

NFVIS 가상 네트워크 이해: OVS, DPDK 및 SR-IOV

목차

[소개](#)

[사용되는 구성 요소](#)

[NFVIS의 네트워킹 개요](#)

[ENCS54XX 플랫폼](#)

[Catalyst 8200 uCPE](#)

[Catalyst 8300 uCPE 1N20](#)

[네트워킹 가상화 기술](#)

[OVS\(Open vSwitch\)](#)

[OVS 브리지](#)

[컨텍스트 스위칭 부족](#)

[DPDK\(데이터 플레인 개발 키트\)](#)

[데이터 복사](#)

[PCIe 패스스루](#)

[단일 루트 I/O 가상화\(SR-IOV\)](#)

[물리적 기능\(PF\)](#)

[VF\(가상 기능\)](#)

[NFVIS 지원 하드웨어에서 SR-IOV 가속화를 위한 권장 드라이버](#)

[DPDK 및 SR-IOV 활용 사례](#)

[DPDK 기본 설정](#)

[SR-IOV 환경 설정](#)

[설정](#)

[DPDK 활성화](#)

[새 네트워크 생성 및 새 OVS 브리지에 연결](#)

[VNF 연결](#)

[관련 문서 및 문서](#)

소개

이 문서에서는 NFVIS 플랫폼이 엔터프라이즈 및 서비스 네트워크의 VNF 통신을 위해 제공하는 가상 네트워킹 체계를 설명합니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 구성 요소를 기반으로 합니다.

- NFVIS 4.7.1-FC4를 실행하는 ENCS5412
- c8300 uCPE 1N20(NFVIS 4.12.1-FC2 실행)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

NFVIS의 네트워킹 개요

내부 관리 네트워크(int-mgmt-net) 및 브리지(int-mgmt-br)는 VNF 모니터링에 내부적으로 사용되며 10.20.0.0/24 서브넷에서 관리 IP 주소를 할당합니다.

ENC54XX 플랫폼

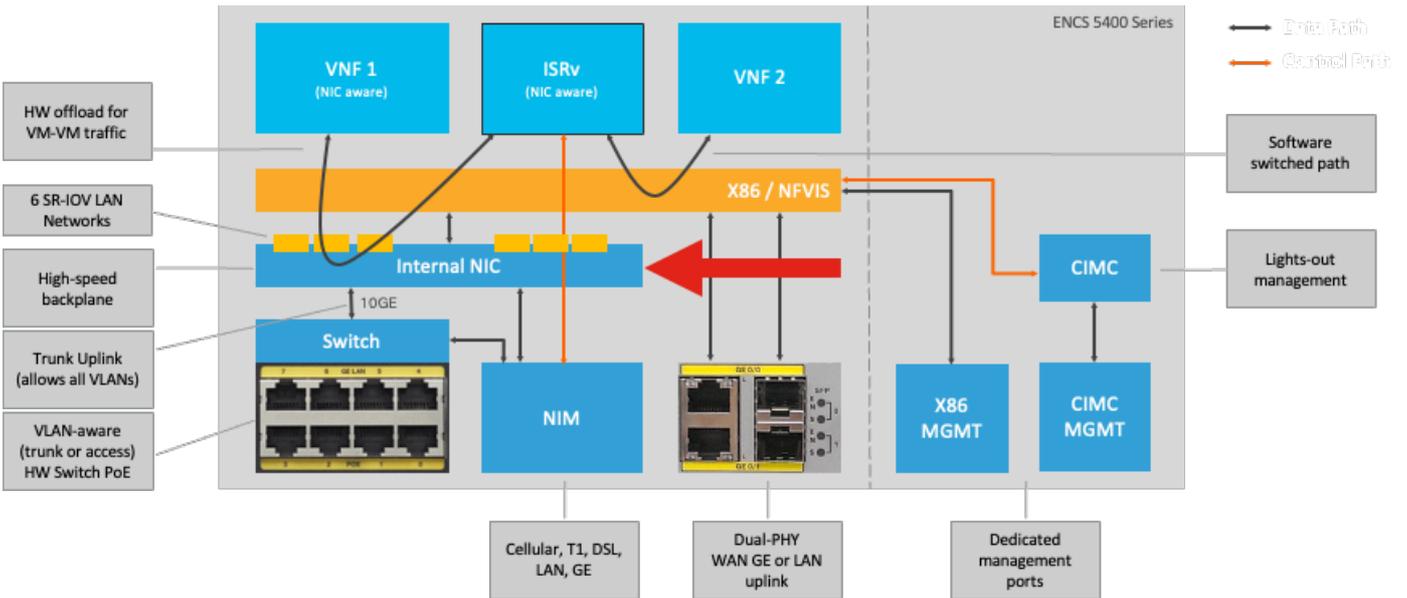


그림 1. 하드웨어 스위치 및 WAN/LAN 업링크 NIC 내부 연결

Catalyst 8200 uCPE

- NFVIS는 관리를 위해 WAN 포트 또는 GE0/2 LAN 포트를 통해 기본적으로 액세스할 수 있습니다.
- WAN 네트워크(wan-net 및 wan2-net) 및 WAN 브리지(wan-br 및 wan2-br)는 기본적으로 DHCP를 활성화하도록 설정됩니다. GE0-0은 기본적으로 WAN 브리지와 GE0-1 및 WAN2 브리지에 연결됩니다.
- Catalyst 8200 UCPE의 관리 IP 주소 192.168.1.1은 GE0-2를 통해 액세스할 수 있습니다.
- GE0-2는 LAN 브리지에 연결됩니다.
- 내부 관리 네트워크(int-mgmt-net) 및 브리지(int-mgmt-br)가 생성되어 시스템 모니터링에 내부적으로 사용됩니다.

