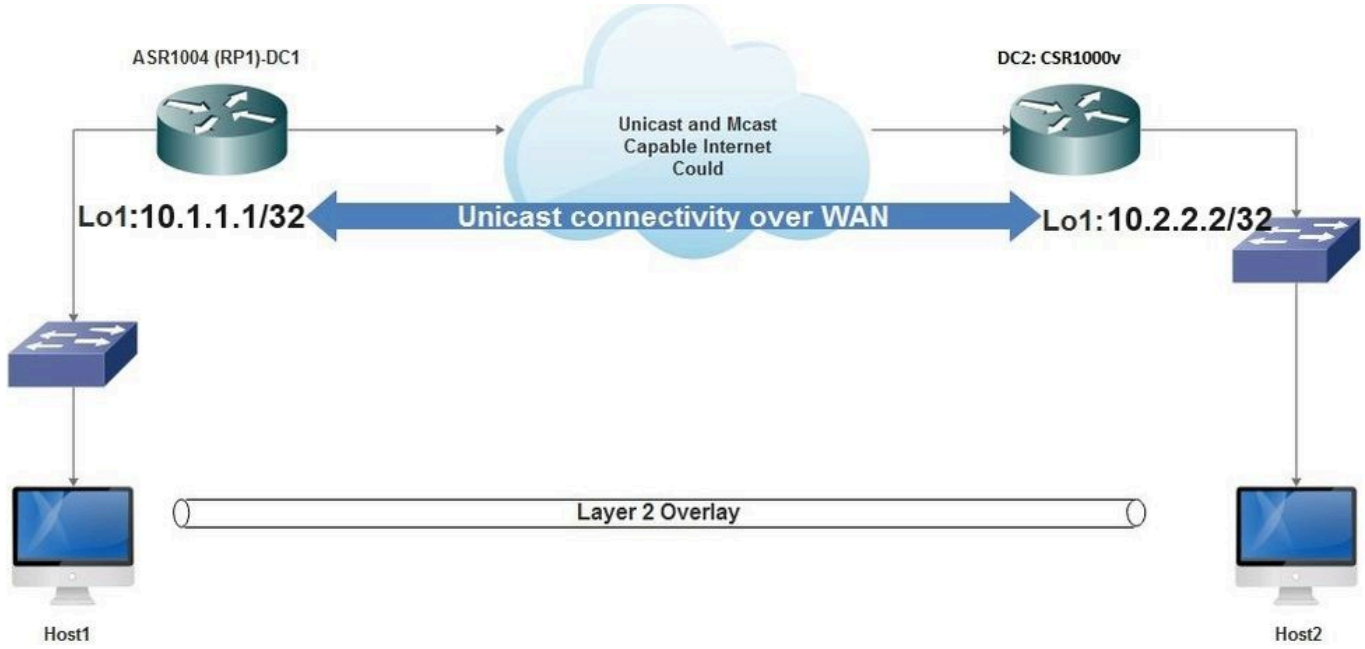
Configuration de DC3(VTEP3)

```
!
!
Vxlan udp port 1024
!
interface Loopback1
ip address 10.3.3.3 255.255.255.255
ip pim sparse-mode
!
!
bridge-domain 1
member vni 6001
member GigabitEthernet2 service-instance 1
!
interface nve1
no ip address
shut
member vni 6001 mcast-group 10.0.0.10
!
source-interface Loopback1
!
interface gig2
no ip address
negotiation auto
```

```
cdp enable
no shut
!
service instance 1 ethernet
encapsulation untagged
!
```

Scénario B : configuration de VXLAN entre deux data centers en mode monodiffusion

Diagramme du réseau



Connectivité monodiffusion sur WAN

Configuration de DC1

```
!
interface nve1
no ip address
member vni 6001
! ingress replication shold be configured as peer data centers loopback IP address.
!
ingress-replication 10.2.2.2
!
source-interface Loopback1
!
!
interface gig0/2/1
no ip address
negotiation auto
cdp enable
!
service instance 1 ethernet
encapsulation untagged
```

```
!
!
!
bridge-domain 1
member vni 6001
member gig0/2/1 service-instance 1
```

Configuration de DC2

```
!
interface nve1
no ip address
member vni 6001
ingress-replication 10.1.1.1
!
source-interface Loopback1
!

!
interface gig5
no ip address
negotiation auto
cdp enable
!
service instance 1 ethernet
encapsulation untagged

!
!
bridge-domain 1
member vni 6001
member gig5 service-instance 1
```

Vérifier

Scénario A : configuration de VXLAN entre trois data centers en mode multidiffusion

Une fois la configuration du scénario A terminée, les hôtes connectés de chaque centre de données doivent pouvoir se joindre au sein du même domaine de diffusion.

