

Intersight マネージドモードでのネイティブ VLAN の問題のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[トラブルシューティングのシナリオ](#)

[VMware ESXi](#)

[vNIC、FIアップリンク、およびアップストリームネットワークデバイスにネイティブ VLAN が設定されていない](#)

[シナリオ 1. ネイティブ VLAN が vNIC レベルで設定されている](#)

[シナリオ 2. FI アップリンクにネイティブ VLAN が設定されている](#)

[vNIC、FI アップリンク、およびアップストリームネットワークデバイスでネイティブ VLAN が設定されている](#)

[シナリオ 1. ネイティブ VLAN が FI アップリンクに設定されているが、アップストリームデバイスが vNIC に設定されていない](#)

[シナリオ 2. ネイティブ VLAN は vNIC で設定されているが、アップストリームデバイスが FI アップリンクで設定されていない](#)

[Windows Server の OS](#)

[パケット キャプチャ](#)

[シナリオ 1. ネイティブ VLAN は FI アップリンクで設定されるが、vNIC では設定されない](#)

[シナリオ 2. ネイティブ VLAN は FI アップリンクと vNIC で設定される](#)

[シナリオ 3. ネイティブ VLAN が OS および vNIC レベルで設定されている](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Intersight Managed Mode (IME) 環境のネイティブ VLAN 設定オプションについて説明し、一般的なシナリオを取り上げています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Unified Computing Systems (UCS) サーバに関する基本知識
- Intersight Managed Mode (IMM) に関する基本的な知識
- ESXi および Windows オペレーティングシステムの基本知識
- ネットワーキングの基本知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Intersight マネージドモード (IMM)
- UCSX-215C-M8
- UCSC-C240-M7SX
- 6536 ファブリック インターコネクト
- 6454 ファブリック インターコネクト
- サーバ X シリーズ ファームウェア バージョン 5.3 (0.240016)
- Fabric Interconnect 6536 ファームウェア バージョン 4.3 (5.250004)
- サーバ C シリーズ ファームウェア バージョン 4.3 (4.241063)
- Fabric Interconnect 6536 ファームウェア バージョン 4.2 (3m)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Intersight Managed Mode 環境のネイティブ VLAN 設定オプションには、二重タギングの原因となる一般的なシナリオがあります。また、この記事では、推奨されるトラブルシューティングの手順についても説明します。

Cisco UCS では、NIC アダプタが仮想化され、vNIC を介して OS に提供されます。これらの仮想アダプタは、通常は トランク ポート として設定される 仮想イーサネット インターフェイス (vEthernet) に接続されます。ネイティブ VLAN は、タグなしのトラフィック (または 802.1Q タグを使用しないトラフィック) を トランク ポート 経由で 伝送 するために使用されます。

インストールされている OS によっては、それ自体のトラフィックのタギングを行う機能がある場合と行わない場合があります。たとえば、VMware ESXi には、複数の VLAN にタグを付ける機能があります。VLAN タギングが使用できないか不要であるオペレーティングシステムでは、タグなしトラフィックに使用するデフォルト VLAN にネイティブ VLAN を選択することをお勧めします。