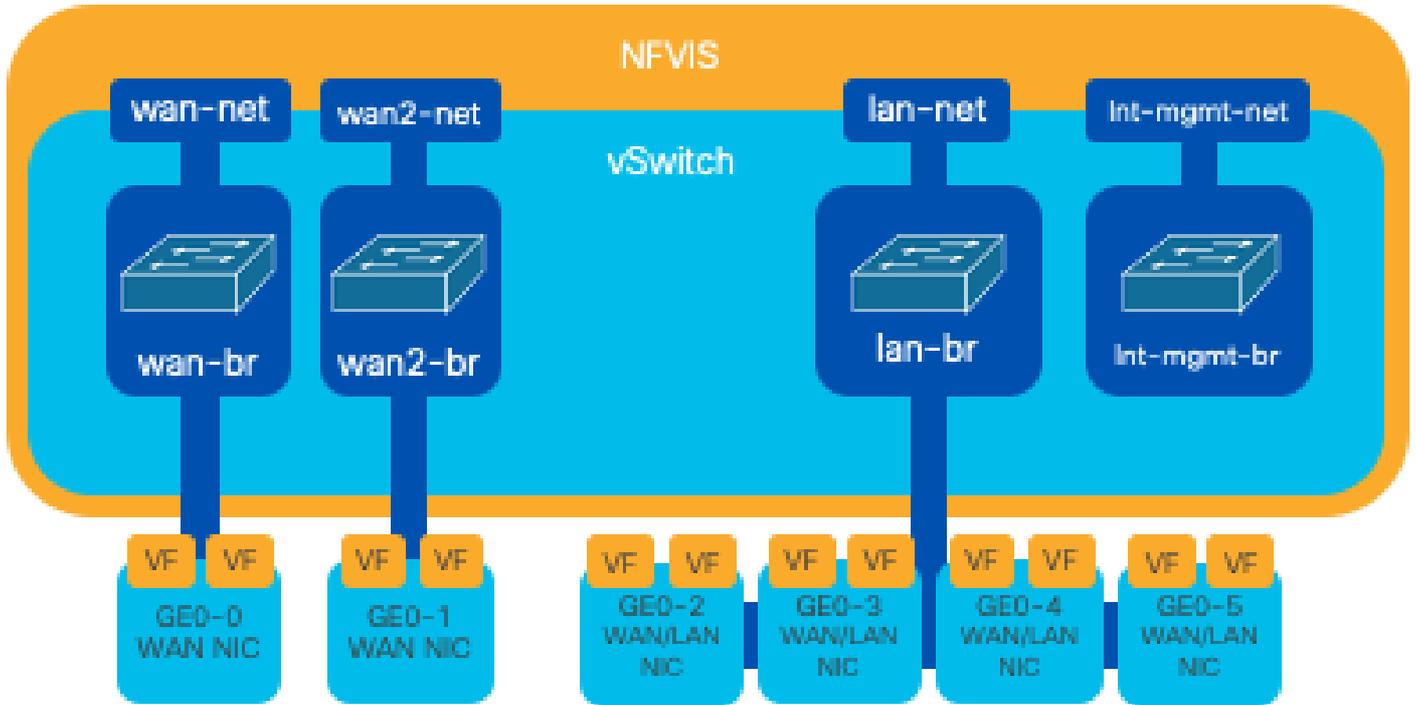


그림 2. 8200 NIC에 할당된 내부 브리징 및 가상 스위치

Catalyst 8300 uCPE 1N20

1. NFVIS는 기본적으로 FPGE(Front Panel Gigabit Ethernet)WAN 포트를 통해 액세스하거나 GE0-2 LAN 포트를 통해 액세스하여 관리할 수 있습니다
2. WAN 네트워크(wan-net) 및 WAN 브리지(wan-br)는 DHCP를 활성화하도록 기본적으로 설정됩니다. GE0-0은 기본적으로 WAN 브리지와 연결됩니다
3. WAN 네트워크(wan2-net) 및 WAN 브리지(wan2-br)는 기본적으로 생성되지만 어떤 물리적 포트와도 연결되지 않습니다
4. GE0-2는 LAN 브리지에 연결되어 있고 다른 모든 포트는 OVS에 연결되어 있지 않습니다
5. C8300-uCPE의 관리 IP 192.168.1.1은 GE0-2를 통해 액세스할 수 있습니다.
6. 내부 관리 네트워크(int-mgmt-net) 및 브리지(int-mgmt-br)가 생성되어 시스템 모니터링에 내부적으로 사용됩니다.