Utilisez ces commandes pour vérifier les configurations. Quelques exemples sont fournis dans le scénario B.

<#root>

```
Router#
```

show nve vni

```
Router#
```

```
show nve vni interface nve1

Router#

show nve interface nve1

Router#

show nve interface nve1 detail

Router#

show nve peers
```

Scénario B : configuration de VXLAN entre deux data centers en mode monodiffusion

Sur DC1 :

<#root>

```
DC1#

show nve vni

Interface    VNI     Multicast-group    VNI state
nve1        6001           N/A               Up

DC1#

show nve interface nve1 detail

Interface: nve1, State: Admin Up, Oper Up Encapsulation: Vxlan
source-interface: Loopback1    (primary:10.1.1.1 vrf:0)
Pkts In     Bytes In      Pkts Out     Bytes Out
60129       6593586        55067        5303698

DC1#

show nve peers

Interface     Peer-IP      VNI        Peer state
nve1          10.2.2.2       6000          -
```

Sur DC2 :

DC2#**show nve vni**

Interface VNI Multicast-group VNI state

nve1 6000 N/A Up

DC2#**show nve interface nve1 detail**

Interface: nve1, State: Admin Up, Oper Up Encapsulation: Vxlan

source-interface: Loopback1 (primary:10.2.2.2 vrf:0)

Pkts In Bytes In Pkts Out Bytes Out

70408 7921636 44840 3950835

DC2#**show nve peers**

Interface Peer-IP VNI Peer state

nve 10.1.1.1 6000 Up

DC2#**show bridge-domain 1**

Bridge-domain 1 (3 ports in all)

State: UP Mac learning: Enabled

Aging-Timer: 300 second(s)

BDI1 (up)

GigabitEthernet0/2/1 service instance 1

vni 6001

AED MAC address Policy Tag Age Pseudoport

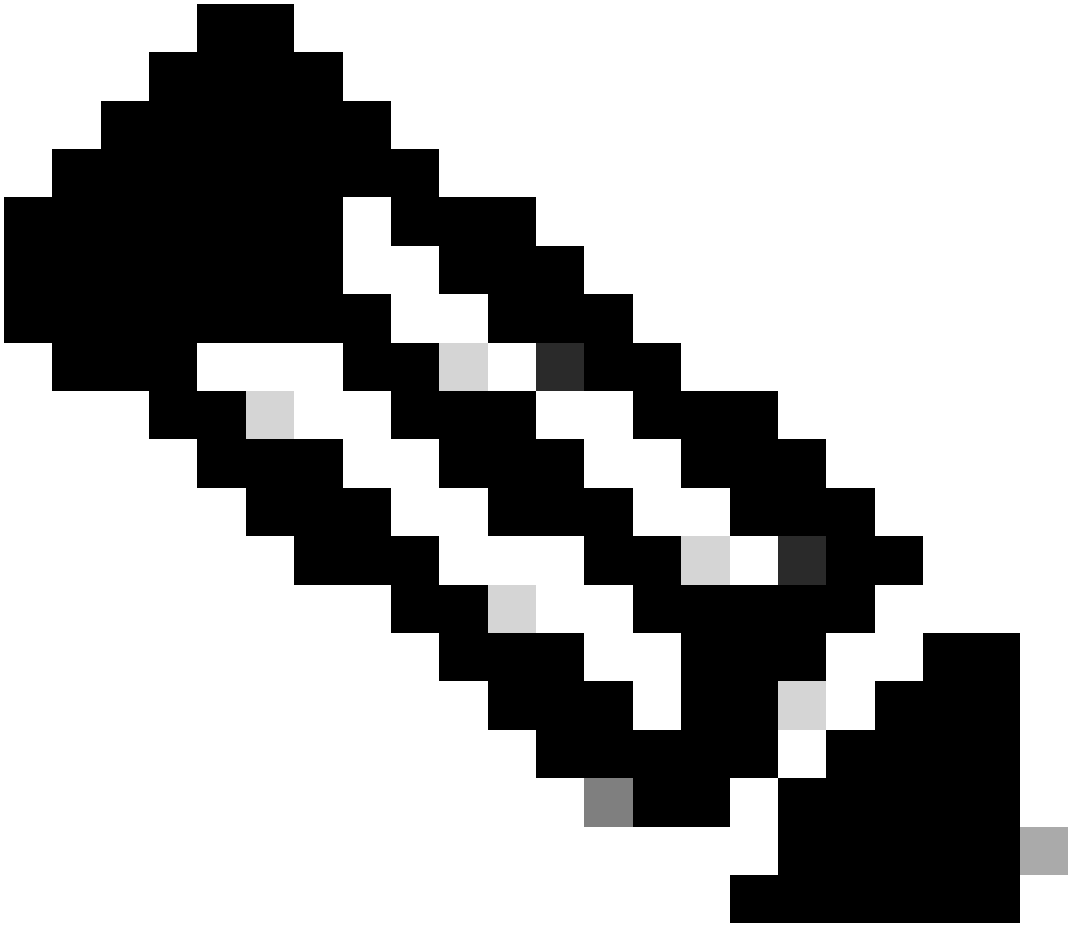
0 7CAD.74FF.2F66 forward dynamic 281 nve1.VNI6001, VxLAN src: 10.1.1.1 dst: 10.2.2.2