トラブルシューティングのシナリオ

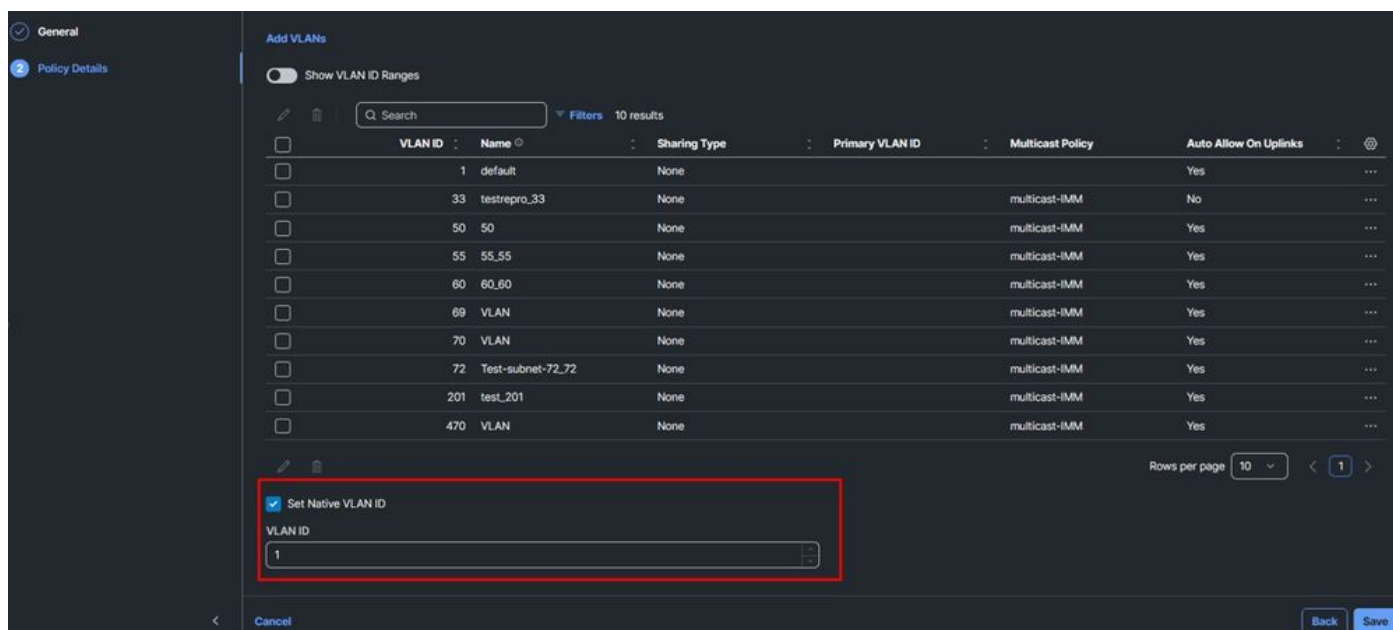
VMware ESXi

vNIC、FI アップリンク、および アップストリーム ネットワーク デバイス に ネイティブ VLAN が 設定 されていない

この例では、VLAN 470 および 72 が 環境内 で 使用 されます。次に、稼働シナリオの例を示します。

- アップリンクにネイティブVLANが設定されていない。

ドメインプロフィール :



CLIの場合 :

FI-A:

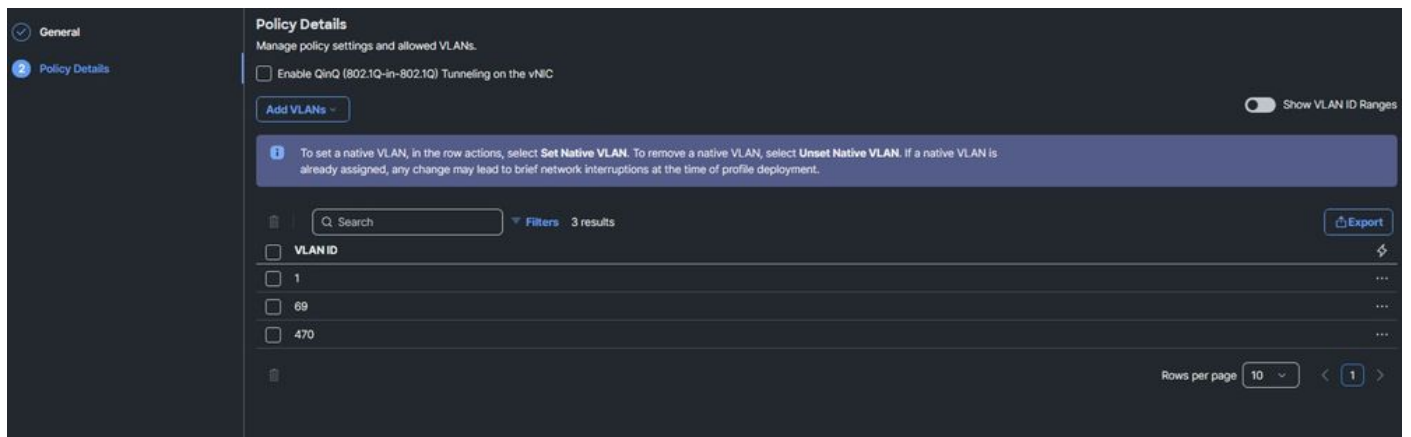
```
6536-A(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
pinning border
switchport mode trunk
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

FI-B:

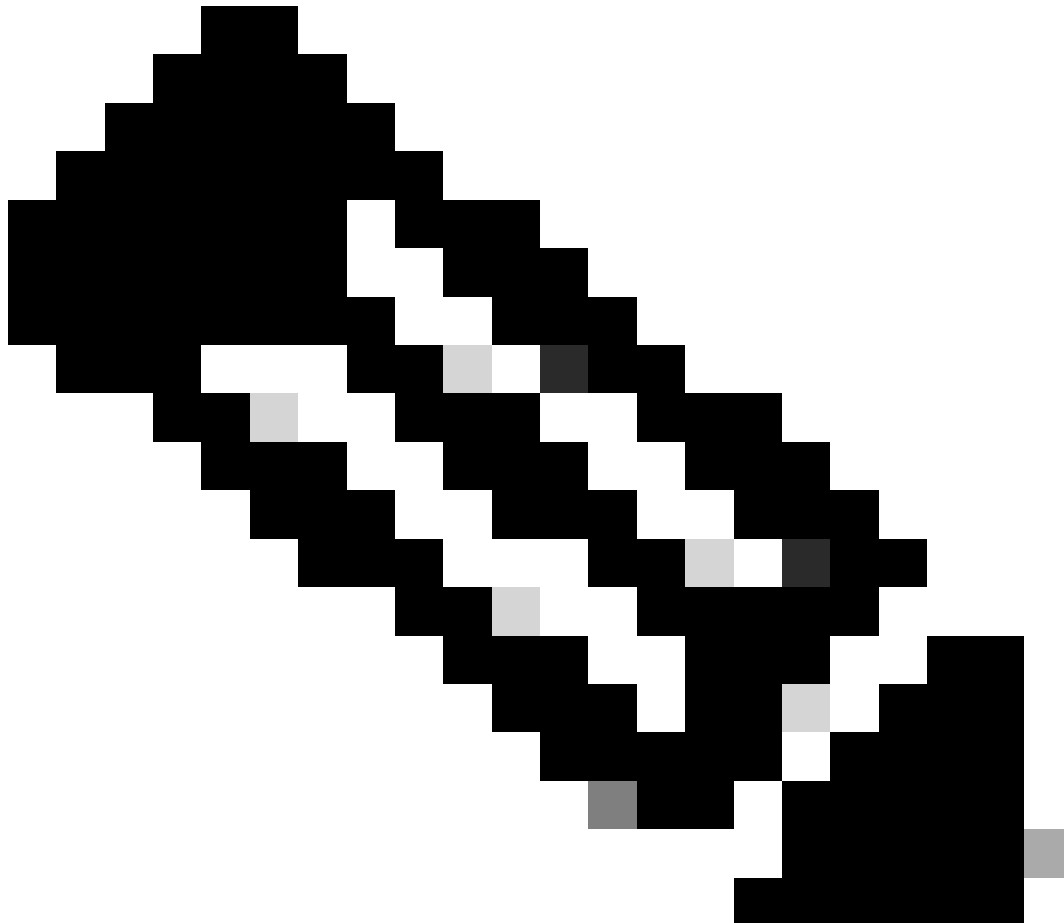
```
6536-B(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
pinning border
switchport mode trunk
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