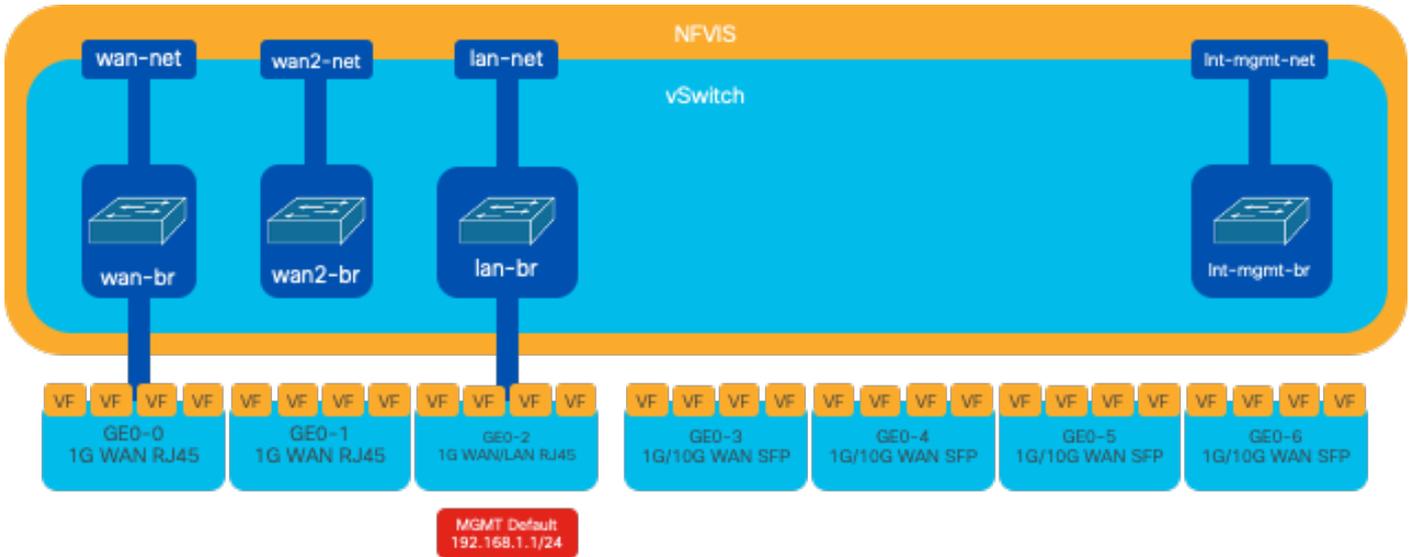


그림 3. 8300 NIC에 할당된 내부 브리징 및 가상 스위치

네트워킹 가상화 기술

OVS(Open vSwitch)

OVS(Open vSwitch)는 프로그래밍 방식의 확장을 통해 네트워크 자동화를 구현하고 NetFlow, sFlow, IPFIX, RSPAN, CLI, LACP, 802.1ag와 같은 표준 관리 인터페이스 및 프로토콜을 지원하도록 설계된 오픈 소스 멀티레이어 가상 스위치입니다. 특히 하이퍼바이저를 통해 VM(가상 머신) 간 네트워크 트래픽을 관리할 수 있는 대규모 가상 환경에서 널리 사용됩니다. NFVIS 인터페이스를 통해 직접 관리되는 정교한 네트워크 토폴로지 및 정책을 생성할 수 있어 네트워크 기능 가상화를 위한 다목적 환경을 제공합니다.

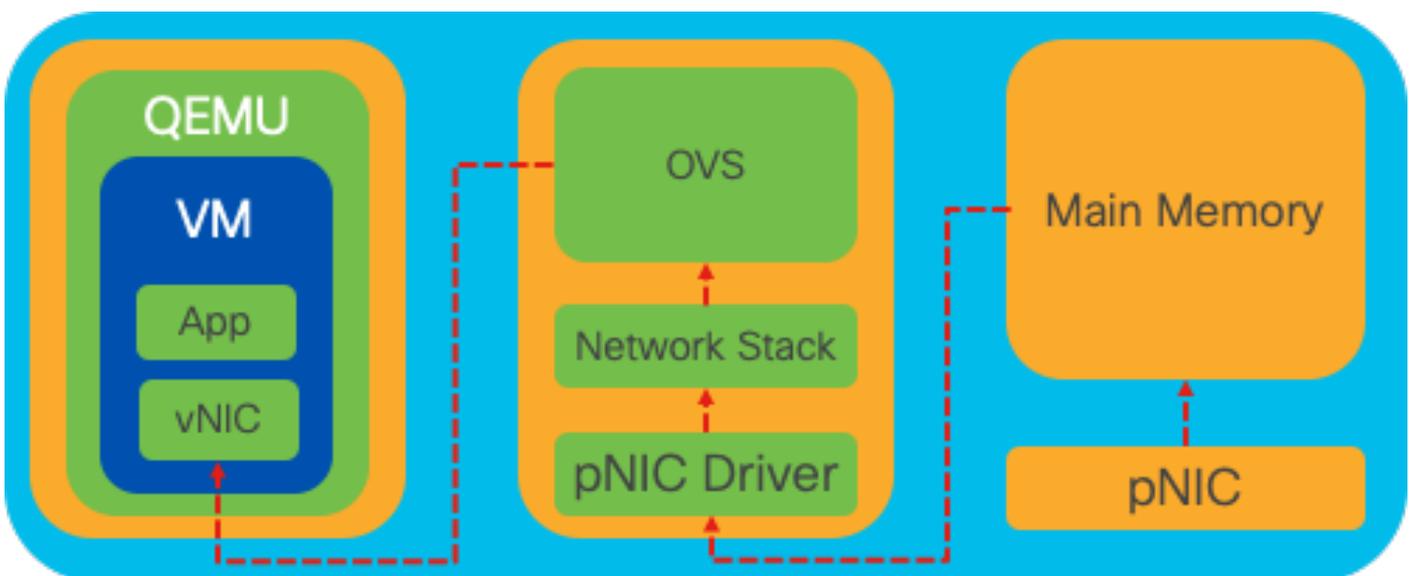


그림 4. Linux 커널 내 OVS 컨피그레이션

OVS 브리지

가상 네트워크 브리지 및 플로우 규칙을 사용하여 호스트 간에 패킷을 전달합니다. 이는 물리적 스

위치처럼 작동하며 가상화만 가능합니다.