0 B838.6130.DA80 forward dynamic 288 nve1.VNI6001, VxLAN src: 10.1.1.1 dst: 10.2.2.2

0 0050.56AD.1AD8 forward dynamic 157 nve1.VNI6001, VxLAN src: 10.1.1.1 dst: 10.2.2.2

Dépannage

Les commandes décrites dans la section Vérifier fournissent les étapes de dépannage de base. Ces diagnostics supplémentaires peuvent être utiles lorsque le système ne fonctionne pas.



Remarque : certains de ces diagnostics peuvent entraîner une augmentation de la mémoire et de l'utilisation du processeur.

Diagnostics de débogage

#debug nve error

*Jan 4 20:00:54.993: NVE-MGR-PEER ERROR: Intf state force down successful for mcast nodes cast nodes

*Jan 4 20:00:54.993: NVE-MGR-PEER ERROR: Intf state force down successful for mcast nodes cast nodes

*Jan 4 20:00:54.995: NVE-MGR-PEER ERROR: Intf state force down successful for peer nodes eer nodes

*Jan 4 20:00:54.995: NVE-MGR-PEER ERROR: Intf state force down successful for peer nodes

#show nve log error

[01/01/70 00:04:34.130 UTC 1 3] NVE-MGR-STATE ERROR: vni 6001: error in create notification to Tunnel
[01/01/70 00:04:34.314 UTC 2 3] NVE-MGR-PEER ERROR: Intf state force up successful for mcast nodes
[01/01/70 00:04:34.326 UTC 3 3] NVE-MGR-PEER ERROR: Intf state force up successful for peer nodes
[01/01/70 01:50:59.650 UTC 4 3] NVE-MGR-PEER ERROR: Intf state force down successful for mcast nodes
[01/01/70 01:50:59.654 UTC 5 3] NVE-MGR-PEER ERROR: Intf state force down successful for peer nodes
[01/01/70 01:50:59.701 UTC 6 3] NVE-MGR-PEER ERROR: Intf state force up successful for mcast nodes
[01/01/70 01:50:59.705 UTC 7 3] NVE-MGR-PEER ERROR: Intf state force up successful for peer nodes
[01/01/70 01:54:55.166 UTC 8 61] NVE-MGR-PEER ERROR: Intf state force down successful for mcast nodes
[01/01/70 01:54:55.168 UTC 9 61] NVE-MGR-PEER ERROR: Intf state force down successful for peer nodes
[01/01/70 01:55:04.432 UTC A 3] NVE-MGR-PEER ERROR: Intf state force up successful for mcast nodes
[01/01/70 01:55:04.434 UTC B 3] NVE-MGR-PEER ERROR: Intf state force up successful for peer nodes
[01/01/70 01:55:37.670 UTC C 61] NVE-MGR-PEER ERROR: Intf state force down successful for mcast nodes

