Troubleshoot Native VLAN Issues on Intersight Managed Mode

Contents

Introduction

This document describes the native VLAN configuration options in a Cisco Intersight-Managed Mode environment, highlighting common scenarios.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding on Unified Computing Systems servers (UCS)
- Basic understanding of Intersight Managed Mode (IMM)
- Basic understanding of ESXi and Windows Operating system
- Basic understanding of Networking

Components Used

The information in this document is based on these software and hardware versions:

- Intersight Managed Mode (IMM)
- UCSX-215C-M8
- UCSC-C240-M7SX
- 6536 Fabric Interconnect
- 6454 Fabric Interconnect
- Server X series Firmware version 5.3(0.240016)
- Fabric interconnect 6536 Firmware version 4.3(5.250004)
- Server C series Firmware version 4.3(4.241063)
- Fabric interconnect 6536 Firmware version 4.2(3m)

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Native VLAN configuration options in a Cisco Intersight-Managed Mode environment have common scenarios that lead to double-tagging. This article additionally provides recommended troubleshooting steps.

In Cisco UCS, the NIC adapters are virtualized and presented to the OS via vNICS. These virtual adapters are connected to a virtual ethernet interface (vEthernet) that is usually configured as a trunk port. The native VLAN is used to carry untagged traffic (or traffic that does not use the 802.1Q tag) over a trunk port.

Depending on the installed OS, it can have the capability or not to do tagging of its own traffic. For example VMWare ESXi has the capability to tag multiple VLANs. For operating systems where VLAN tagging is unavailable or unnecessary, it is advisable to select a native VLAN for the default VLAN you wish to use for untagged traffic.

Troubleshooting Scenarios

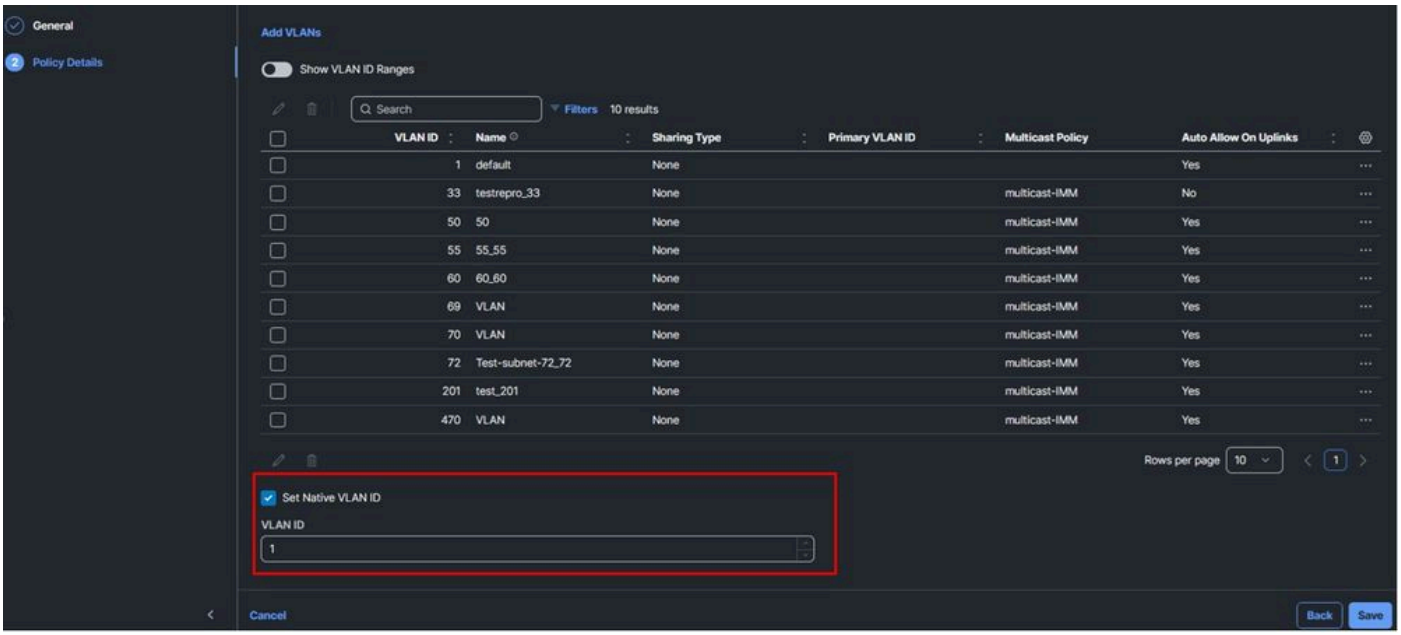
VMware ESXi

Native VLAN not Configured on the vNIC, FI Uplinks nor Upstream Network Devices

In this example, VLANs 470 and 72 are used within the environment. Here is an example with a working scenario.

- No native VLAN configured in the uplinks.