- vNICでネイティブVLANが設定されていない

イーサネットネットワークグループポリシー :



CLIの場合：



注：サーバのvEthernetは、Servers > Inventory > Network Adaptersの順に選択し、VICカードを選択してInterfacesをクリックすると表示されます。

General

Inventory

UCS Server Profile

HCL

Topology

Metrics

Connectivity

Expand All

Motherboard

Boot

Management Controller

CPUs

Memory

Network Adapters

- Adapter UCSX-ME-V5Q50G_FCH281175L9
- Adapter UCSX-ML-V5Q50G_FCH2817742H

Storage Controllers

TPM

Adapter UCSX-ML-V5Q50G_FCH2817742H

General

Interfaces

DCE Interfaces

Name	OperState	IO Module Port	MAC Address
1	up	chassis-1-loc-2-muxhostport-port-29	EC:19:2E:56:5A:09
2	up	chassis-1-loc-2-muxhostport-port-30	EC:19:2E:56:5A:0A
3	up	chassis-1-loc-1-muxhostport-port-29	EC:19:2E:56:5A:0B
4	up	chassis-1-loc-1-muxhostport-port-30	EC:19:2E:56:5A:0C

NIC Interfaces

Name	MAC Address	QinQ VLAN	VIF ID	Active Oper State	Passive VIF ID	Passive Oper State	QoS Policy	Rate Limit (Mbps)
vNIC-A	00:25:85:01:00:34	-	800	Up	-	-	IMM-QOS	100000
vNIC-B	00:25:85:01:00:35	-	801	Up	-	-	IMM-QOS	100000

HBA Interfaces

Name	WWPN	VIF ID	Oper State	QoS Policy	Rate Limit (Mbps)
------	------	--------	------------	------------	-------------------

NO ITEMS AVAILABLE

FI-A:

```
6536-A(nx-os)# show running-config interface vethernet 800
interface Vethernet800
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

FI-B:

```
6536-B(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

- OSで設定されているVLAN:

Configure Management Network	VLAN (optional)
Network Adapters VLAN (optional) IPv4 Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	470 A VLAN is a virtual network within a physical network. Because several VLANs can co-exist on the same physical network segment, VLAN configuration and partitioning is often more flexible, better isolated, and less expensive than flat networks based on traditional physical topology. If you are unsure how to configure or use a VLAN, it is safe to leave this option unset.