#show nve log event

[01/04/70 19:48:51.883 UTC 1DD16 68] NVE-MGR-DB: Return vni 6001 for pi_hdl[0x437C9B68]
[01/04/70 19:48:51.884 UTC 1DD17 68] NVE-MGR-DB: Return pd_hdl[0x1020010] for pi_hdl[0x437C9B68]
[01/04/70 19:48:51.884 UTC 1DD18 68] NVE-MGR-DB: Return vni 6001 for pi_hdl[0x437C9B68]
[01/04/70 19:49:01.884 UTC 1DD19 68] NVE-MGR-DB: Return pd_hdl[0x1020010] for pi_hdl[0x437C9B68]
[01/04/70 19:49:01.884 UTC 1DD1A 68] NVE-MGR-DB: Return vni 6001 for pi_hdl[0x437C9B68]
[01/04/70 19:49:01.885 UTC 1DD1B 68] NVE-MGR-DB: Return pd_hdl[0x1020010] for pi_hdl[0x437C9B68]
[01/04/70 19:49:01.885 UTC 1DD1C 68] NVE-MGR-DB: Return vni 6001 for pi_hdl[0x437C9B68]
[01/04/70 19:49:11.886 UTC 1DD1D 68] NVE-MGR-DB: Return pd_hdl[0x1020010] for pi_hdl[0x437C9B68]
[01/04/70 19:49:11.886 UTC 1DD1E 68] NVE-MGR-DB: Return vni 6001 for pi_hdl[0x437C9B68]
[01/04/70 19:49:11.887 UTC 1DD1F 68] NVE-MGR-DB: Return pd_hdl[0x1020010] for pi_hdl[0x437C9B68]
[01/04/70 19:49:11.887 UTC 1DD20 68] NVE-MGR-DB: Return vni 6001 for pi_hdl[0x437C9B68]
[01/04/70 19:49:21.884 UTC 1DD21 68] NVE-MGR-DB: Return pd_hdl[0x1020010] for pi_hdl[0x437C9B68]

Capture de paquets intégrée

La fonctionnalité Embedded Packet Capture (EPC) disponible dans le logiciel Cisco IOS XE peut fournir des informations supplémentaires pour le dépannage.

Par exemple, cette capture explique le paquet encapsulé par VXLAN :

Configuration EPC (TEST_ACL est la liste d'accès utilisée pour filtrer les données de capture) :

<#root>

#

monitor capture TEST access-list TEST_ACL interface gigabitEthernet0/2/0 both

#

monitor capture TEST buffer size 10

#

monitor capture TEST start

Voici le vidage de paquets qui en résulte :