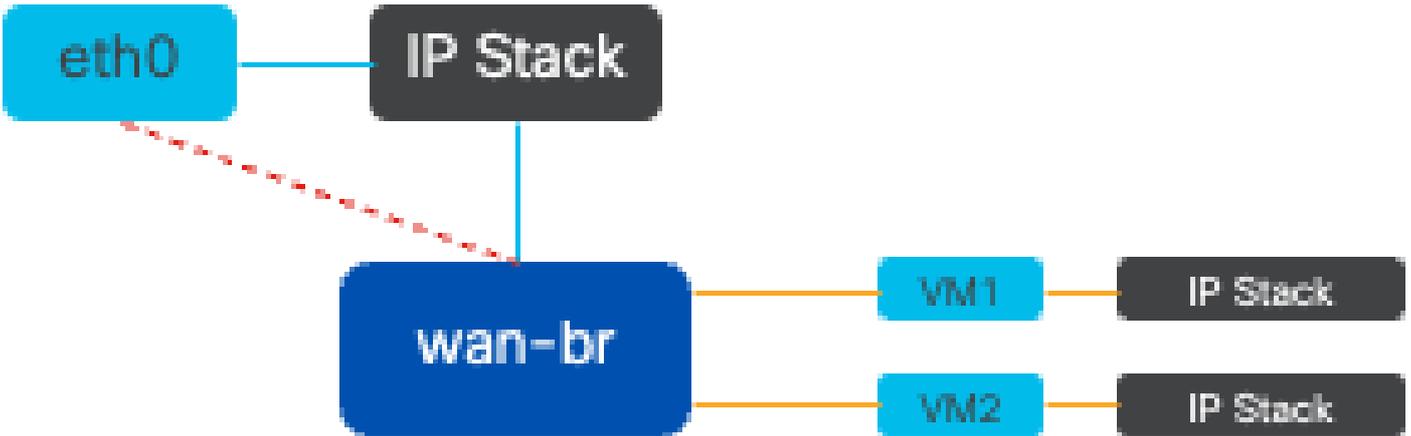


그림 5. wan-br 브리지에 연결된 2개의 VM 또는 VNF의 구현 예

컨텍스트 스위칭 부족

네트워크 패킷이 NIC(Network Interface Card)에 도착하면 인터럽트를 트리거하고 즉시 주의가 필요하다는 신호를 프로세서에 보냅니다. CPU는 인터럽트 처리라고 하는 프로세스인 인터럽트를 처리하기 위해 현재 작업을 일시 중지합니다. 이 단계에서 CPU는 운영 체제 커널의 제어 하에 NIC에서 메모리로 패킷을 읽고 패킷 대상 및 목적에 따라 다음 단계를 결정합니다. 목표는 패킷을 신속하게 처리하거나 의도된 애플리케이션으로 라우팅하여 레이턴시를 최소화하고 처리량을 최대화하는 것입니다.

컨텍스트 전환은 CPU가 한 환경(컨텍스트)에서 다른 환경으로 작업을 실행하던 것을 전환하는 프로세스입니다. 이는 사용자 모드와 커널 모드 간에 이동할 때 특히 관련이 있습니다.

- 사용자 모드: 대부분의 애플리케이션이 실행되는 제한된 처리 모드입니다. 사용자 모드의 애플리케이션은 하드웨어 또는 참조 메모리에 직접 액세스할 수 없으며 이러한 작업을 수행하려면 운영 체제 커널과 통신해야 합니다.
- 커널 모드: 이 모드는 운영 체제에 하드웨어 및 모든 메모리에 대한 전체 액세스 권한을 부여합니다. 커널은 임의의 CPU 명령을 실행하고 임의의 메모리 주소를 참조할 수 있다. 커널 모드는 하드웨어 디바이스, 메모리 관리 및 시스템 호출 실행과 같은 작업을 수행하는 데 필요합니다.

애플리케이션이 커널 레벨 권한이 필요한 작업(예: 네트워크 패킷 읽기)을 수행해야 하는 경우, 컨텍스트 스위치가 발생합니다. CPU는 사용자 모드에서 커널 모드로 전환하여 작업을 실행합니다. 완료되면 다른 컨텍스트 스위치에서 CPU를 사용자 모드로 반환하여 애플리케이션 실행을 계속합니다. 이러한 스위칭 프로세스는 시스템 안정성과 보안을 유지하는 데 중요하지만 성능에 영향을 줄 수 있는 오버헤드를 초래합니다.

OVS는 주로 운영 체제 사용자 공간에서 실행되며, 데이터 처리량이 증가하면 병목 현상이 발생할 수 있습니다. CPU가 패킷을 처리하기 위해 커널 모드로 전환하려면 더 많은 컨텍스트 스위치가 필요하기 때문에 성능이 느려지기 때문입니다. 이러한 제한은 패킷 속도가 높거나 정확한 타이밍이 중요한 환경에서 특히 두드러집니다. 이러한 성능 제한을 해결하고 최신 고속 네트워크의 요구 사항을 충족하기 위해 DPDK(Data Plane Development Kit) 및 SR-IOV(Single Root I/O

Virtualization)와 같은 기술이 개발되었습니다.

DPDK(데이터 플레인 개발 키트)

DPDK는 광범위한 CPU 아키텍처에서 패킷 처리 워크로드를 가속화하기 위해 설계된 라이브러리 및 드라이버 집합입니다. DPDK는 기존의 커널 네트워킹 스택을 우회함으로써(컨텍스트 스위칭을 피함) 데이터 플레인 처리량을 크게 높이고 레이턴시를 줄일 수 있습니다. 이는 특히 저지연 통신이 필요한 고처리량 VNF에 유리하므로 NFVIS는 성능에 민감한 네트워크 기능을 위한 이상적인 플랫폼입니다.