Domain profile:



Via CLI:

FI-A:

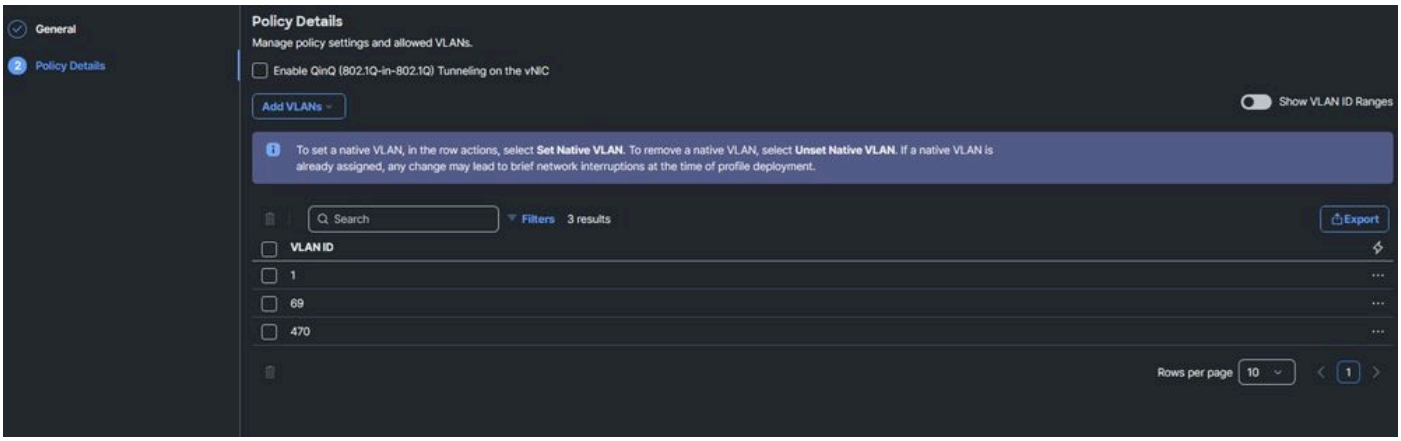
```
6536-A(nx-os)# show running-config interface ethernet 1/1
  description Uplink PC Member
  pinning border
  switchport mode trunk
  switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

FI-B:

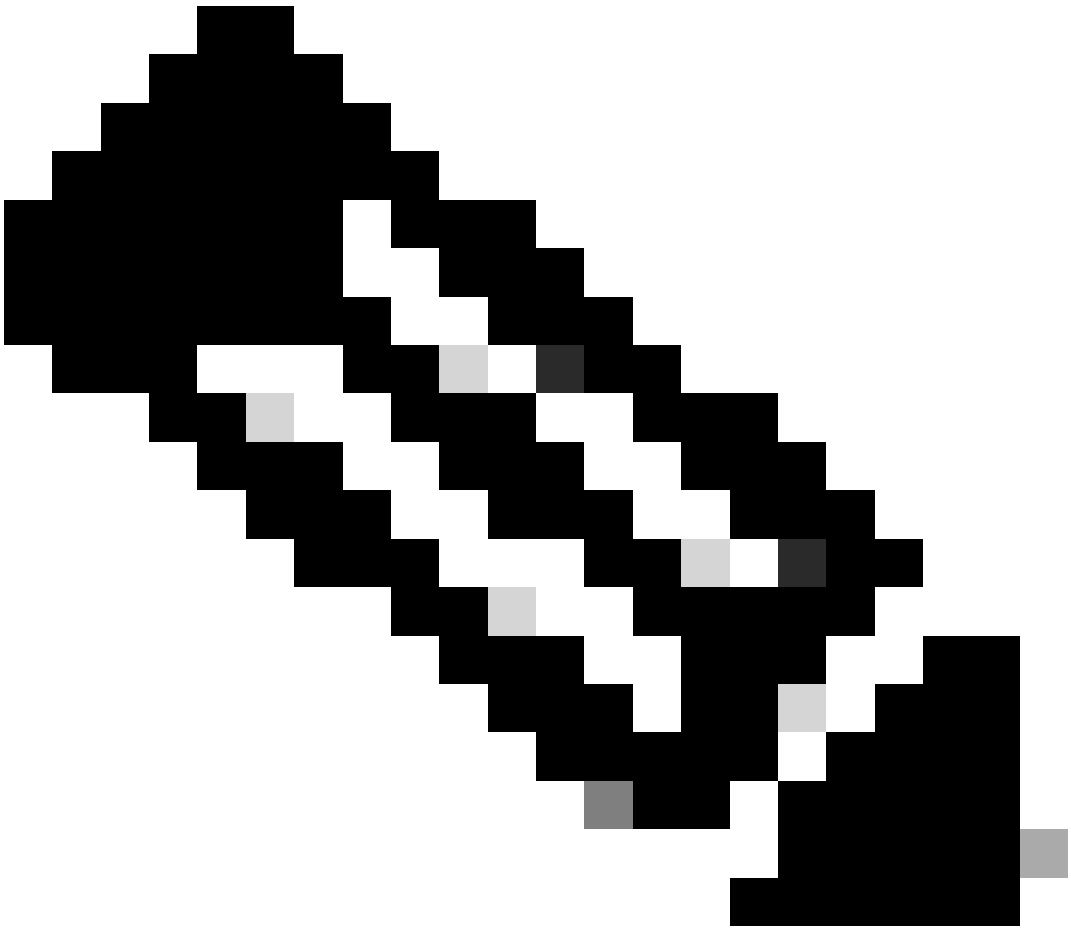
```
6536-B(nx-os)# show running-config interface ethernet 1/1
  description Uplink PC Member
  pinning border
  switchport mode trunk
  switchport trunk allowed vlan 1,50,55,60,69-70,72,201,470
```

- No native VLAN configures in the vNICs.

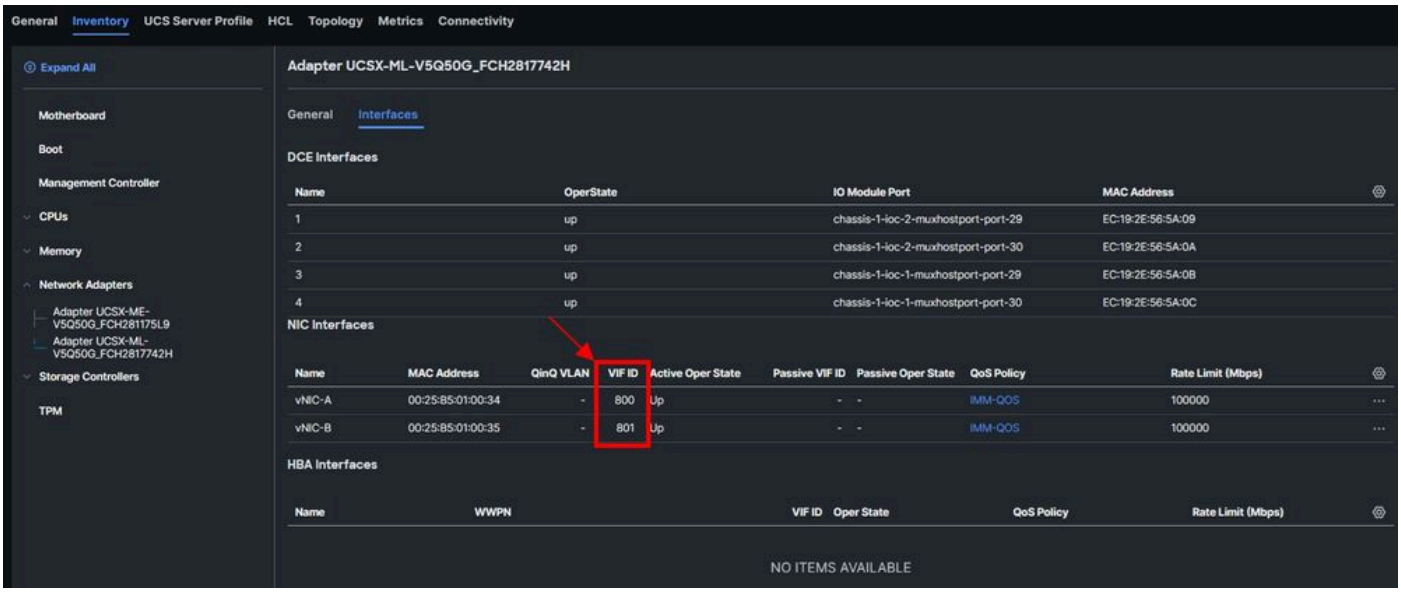
Ethernet Network Group policy:



Via CLI:



Note: You can see the vEthernets in your servers through the path **Servers > Inventory > Network Adapters**, then select the **VIC card** and click **Interfaces**.



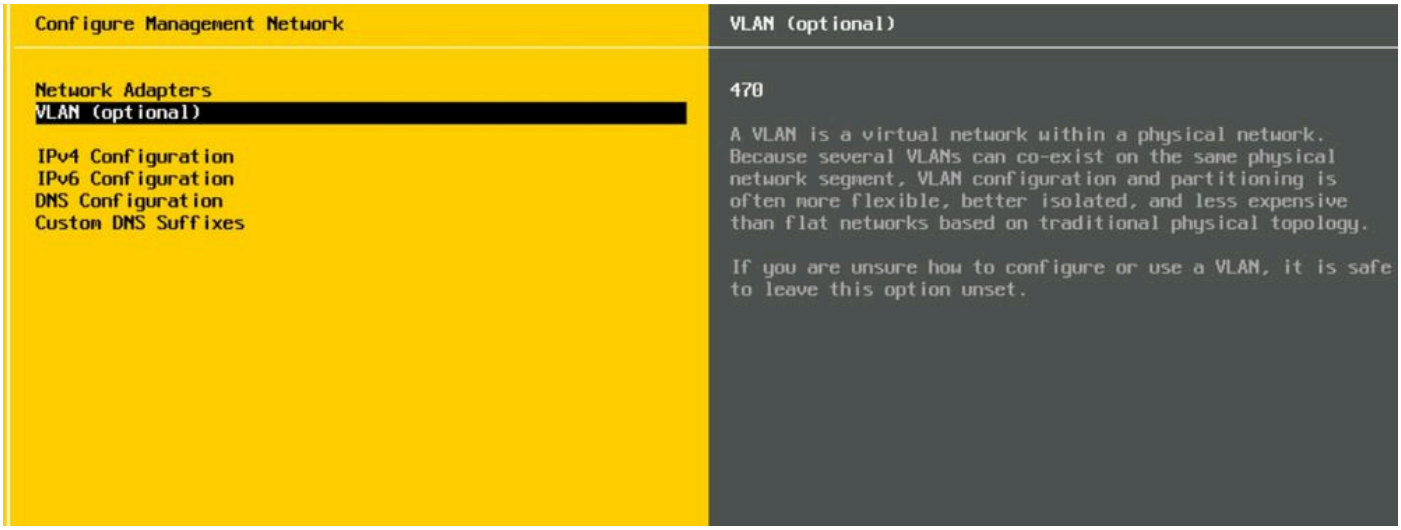
FI-A:

```
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
```

- VLAN configured in OS:



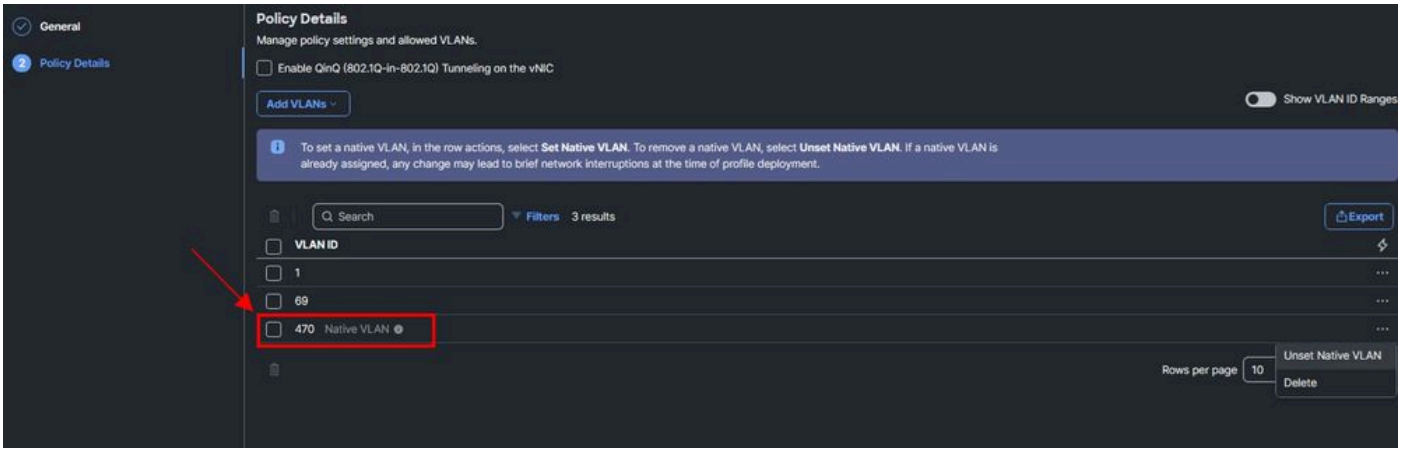
- Ping test is successful:

```
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
```

Scenario 1. Native VLAN is Configured at the vNICs Level

If you configure the VLAN as Native in the Ethernet Network group, this can cause network connectivity loss due the VLAN tagging issues.

- Configuration in the Ethernet Network Group:



Via CLI:

FI-A:

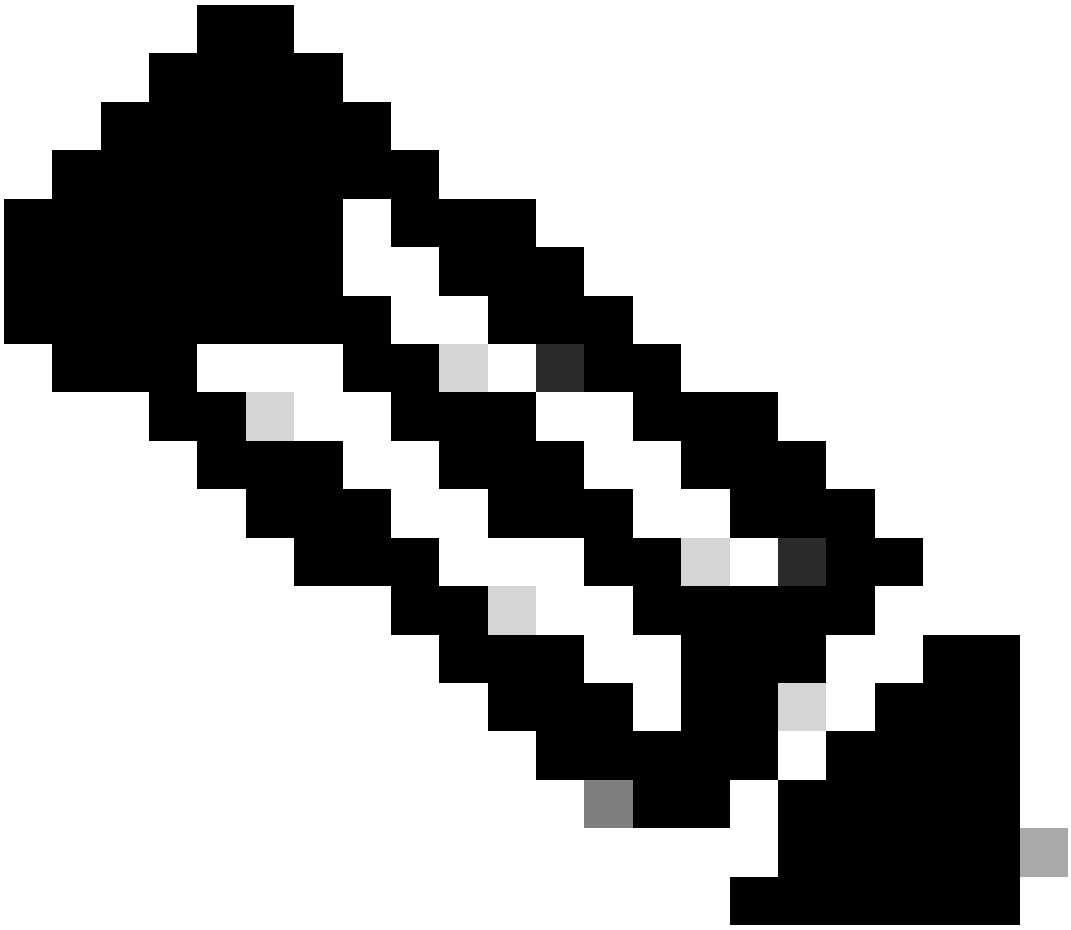
```
6536-A(nx-os)# show running-config interface vethernet 800
interface Vethernet800
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69,470
```

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 test is unsuccessful.



Note: Once you remove the Native VLAN from the Network group, the connectivity is recovered.

Scenario 2. Native VLAN is Configured in the FI Uplinks

- VIa 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
```