<#root>

#

show monitor capture TEST buffer dump

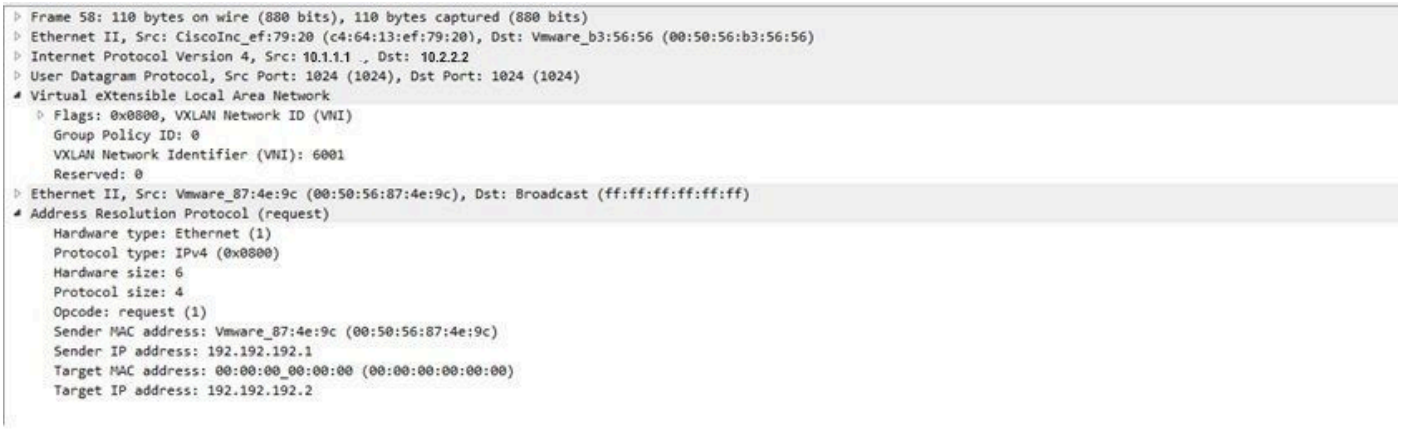
#

monitor capture TEST export bootflash:TEST.pcap

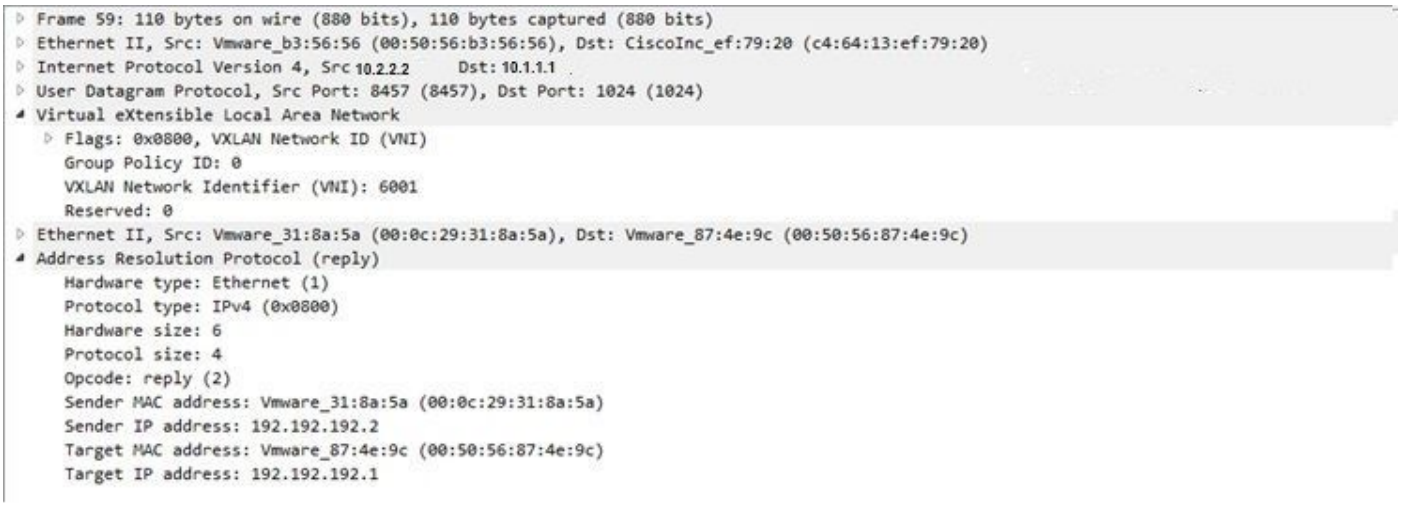
// with this command you can export the capture in pcap format to the bootflash, which can be downloade

Voici un exemple qui explique comment le protocole ICMP (Internet Control Message Protocol) simple fonctionne sur VXLAN.

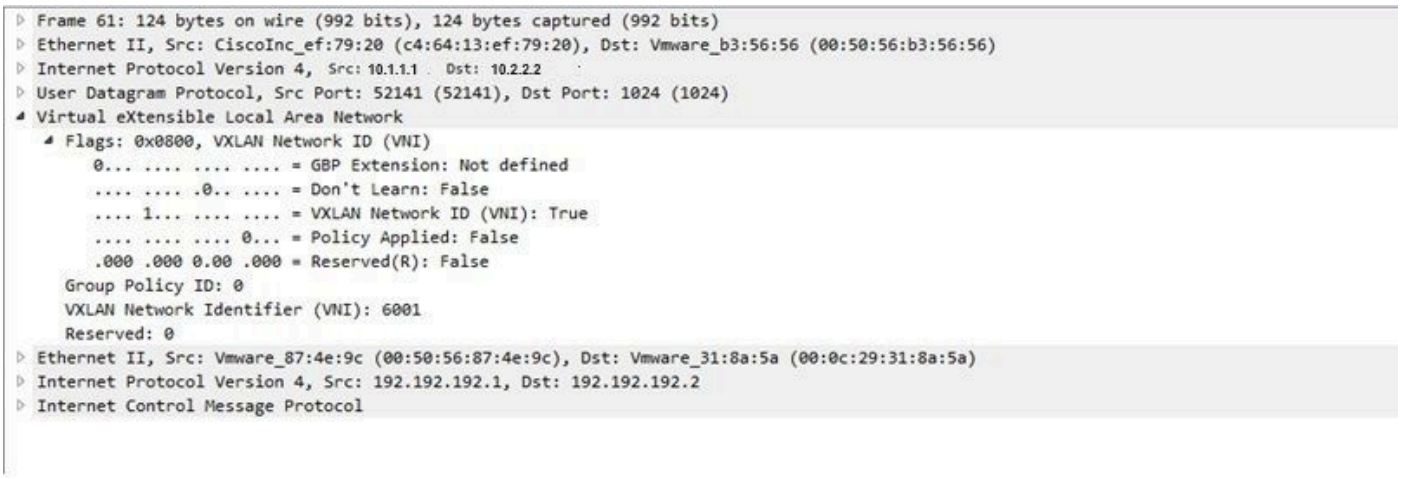
Protocole ARP (Address Resolution Protocol) envoyé sur la superposition VXLAN :