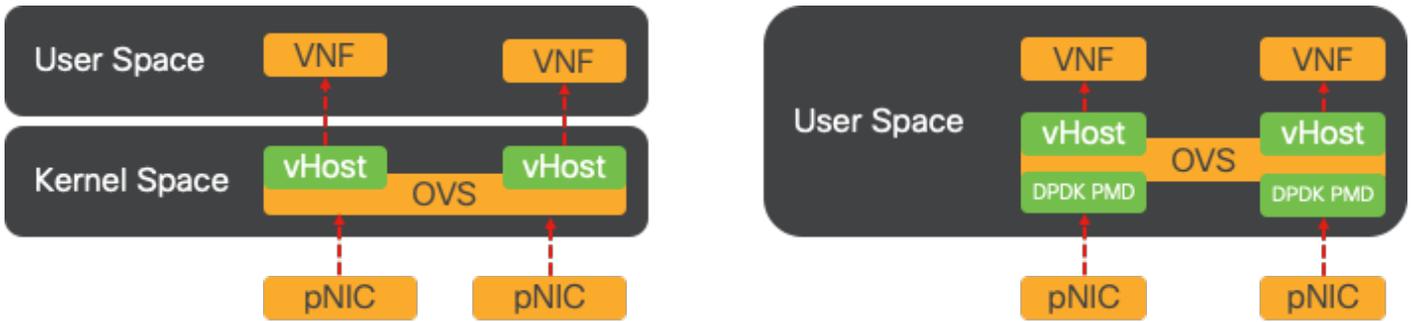


그림 6. 기존 OVS(왼쪽) 및 DPDK OVS(오른쪽) 컨텍스트 스위칭 최적화

OVS에 대한 DPDK 지원은 ENCS의 경우 NFVIS 3.10.1에서, 다른 플랫폼의 경우 3.12.2에서 시작되었습니다.

- 비 DPDK OVS보다 우수한 SRIOV 부근의 서비스 체인 처리량
- VNF에 대한 가상 드라이버가 필요합니다.
- 지원되는 플랫폼:
 - 3.10.1 이상 종료
 - UCSE, UCS-C, CSP5K 3.12.1 이상
 - 4.12.1 이후 포트 채널용 DPDK 지원
- 패킷/트래픽 캡처: DPDK에서는 지원되지 않습니다.
- PNIC의 스펜 트래픽: DPDK에서는 지원되지 않습니다.
- OVS-DPDK가 활성화된 후에는 개별 기능으로 비활성화할 수 없습니다. DPDK를 비활성화하는 유일한 방법은 공장 재설정입니다.

데이터 복사

기존의 네트워킹 방식에서는 VM 메모리의 대상에 도달하기 전에 데이터를 여러 번 복사해야 하는 경우가 많습니다. 예를 들어, 패킷은 NIC에서 커널 공간으로 복사한 다음 가상 스위치(예: OVS)에서 처리할 사용자 공간으로 복사하고 마지막으로 VM 메모리로 복사해야 합니다. 각 복사 작업은 커널 네트워킹 스택을 우회하여 DPDK가 제공하는 성능 향상에도 불구하고 지연을 발생시키고 CPU 사용률을 높입니다.

이러한 오버헤드에는 VM에 전달되기 전에 사용자 공간에서 패킷을 처리하는 데 필요한 메모리 복사본 및 처리 시간이 포함됩니다. PCIe Passthrough 및 SR-IOV는 기존 가상화 방식과 동일한 정도로 호스트 운영 체제를 사용하지 않고 물리적 네트워크 디바이스(예: NIC)를 여러 VM 간에 직접 공유할 수 있도록 함으로써 이러한 병목 현상을 해결합니다.

PCIe 패스스루

이 전략에는 하이퍼바이저를 우회하여 VNF(Virtual Network Functions)가 NIC(Network Interface Card)에 직접 액세스할 수 있도록 하여 거의 최대 처리량을 달성하는 것이 포함됩니다. 이 접근 방식을 PCI 패스스루라고 하며, 하이퍼바이저의 개입 없이 게스트 운영 체제 전용으로 전체 NIC를 사용할 수 있습니다. 이 설정에서는 가상 머신이 NIC에 직접 연결된 것처럼 작동합니다. 예를 들어, 2개의 NIC 카드를 사용할 수 있는 경우 각 카드를 서로 다른 VNF에 독점적으로 할당하여 직접 액세스할 수 있습니다.

그러나 이 방법은 두 개의 NIC만 사용할 수 있고 두 개의 개별 VNF에서 독점적으로 사용할 수 있는 경우, 사용 가능한 전용 NIC가 없기 때문에 세 번째 VNF와 같은 추가 VNF는 NIC 액세스 없이 그대로 남아 있다는 단점이 있습니다. 대체 솔루션으로는 SR-IOV(Single Root I/O Virtualization)를 사용하는 것이 있습니다.

단일 루트 I/O 가상화(SR-IOV)

NIC(Network Interface Card)와 같은 단일 물리적 PCI 장치가 여러 개의 개별 가상 장치로 나타날 수 있도록 하는 사양입니다. 이 기술은 물리적 네트워크 디바이스에 대한 VM 직접 액세스를 제공하여 오버헤드를 줄이고 I/O 성능을 향상합니다. 단일 PCIe 디바이스를 여러 가상 슬라이스로 분할하여 각기 다른 VM 또는 VNF에 할당함으로써 한정된 수의 NIC로 인한 제한을 효과적으로 해결합니다. VF(Virtual Functions)라고 알려진 이러한 가상 슬라이스는 여러 VNF 간에 공유 NIC 리소스를 허용합니다. PF(Physical Function)는 SR-IOV 기능을 지원하는 실제 물리적 구성 요소를 의미합니다.

NFVIS는 SR-IOV를 활용하여 특정 VNF에 전용 NIC 리소스를 할당함으로써 네트워크 패킷의 DMA(Direct Memory Access)를 각 VM 메모리에 직접 구현하여 높은 성능과 낮은 레이턴시를 보장합니다. 이 접근 방식은 CPU 개입을 최소화하여 패킷을 처리하기만 하면 CPU 사용량이 줄어듭니다. 이는 특히 보장된 대역폭이 필요하거나 성능 요구 사항이 엄격한 애플리케이션에 유용합니다.