If you try to ping the OS with the Native VLAN configured in the uplinks, the ping test is unsuccessful.

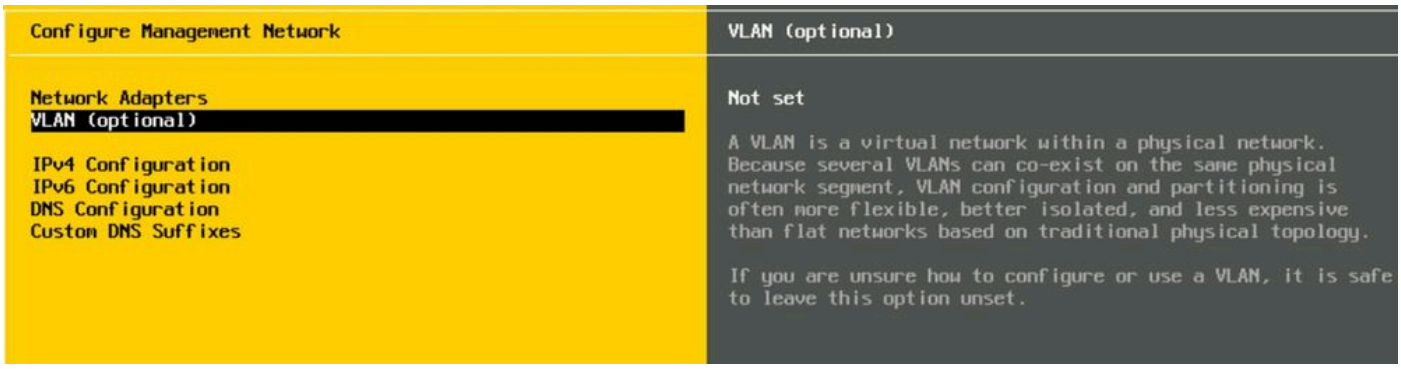
To fix this condition, you need to remove the VLAN from the uplink and leave the VLAN configured at the ESXi (OS) level.

Native VLAN is Configured at the vNICs, FI Uplinks and Upstream Network Devices

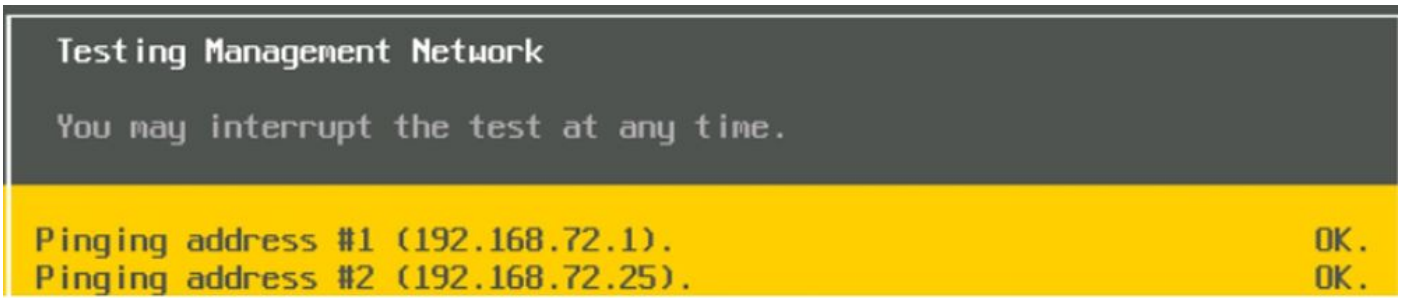
For this recreation, another VLAN was used. In this scenario, the VLAN used is 72.

Considerations:

1. VLAN 72 is configured as Native into our Catalyst DG.
2. VLAN 72 is configured as Native into our Nexus device.
3. VLAN 72 is configured as Native in the FI uplinks.
4. VLAN 72 is configured as Native in the vNICs.
5. VLAN is not tagged in the OS.