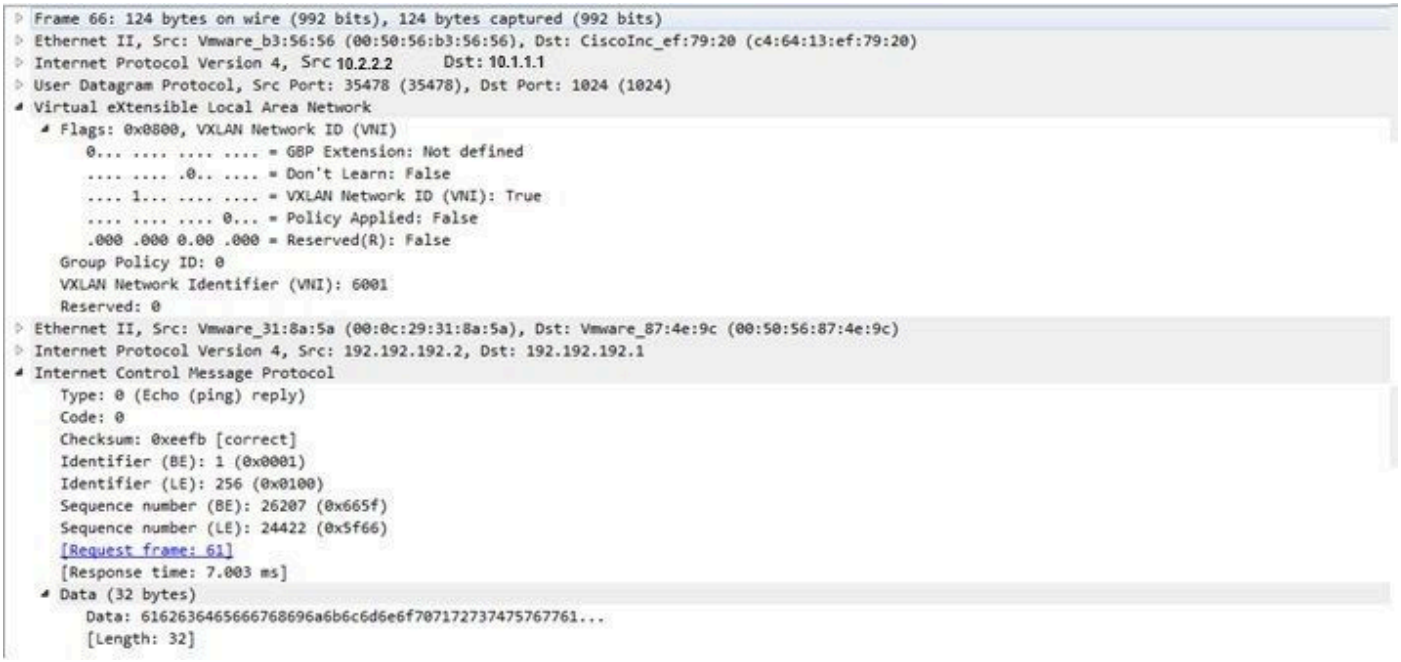
Réponse ARP :



Requête ICMP :



Réponse ICMP :



Commandes de débogage et de dépannage supplémentaires

Cette section décrit quelques commandes de débogage et de dépannage supplémentaires.