- pingテストが成功しました。

```
C:\Users\ >ping 10.31.123.106

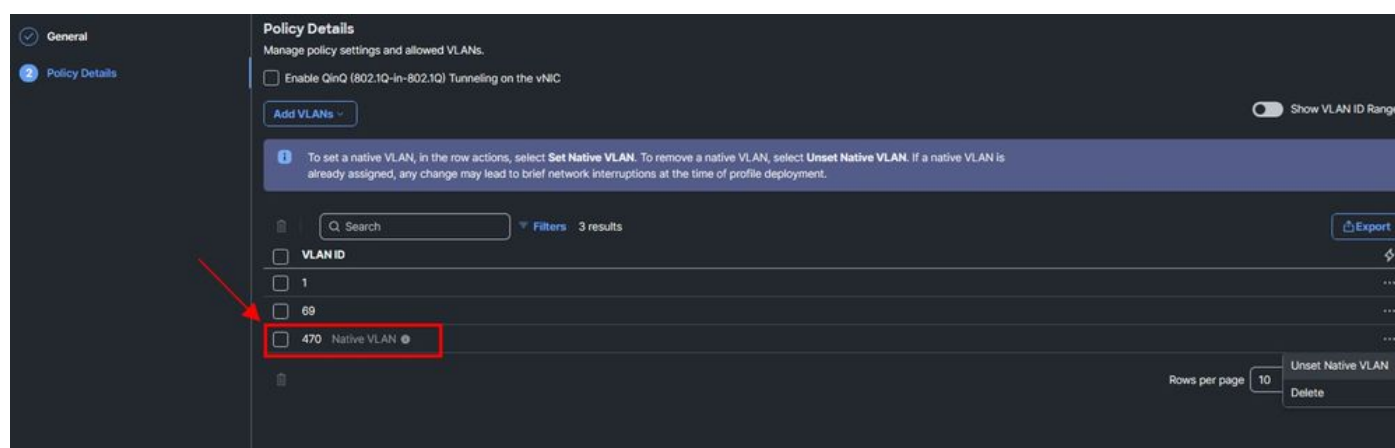
Pinging 10.31.123.106 with 32 bytes of data:
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64
Reply from 10.31.123.106: bytes=32 time<1ms TTL=64

Ping statistics for 10.31.123.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

シナリオ 1.ネイティブVLANがvNICレベルで設定されている

イーサネットネットワークグループでVLANをネイティブとして設定すると、VLANタギングの問題が原因でネットワーク接続が失われる可能性があります。

- イーサネットネットワークグループの設定：



CLIの場合：

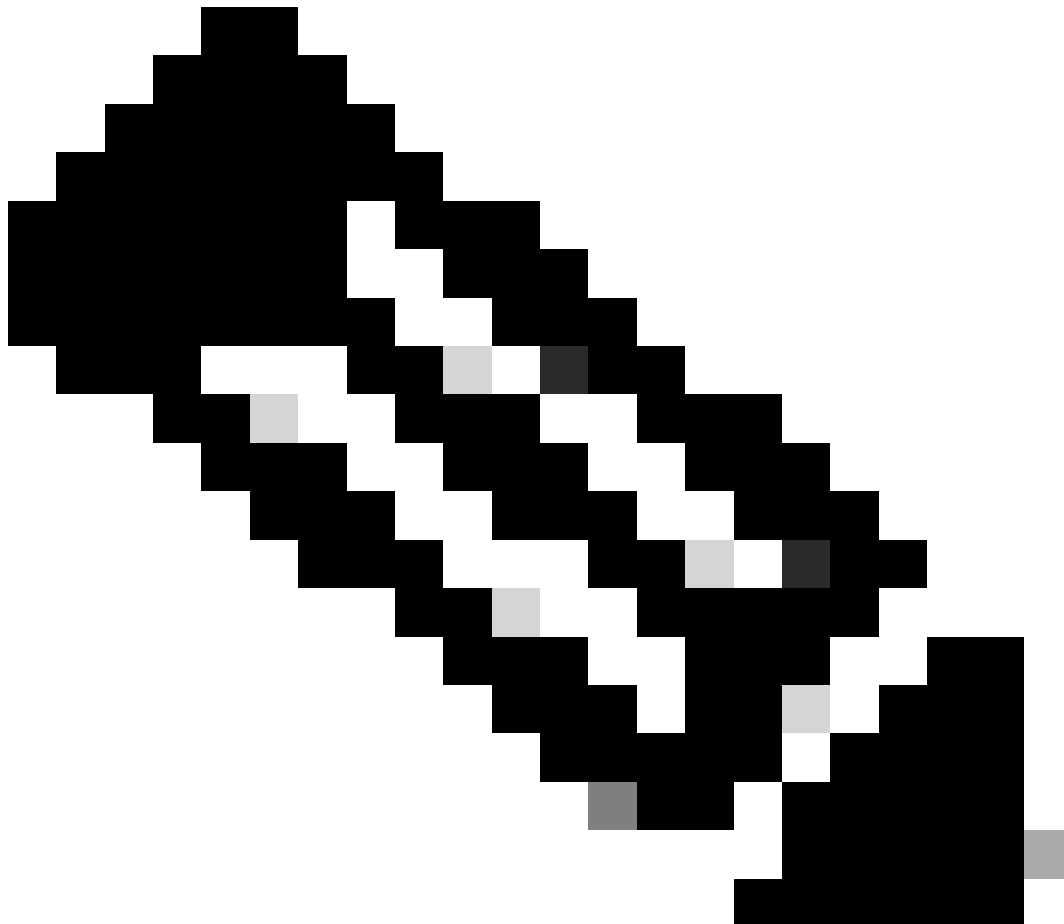
FI-A:

```
6536-A(nx-os)# show running-config interface vethernet 800
interface Vethernet800
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

FI-B:

```
6536-B(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

- pingテストが失敗する
-



注:NetworkグループからネイティブVLANを削除すると、接続は回復します。

シナリオ 2.FIアップリンクにネイティブVLANが設定されている

- V1a CLI:

FI A