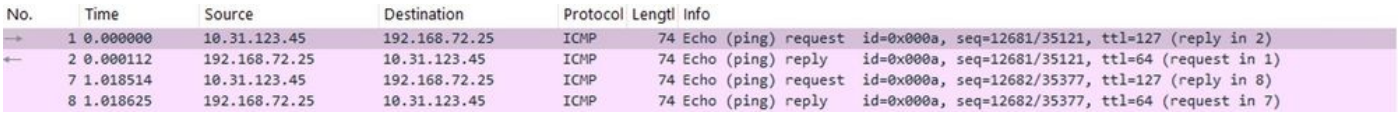
If you use these considerations, and try a ping test, you can see that ping is working as expected:



Packet capture at OS level:

Another way to see if the data plane is working as expected, you can perform a packet capture at OS level, for this troubleshooting article you used the pktcap-uw tool allows to capture traffic that flows through physical network adapters, example:

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



No.	Time	Source	Destination	Protocol	Lengtl	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 capture:
ELAM capture can be useful when you are troubleshooting Native VLAN issues, the tool allows real time view of the packets being forwarded at the ASIC level. It is nondisruptive to the data plane, for troubleshooting purposes, focus only on the MAC and IP Address of the Source and Destination Device.
Example when packets are working:

```
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-insel6)# set outer ipv4 src_ip 192.168.72.25 dst_ip 192.168.72.1
root@module-1(TAH-elam-insel6)# start
root@module-1(TAH-elam-insel6)# 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
.1q 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
```

In the output obtained, it is evident that the src and dst is on VLAN 72. This is expected because you know you are using VLAN 72 as native in all paths and it has arrived on port ethernet 1/10, designated the dpid 72 interface, dpid is the ASIC port internal identifier and the mapping can be found using **show interface hardware-mappings**:

```
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
```

Based on the information obtained in the **show interface hardware-mappings** command, the destination port is port Ethernet 1/1 which is one of the uplinks in the UCS Domain.

Scenario 1. Native VLAN is Configured in the FI Uplinks, Upstream Device not Configured at the vNIC

This time, it is evident that ICMP request stop working which is expected because the native VLAN is removed from the vNICs:

ELAM Capture.

In this case, it cannot be pinged, and if you try to use the IP address of the source and destination, it does not work because there is no connection. In this particular case, set the MAC addresses as filter to obtain more information:

```
root@module-1(TAH-elam-insel6)# set outer l2 src_mac 00:25:B5:01:00:34 dst_mac ff:ff:ff:ff:ff:ff
root@module-1(TAH-elam-insel6)# start
root@module-1(TAH-elam-insel6)# 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
```

You can see the VLAN for the MAC address 00:25:B5:01:00:34 (vNIC-A) is using is VLAN 1, this is incorrect because you need to use VLAN 72.

Scenario 2. Native VLAN is Configured at vNIC, but Upstream Device not Configured in FI Uplinks

ELAM Capture:

```
root@module-1(TAH-elam-insel6)# set outer l2 src_mac 00:25:B5:01:00:34 dst_mac ff:ff:ff:ff:ff:ff
root@module-1(TAH-elam-insel6)# start
root@module-1(TAH-elam-insel6)# 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
.1q 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
```

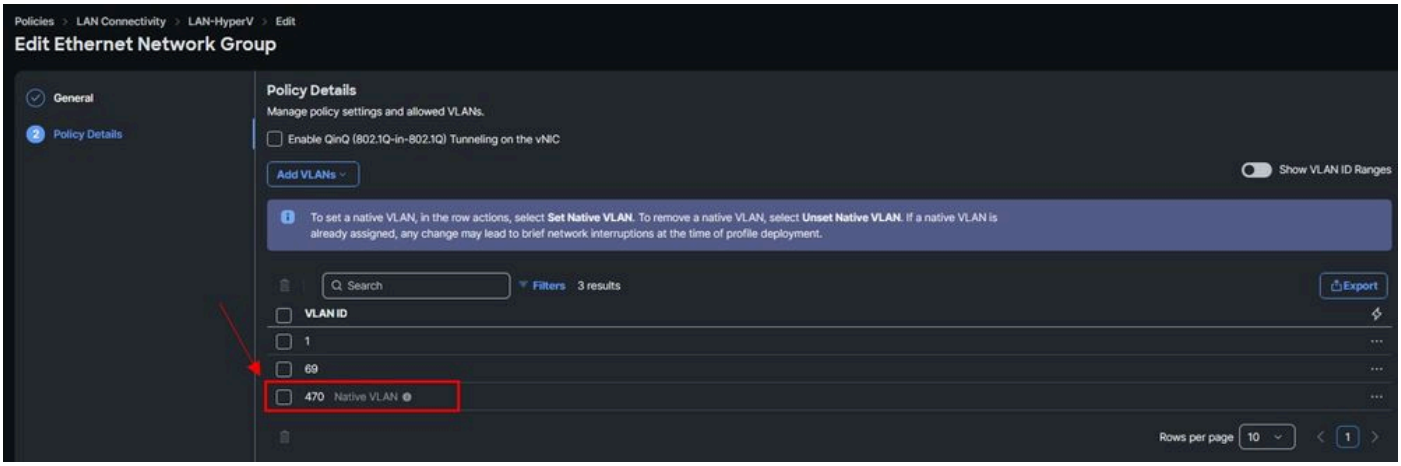
In the output, it is evident that the correct VLAN 72 is being used. However, if you check the configuration in the uplink, you can see native VLAN is not configured:

```
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
```