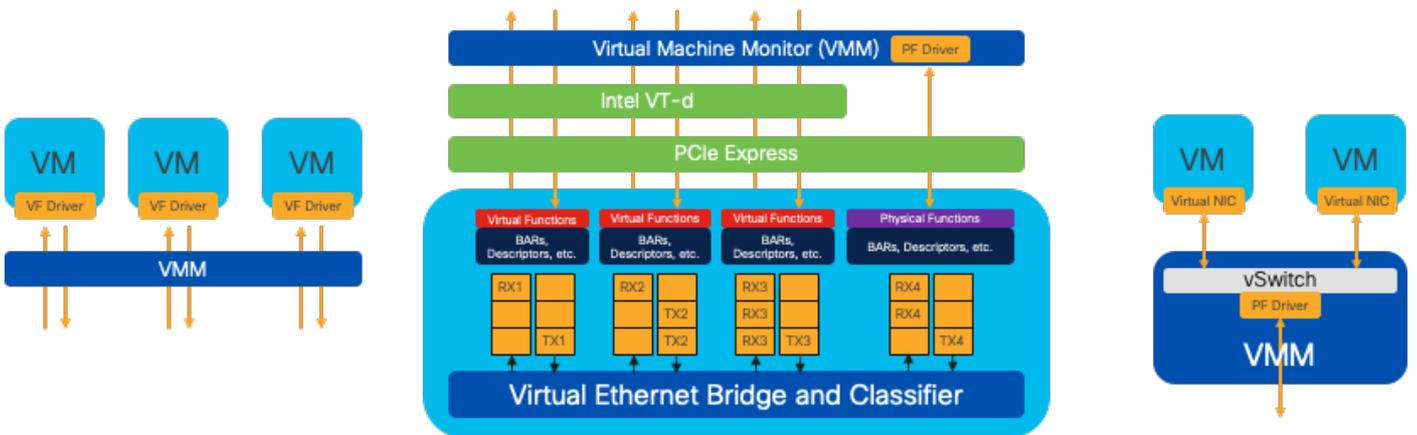


그림 7. 하드웨어 기능을 통한 NFVIS SR-IOV PCIe 리소스 분리

물리적 기능(PF)

모든 기능을 갖춘 PCIe 기능이며 특정 네트워킹 기능을 제공하는 전용 하드웨어 박스를 의미합니다. 이러한 기능은 다른 PCIe 장치처럼 검색, 관리 및 조작할 수 있는 모든 기능을 갖춘 PCIe 기능입니다.

다. 물리적 기능에는 PCIe 장치를 구성하고 제어하는 데 사용할 수 있는 SR-IOV 기능이 포함됩니다

VF(가상 기능)

간소화된 기능은 구성 리소스를 최소화하고(경량화) 단순한 PCIe 기능으로서 I/O 처리에만 중점을 둡니다. 모든 가상 함수는 물리적 함수에서 비롯됩니다. 디바이스 하드웨어는 가능한 가상 기능 수를 제한합니다. 하나의 이더넷 포트, 즉 물리적 장치는 여러 가상 기능에 대응할 수 있으며, 이 가상 기능은 서로 다른 가상 시스템에 할당될 수 있습니다.

NFVIS 지원 하드웨어에서 SR-IOV 가속화를 위한 권장 드라이버

플랫폼	NIC	NIC 드라이버
ENCS 54XX	백플레인 스위치	i40e
ENCS 54XX	GE0-0 및 GE0-1	IGB
Catalyst 8200 uCPE	GE0-0 및 GE0-1	ixgbe
Catalyst 8200 uCPE	GE0-2 및 GE0-5	IGB

DPDK 및 SR-IOV 활용 사례

DPDK 기본 설정

특히 네트워크 트래픽이 주로 east-west로 이동하는 경우(즉, 동일한 서버 내에 머무르는 경우) DPDK는 SR-IOV보다 성능이 뛰어납니다. 그 이유는 간단합니다. NIC에 액세스할 필요 없이 서버 내에서 트래픽을 내부적으로 관리할 경우 SR-IOV는 아무런 이점도 제공하지 않습니다. 실제로 SR-IOV는 트래픽 경로를 불필요하게 확장하고 NIC 리소스를 소비함으로써 잠재적으로 비효율성을 초래할 수 있습니다. 따라서 내부 서버 트래픽 관리에서는 DPDK를 활용하는 것이 더 효율적입니다.