```
6536-A(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
switchport mode trunk
switchport trunk native vlan 470 <<<<<<<<<<
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

FI-B

```
6536-B(nx-os)# show running-config interface ethernet 1/1
switchport mode trunk
switchport trunk native vlan 470 <<<<<<<<<<
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

アップリンクに設定されているネイティブVLANを使用してOSにpingを実行しようとすると、pingテストは失敗します。

この状態を修正するには、アップリンクからVLANを削除し、VLANをESXi(OS)レベルで設定したままにする必要があります。

vNIC、FIアップリンク、およびアップストリームネットワークデバイスでネイティブVLANが設定されている

この再現のために、別のVLANが使用されました。このシナリオでは、使用されるVLANは72です。

考慮事項:

1. VLAN 72はCatalyst DGにネイティブとして設定されています
2. VLAN 72は、Nexusデバイスにネイティブとして設定されています
3. VLAN 72は、FIアップリンクでネイティブとして設定されます
4. VLAN 72は、vNICでネイティブとして設定されています
5. VLANはOSでタグ付けされません。

Configure Management Network	VLAN (optional)
Network Adapters VLAN (optional) IPv4 Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	Not set A VLAN is a virtual network within a physical network. Because several VLANs can co-exist on the same physical network segment, VLAN configuration and partitioning is often more flexible, better isolated, and less expensive than flat networks based on traditional physical topology. If you are unsure how to configure or use a VLAN, it is safe to leave this option unset.

次の考慮事項を使用して、pingテストを実行すると、pingが期待どおりに動作していることを確認できます。

Testing Management Network

You may interrupt the test at any time.

Pinging address #1 (192.168.72.1).
Pinging address #2 (192.168.72.25).

OK.
OK.

OSレベルでのパケットキャプチャ：

データプレーンが期待どおりに動作しているかどうかを確認するもう1つの方法では、OSレベルでパケットキャプチャを実行できます。このトラブルシューティング記事では、pktcap-uwツールを使用して、物理ネットワークアダプタを通過するトラフィックをキャプチャしました。次に例を示します。

```
pktcap-uw --uplink vmnic0 --dir 2 -o /vmfs/volumes/datastore1/pcaps/nativeworking.pcap -i icmp:
```

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	10.31.123.45	192.168.72.25	ICMP	74	Echo (ping) request id=0x000a, seq=12681/35121, ttl=127 (reply in 2)
← 2	0.000112	192.168.72.25	10.31.123.45	ICMP	74	Echo (ping) reply id=0x000a, seq=12681/35121, ttl=64 (request in 1)
7	1.018514	10.31.123.45	192.168.72.25	ICMP	74	Echo (ping) request id=0x000a, seq=12682/35377, ttl=127 (reply in 8)
8	1.018625	192.168.72.25	10.31.123.45	ICMP	74	Echo (ping) reply id=0x000a, seq=12682/35377, ttl=64 (request in 7)

ELAMキャプチャ：

ELAMキャプチャは、ネイティブVLANの問題をトラブルシューティングするときに役立ちます。このツールでは、ASICレベルで転送されているパケットのリアルタイムビューが可能です。トラブルシューティングの目的で、データプレーンを中断せずに「送信元および宛先デバイスのMACアドレスおよびIPアドレス」だけに焦点を当てます。

パケットが動作している場合の例：

```
root@IMM-SAAS-MXSVLAB-6536-A(nx-os)# attach module 1
root@module-1# debug platform internal tah elam asic 0
root@module-1(TAH-elam)# trigger init asic 0 slice 1 lu-a2d 1 in-select 6 out-select 0
Slot 1: param values: start asic 0, start slice 1, lu-a2d 1, in-select 6, out-select 0
root@module-1(TAH-elam-inse16)# set outer ipv4 src_ip 192.168.72.25 dst_ip 192.168.72.1
root@module-1(TAH-elam-inse16)# start
root@module-1(TAH-elam-inse16)# report
HEAVENLY ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 1
=====
```

```
Incoming Interface: Eth1/10
Src Idx : 0x1001, Src BD : 72
Outgoing Interface Info: dmod 1, dpid 72
Dst Idx : 0x601, Dst BD : 72
```

Packet Type: IPv4

```
Dst MAC address: B0:8B:CF:C8:A2:6B
Src MAC address: 00:25:B5:01:00:34
.lq Tag0 VLAN: 72, cos = 0x0
```

```
Dst IPv4 address: 192.168.72.1
Src IPv4 address: 192.168.72.25
```

```
Ver      = 4, DSCP      = 0, Don't Fragment = 0
Proto    = 1, TTL       = 64, More Fragments = 0
Hdr len  = 20, Pkt len  = 84, Checksum      = 0xc0a9
```

```
L4 Protocol : 1
ICMP type    : 8
ICMP code    : 0
```

Drop Info:

```
LUA:
LUB:
LUC:
LUD:
Final Drops:
```

```
vntag:
vntag_valid : 1
vntag_vir   : 195
vntag_svif  : 195
```

得られた出力から、srcとdstがVLAN 72にあることがわかります。これは、すべてのパスでネイティブとしてVLAN 72を使用しており、dpid 72インターフェイスの宛先であるポートイーサネット1/10に到達しているためです。dpidはASICポートの内部識別子で、マッピングはshow interface hardware-mappingsを使用して確認できます。

```
6536-A(nx-os)# show interface hardware-mappings
```

Name	Ifindex	Smod	Unit	HPort	FPort	NPort	VPort	Slice	SPort	SrcId	MacId	MacSP	VIF	Block	BlkSrcID
Eth1/1	1a000000	1	0	72	255	0	-1	1	0	0	18	0	1537	0	0

```
6536-A(nx-os)# show hardware internal tah interface ethernet 1/1
```

```
#####
```

```
IfIndex: 0x1a000000
```

```
DstIndex: 6144
```

```
IfType: 26
```

```
Asic: 0
```

```
Asic: 0
```

```
AsicPort: 72
```

```
SrcId: 0
```

```
Slice: 1
```

```
PortOnSlice: 0
```

```
Table entries for interface Ethernet1/1
```

show interface hardware-mappingsコマンドで取得された情報に基づくと、宛先ポートはUCSドメインのアップリンクの1つであるポートEthernt 1/1です。

シナリオ 1. ネイティブVLANがFIアップリンクに設定されているが、アップストリームデバイスがvNICに設定されていない

今回は、ネイティブVLANがvNICから削除されているため、ICMP要求が機能しなくなることが明らかです。

ELAMキャプチャ。

この場合、pingを実行できません。送信元と宛先のIPアドレスを使用しようとしても、接続がないため機能しません。この特定のケースでは、MACアドレスをフィルタとして設定し、詳細な情報を取得します。

```
root@module-1(TAH-elam-inse16)# set outer 12 src_mac 00:25:B5:01:00:34 dst_mac ff:ff:ff:ff:ff:ff
root@module-1(TAH-elam-inse16)# start
root@module-1(TAH-elam-inse16)# report
HEAVENLY ELAM REPORT SUMMARY
slot - 1, ASIC - 0, slice - 1
=====
```

```
Incoming Interface: Eth1/10
Src Idx : 0x1001, Src BD : 1
Outgoing Interface Info: dmod 1, dpid 72
Dst Idx : 0x601, Dst BD : 72
```

Packet Type: ARP

```
Dst MAC address: FF:FF:FF:FF:FF:FF
Src MAC address: 00:25:B5:01:00:34
.1q Tag0 VLAN: 1, cos = 0x0
```

```
Target Hardware address: 00:00:00:00:00:00
Sender Hardware address: 00:25:B5:01:00:34
Target Protocol address: 192.168.72.1
Sender Protocol address: 192.168.72.25
ARP opcode: 1
```

Drop Info:

```
LUA:
LUB:
LUC:
LUD:
Final Drops:
```

```
vntag:
vntag_valid : 1
vntag_vir : 195
vntag_svif : 195
```

6536-A(nx-os)# show interface hardware-mappings

Name	Ifindex	Smod	Unit	HPort	FPort	NPort	VPort	Slice	SPort	SrcId	MacId	MacSP	VIF	Block	BlkSrcID
Eth1/1	1a000000	1	0	72	255	0	-1	1	0	0	18	0	1537	0	0

MACアドレス00:25:B5:01:00:34(vNIC-A)が使用しているVLANがVLAN 1であることがわかります。これはVLAN 72を使用する必要があるので正しくありません。

シナリオ 2.ネイティブVLANはvNICで設定されているが、アップストリームデバイスがFIアップリンクで設定されていない

ELAMキャプチャ：

```
root@module-1(TAH-elam-inse16)# set outer 12 src_mac 00:25:B5:01:00:34 dst_mac ff:ff:ff:ff:ff:ff
root@module-1(TAH-elam-inse16)# start
root@module-1(TAH-elam-inse16)# report
HEAVENLY ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 1
=====
```

```
Incoming Interface: Eth1/10
Src Idx : 0x1001, Src BD : 72
Outgoing Interface Info: met_ptr 0
```

Packet Type: ARP

```
Dst MAC address: FF:FF:FF:FF:FF:FF
Src MAC address: 00:25:B5:01:00:34
.lq Tag0 VLAN: 72, cos = 0x0
```

```
Target Hardware address: 00:00:00:00:00:00
Sender Hardware address: 00:25:B5:01:00:34
Target Protocol address: 192.168.72.1
Sender Protocol address: 192.168.72.25
ARP opcode: 1
```

Drop Info:

```
LUA:
LUB:
LUC:
LUD:
Final Drops:
```

```
vntag:
vntag_valid    : 1
vntag_vir      : 195
vntag_svif     : 195
```

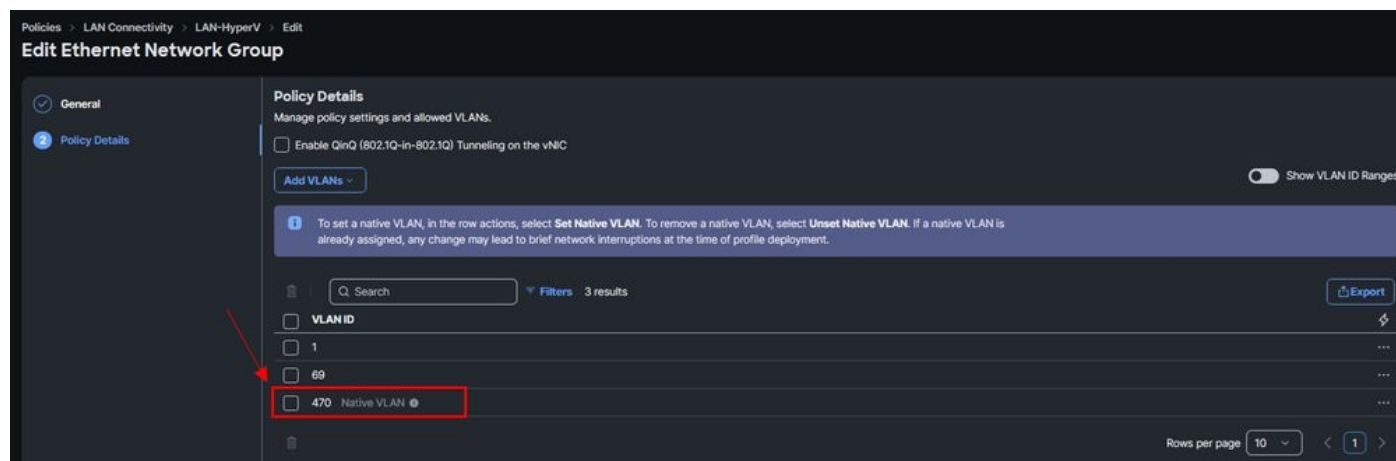
出力から、正しいVLAN 72が使用されていることがわかります。ただし、アップリンクの設定を確認すると、ネイティブVLANが設定されていないことがわかります。

```
6536-A(nx-os)# show running-config interface ethernet 1/1
description Uplink PC Member
switchport mode trunk
switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

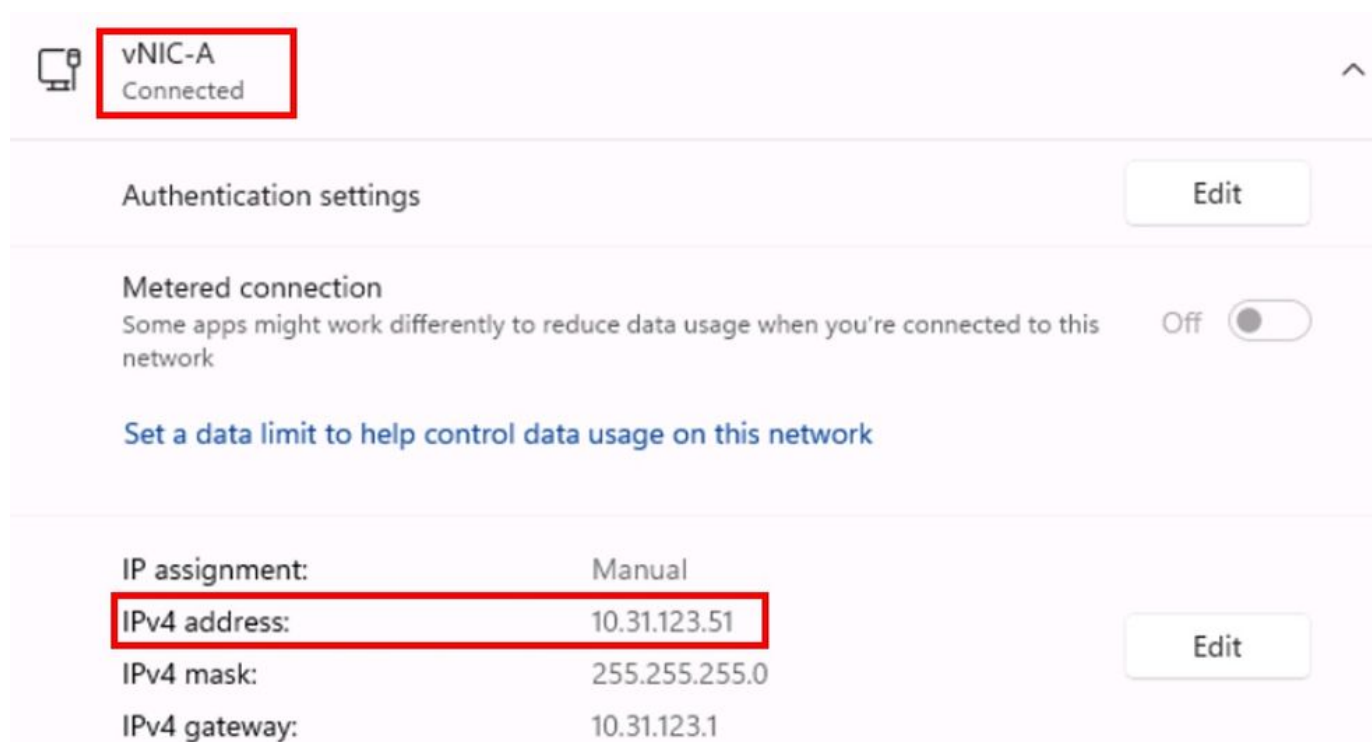
Windows ServerのOS

ネイティブVLANの問題は、Windows OSにも存在する可能性があります。通常、この問題は、ネイティブVLANがvNICでタグ付けされていないために発生する可能性があります。