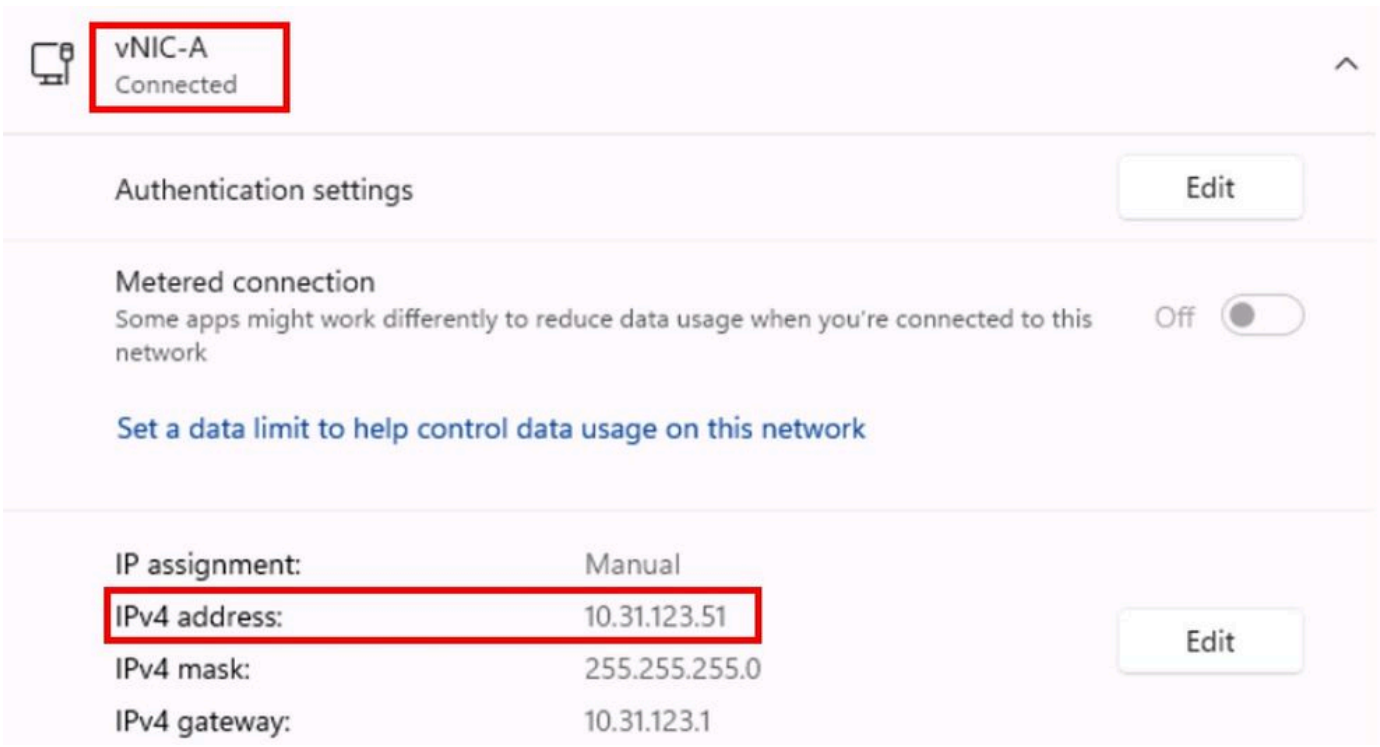
Windows Server OS

Native VLAN issue can also be present in Windows OS, usually the issue can occur because the native VLAN is not tagged on the vNIC.

For this scenario, the Native VLAN 470 was used:



vNIC used is connected in Windows:



Packet Capture

If you try to ping to the network, you can see that the packet capture is working as expected because native VLAN is tagged in the vNIC:

No.	Time	Source	Destination	Protocol	Lengtl	Info
1631	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)

Scenario 1. Native VLAN is configured in FI Uplinks but not Configured at vNIC

- vNIC level:

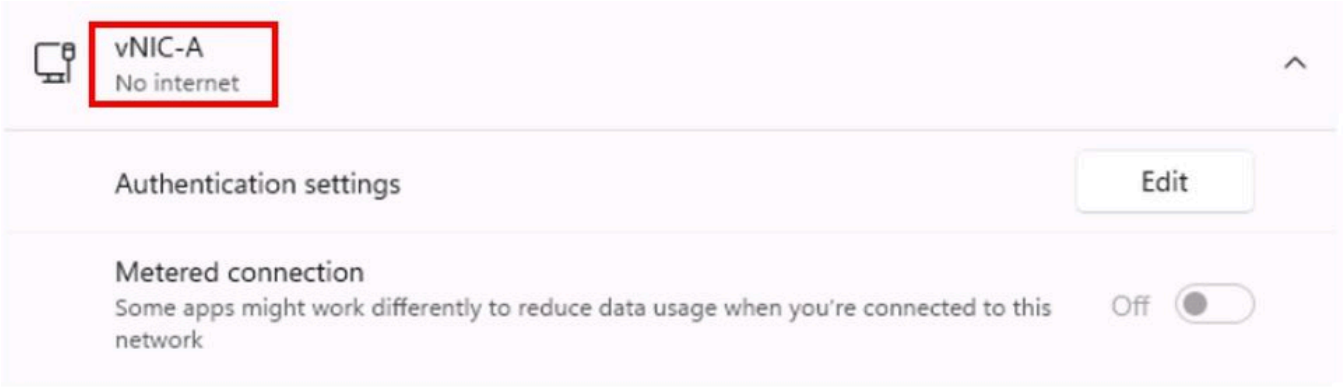
```
6454-A(nx-os)# show running-config interface vethernet 801
interface Vethernet801
  switchport mode trunk
  switchport trunk allowed vlan 1,69,470
```

- FI-A level:

```
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
```

vNIC used is not connected in Windows:



If you try to ping, is expected this can not work.