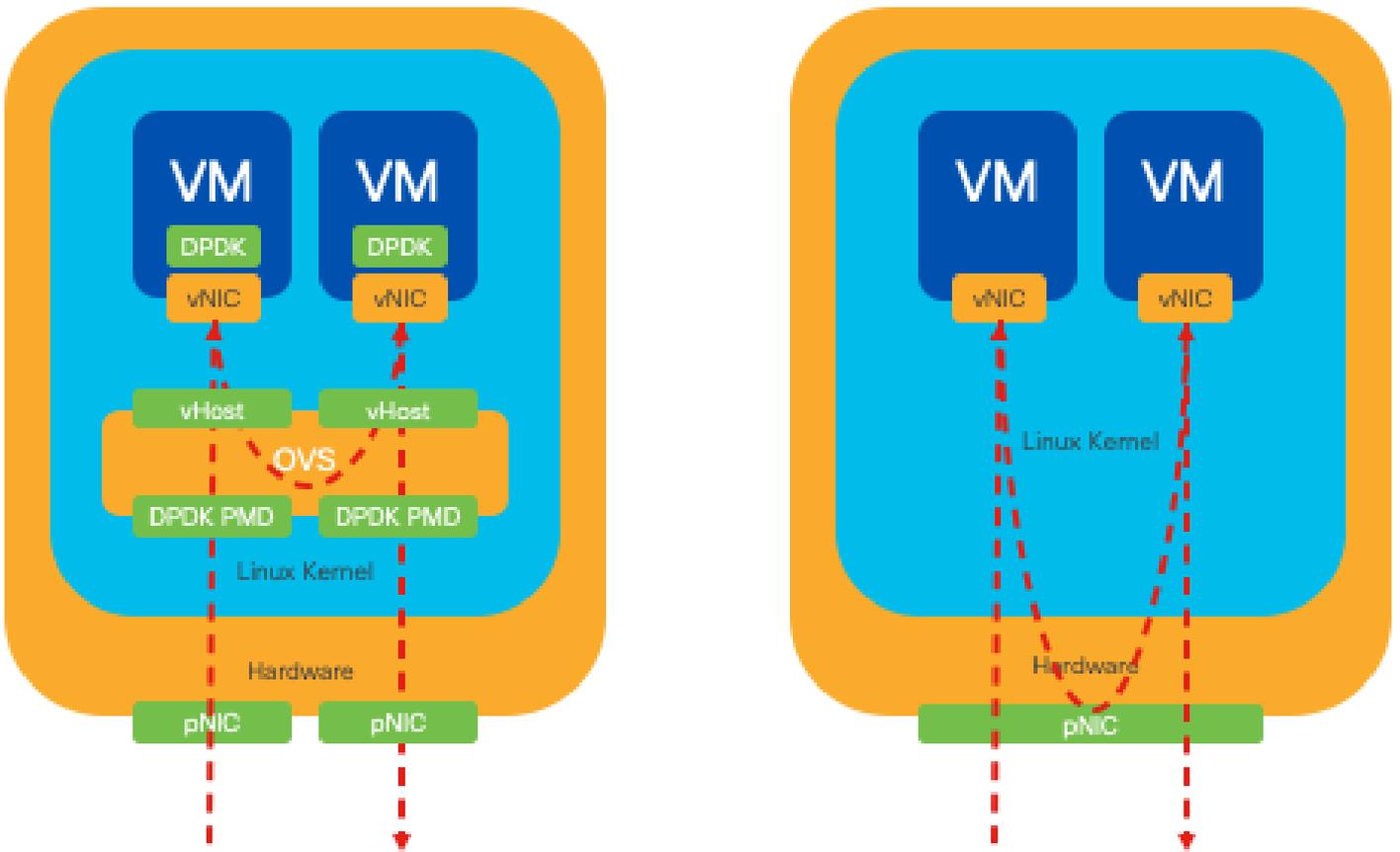


그림 8. East-to-West 트래픽의 DPDK 및 SR-IOV 패킷 이동

SR-IOV 환경 설정

네트워크 트래픽이 북에서 남으로, 또는 동에서 서로 이동하는 경우 특히 서버 간에 SR-IOV를 사용하는 것이 DPDK보다 유리합니다. 특히 서버 간 통신에서는 더욱 그렇습니다. 이러한 트래픽은 불가피하게 NIC를 통과해야 하므로 DPDK가 향상된 OVS를 선택하면 추가적인 복잡성과 잠재적인 성능 제약이 불필요하게 발생할 수 있습니다. 따라서 SR-IOV는 이러한 상황에서 바람직한 선택으로 나타나며, 서버 간 트래픽을 처리하기 위한 간단하고 효율적인 경로를 제공합니다.