このシナリオでは、ネイティブVLAN 470が使用されました。



使用されるvNICはWindowsで接続されます。



パケット キャプチャ

ネットワークにpingを実行すると、ネイティブVLANがvNICでタグ付けされているため、パケットキャプチャが期待どおりに動作していることが確認できます。

No.	Time	Source	Destination	Protocol	Length	Info
1632	157.599402	10.31.123.45	10.31.123.51	ICMP	74	Echo (ping) request id=0x000a, seq=29175/63345, ttl=128 (reply in 1632)
1632	157.599645	10.31.123.51	10.31.123.45	ICMP	74	Echo (ping) reply id=0x000a, seq=29175/63345, ttl=128 (request in 1631)
1634	157.881196	10.61.94.90	10.31.123.51	ICMP	74	Echo (ping) request id=0x0002, seq=6442/10777, ttl=106 (reply in 1635)
1635	157.881469	10.31.123.51	10.61.94.90	ICMP	74	Echo (ping) reply id=0x0002, seq=6442/10777, ttl=128 (request in 1634)

シナリオ 1.ネイティブVLANはFIアップリンクで設定されるが、vNICでは設定されない

- vNICレベル :

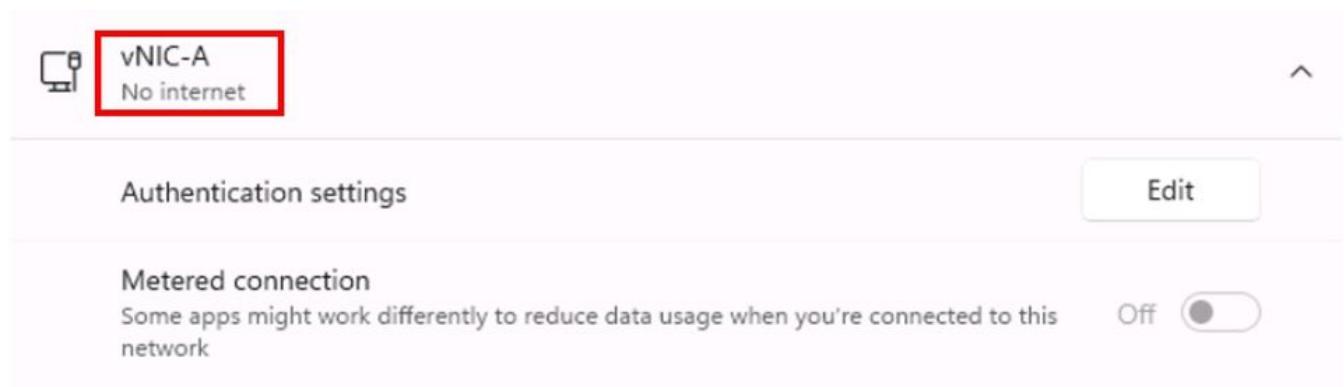
```
6454-A(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

- FI-Aレベル :

```
6454-A(nx-os)# show running-config interface ethernet 1/15-16
interface Ethernet1/15
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470

interface Ethernet1/16
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470
```

使用されるvNICがWindowsに接続されていない :



pingを実行しようとしても、これは機能しないはずです。

シナリオ 2.ネイティブVLANはFIアップリンクとvNICで設定される

- vNICレベル :

```
6454-A(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

- FI-Aレベル :

```
IMM-SAAS-MXSVLAB-6454-A(nx-os)# show running-config interface ethernet
interface Ethernet1/15
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470

interface Ethernet1/16
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470
```

この設定では接続が許可されません。pingテストを実行しても応答がないことが予想されます。

シナリオ 3.ネイティブVLANがOSおよびvNICレベルで設定されている

- OS側 :

NIC Teaming

×

New team interface

VLAN 470 - VLAN 470

Team: VLAN 470

Type: Primary interface

VLAN membership

☐ **Default**
The default interface handles all traffic that is not claimed by other VLAN-specific interfaces.

☒ **Specific VLAN:**

←

OK Cancel

- vNICレベル :

```
6454-A(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

- pingテストが機能せず、接続できない。

関連情報

- [Cisco Intersightマネージドモード設定ガイド](#)
- [UCSでのCisco ELAMの設定](#)
- [pktcap-uwツールを使用したESXiでのパケットキャプチャ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。