Scenario 2. Native VLAN is Configured at FI Uplinks and at vNIC

- vNIC level:

```
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 level:

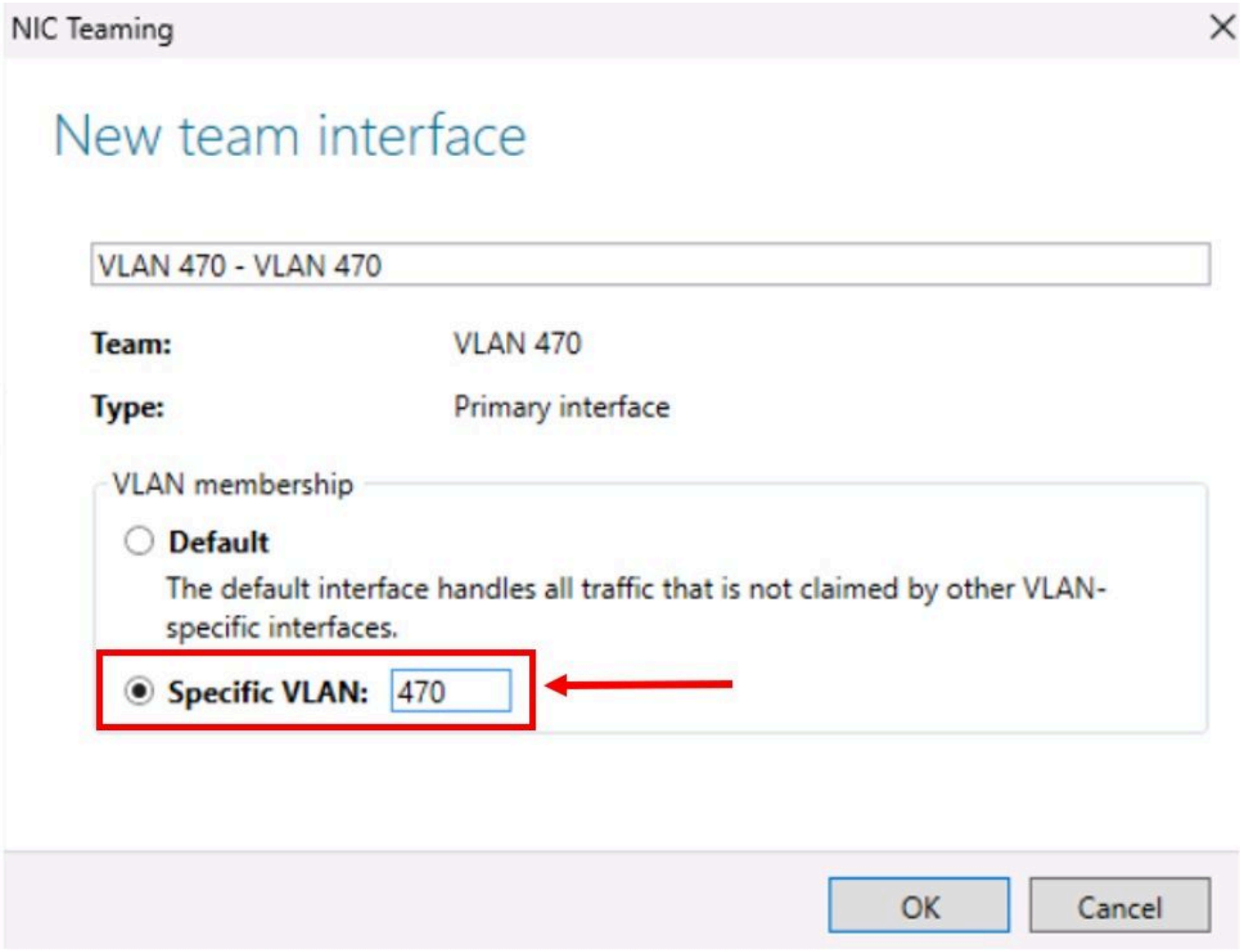
```
IMM-SAAS-MXSVLAB-6454-A(nx-os)# show running-config interface ethernet
interface Ethernet1/15
  description Uplink PC Member
  switchport mode trunk
  switchport trunk native vlan 470 <<<<<<<<<<
  switchport trunk allowed vlan 1,69-70,72,470

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

This configuration does not allow connectivity, it is expected that you do not get a response when doing a

ping test..

Scenario 3. Native VLAN is Configured at OS and vNIC Level

- OS side:



- vNIC level:

```
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
```

- The ping test does not work and you do not have connectivity.

Related Information

- Cisco Intersight Managed Mode Configuration Guide
- Cisco Configure ELAM on UCS

- Packet Capture on ESXi Using the pktcap-uw Tool