Dans cet exemple, les parties en surbrillance du débogage montrent que l'interface NVE n'a pas pu joindre le groupe de multidiffusion. Par conséquent, l'encapsulation VXLAN n'a pas été activée pour VNI 6002. Ces résultats de débogage indiquent des problèmes de multidiffusion sur le réseau.

#debug nve all

*Jan 5 06:13:55.844: NVE-MGR-DB: creating mcast node for **10.0.0.10**

***Jan 5 06:13:55.846: NVE-MGR-MCAST: IGMP add for (0.0.0.0,10.0.0.10) was failure**

*Jan 5 06:13:55.846: NVE-MGR-DB ERROR: Unable to join mcast core tree

*Jan 5 06:13:55.846: NVE-MGR-DB ERROR: Unable to join mcast core tree

***Jan 5 06:13:55.846: NVE-MGR-STATE ERROR: vni 6002: error in create notification to mcast**

***Jan 5 06:13:55.846: NVE-MGR-STATE ERROR: vni 6002: error in create notification to mcast**

*Jan 5 06:13:55.849: NVE-MGR-TUNNEL: Tunnel Endpoint 10.0.0.10 added

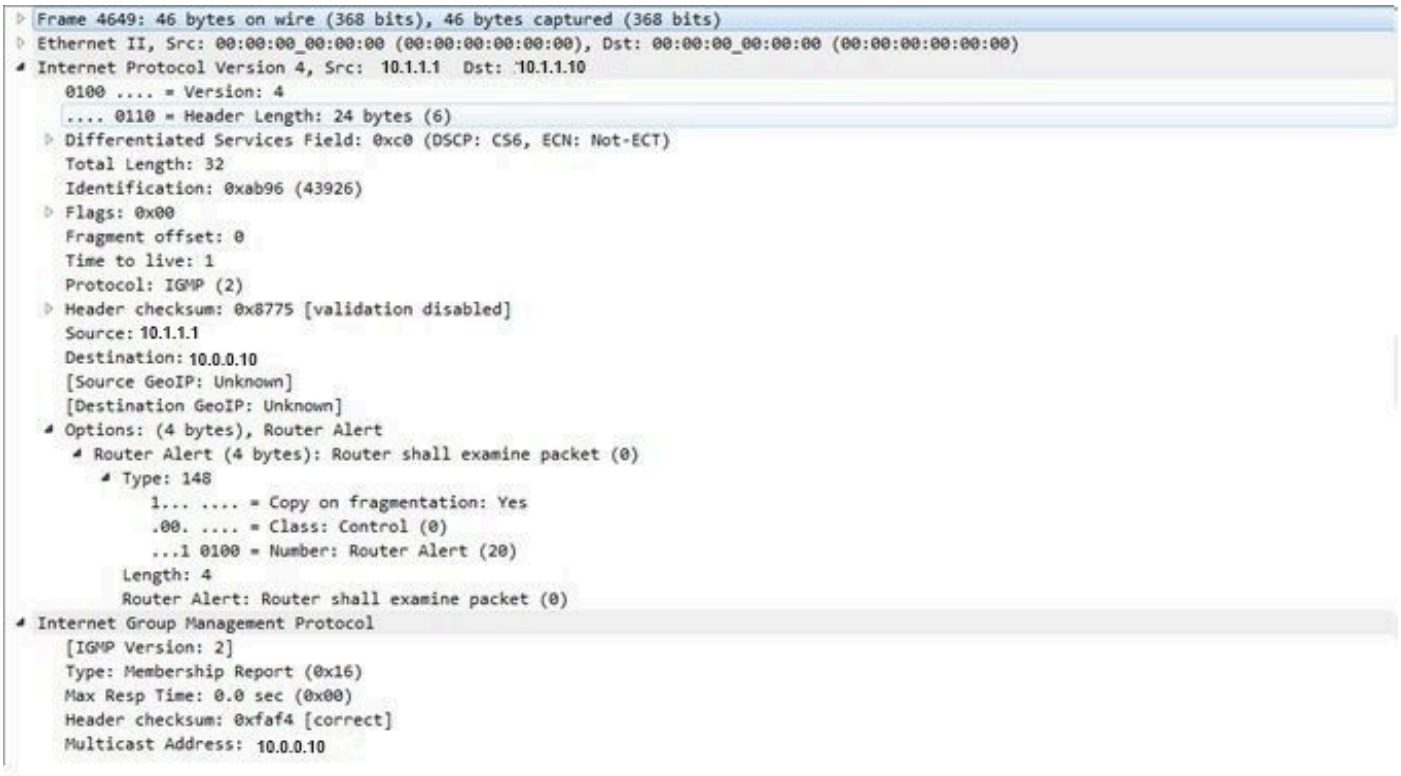
*Jan 5 06:13:55.849: NVE-MGR-TUNNEL: Endpoint 10.0.0.10 added

*Jan 5 06:13:55.851: NVE-MGR-EI: Notifying BD engine of VNI 6002 create

*Jan 5 06:13:55.857: NVE-MGR-DB: Return vni 6002 for pi_hdl[0x437C9B28]

***Jan 5 06:13:55.857: NVE-MGR-EI: VNI 6002: BD state changed to up, vni state to Down**

Voici le rapport d'adhésion au protocole IGMP (Internet Group Management Protocol) qui peut être envoyé une fois que le VNI rejoint le groupe mcast :



Cet exemple montre le résultat de débogage attendu après la configuration d'un VNI sous NVE pour le mode multidiffusion, si la multidiffusion fonctionne comme prévu :

*Jan 5 06:19:20.335: NVE-MGR-DB: [IF 0x14]VNI node creation

*Jan 5 06:19:20.335: NVE-MGR-DB: VNI Node created [437C9B28]

*Jan 5 06:19:20.336: NVE-MGR-PD: VNI 6002 create notification to PD

*Jan 5 06:19:20.336: NVE-MGR-PD: VNI 6002 Create notif successful, map [pd 0x1020017] to [pi 0x437C9B28]

*Jan 5 06:19:20.336: NVE-MGR-DB: creating mcast node for 10.0.0.10

***Jan 5 06:19:20.342: NVE-MGR-MCAST: IGMP add for (0.0.0.0,10.0.0.10) was successful**

***Jan 5 06:19:20.345: NVE-MGR-TUNNEL: Tunnel Endpoint 10.0.0.10 added**

***Jan 5 06:19:20.345: NVE-MGR-TUNNEL: Endpoint 10.0.0.10 added**

*Jan 5 06:19:20.347: NVE-MGR-EI: Notifying BD engine of VNI 6002 create

*Jan 5 06:19:20.347: NVE-MGR-DB: Return pd_hdl[0x1020017] for pi_hdl[0x437C9B28]

*Jan 5 06:19:20.347: NVE-MGR-DB: Return vni 6002 for pi_hdl[0x437C9B28]

*Jan 5 06:19:20.349: NVE-MGR-DB: Return vni state Create for pi_hdl[0x437C9B28]

*Jan 5 06:19:20.349: NVE-MGR-DB: Return vni state Create for pi_hdl[0x437C9B28]

*Jan 5 06:19:20.349: NVE-MGR-DB: Return vni 6002 for pi_hdl[0x437C9B28]

***Jan 5 06:19:20.351: NVE-MGR-EI: L2FIB query for info 0x437C9B28**

*Jan 5 06:19:20.351: NVE-MGR-EI: PP up notification for bd_id 3

*Jan 5 06:19:20.351: NVE-MGR-DB: Return vni 6002 for pi_hdl[0x437C9B28]

*Jan 5 06:19:20.352: NVE-MGR-STATE: vni 6002: Notify clients of state change Create to Up

*Jan 5 06:19:20.352: NVE-MGR-DB: Return vni 6002 for pi_hdl[0x437C9B28]

*Jan 5 06:19:20.353: NVE-MGR-PD: VNI 6002 Create to Up State update to PD successful

*Jan 5 06:19:20.353: NVE-MGR-EI: VNI 6002: BD state changed to up, vni state to Up

*Jan 5 06:19:20.353: NVE-MGR-STATE: vni 6002: No state change Up

*Jan 5 06:19:20.353: NVE-MGR-STATE: vni 6002: New State as a result of create Up

Informations connexes

- **Prise en charge de Cisco CSR 1000V VxLAN**
- **Guide de configuration logicielle des routeurs à services d'agrégation de la gamme Cisco ASR 1000**
- **Assistance technique de Cisco et téléchargements**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.