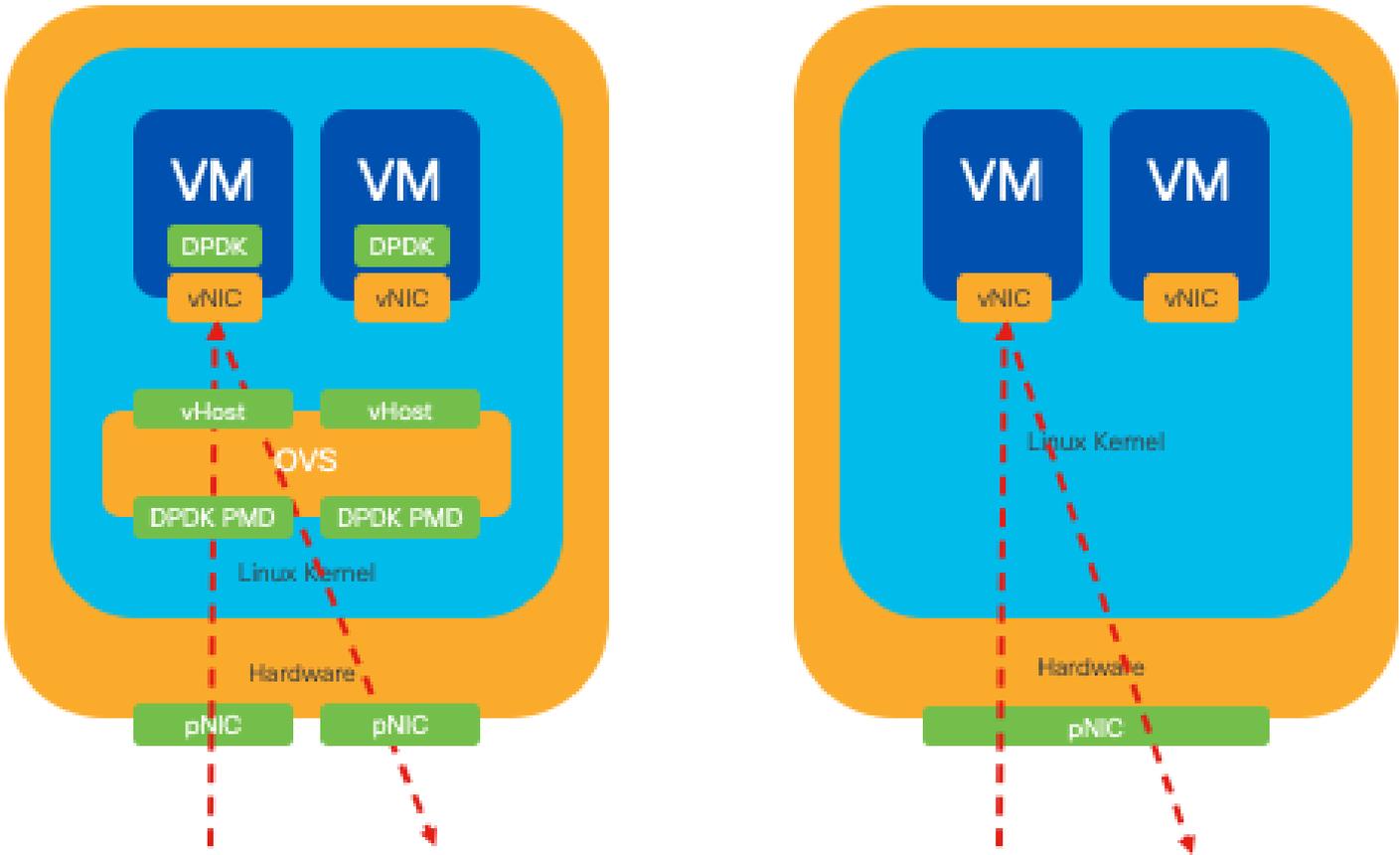
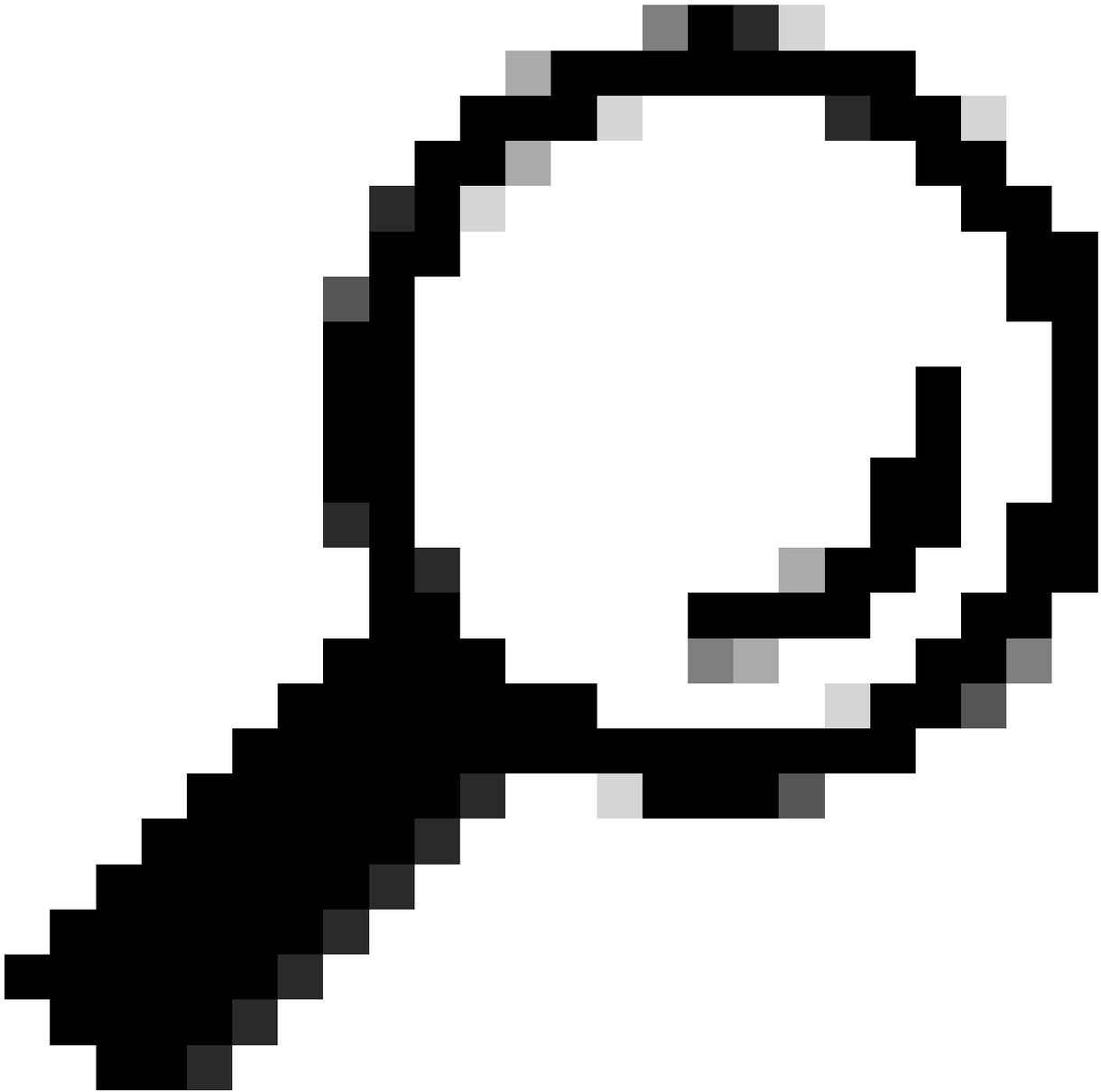


그림 9. North-to-South 트래픽의 DPDK 및 SR-IOV 패킷 이동



팁: 앞서 설명한 대로 DPDK가 OVS와 함께 사용되는 시나리오를 제외하고 VNF(Virtual Network Function) 내에서 SR-IOV와 DPDK를 통합하여 SR-IOV 기반 설정의 성능을 향상시킬 수 있다는 점을 기억하십시오.

설정

DPDK 활성화

GUI에서 DPDK를 활성화하려면 Configuration(컨피그레이션) > Virtual Machine(가상 머신) > Networking(네트워킹) > Networks(네트워크)로 이동해야 합니다. 메뉴를 클릭한 다음 스위치를 클릭하여 기능을 활성화합니다

Networks

Networks Information and Configuration

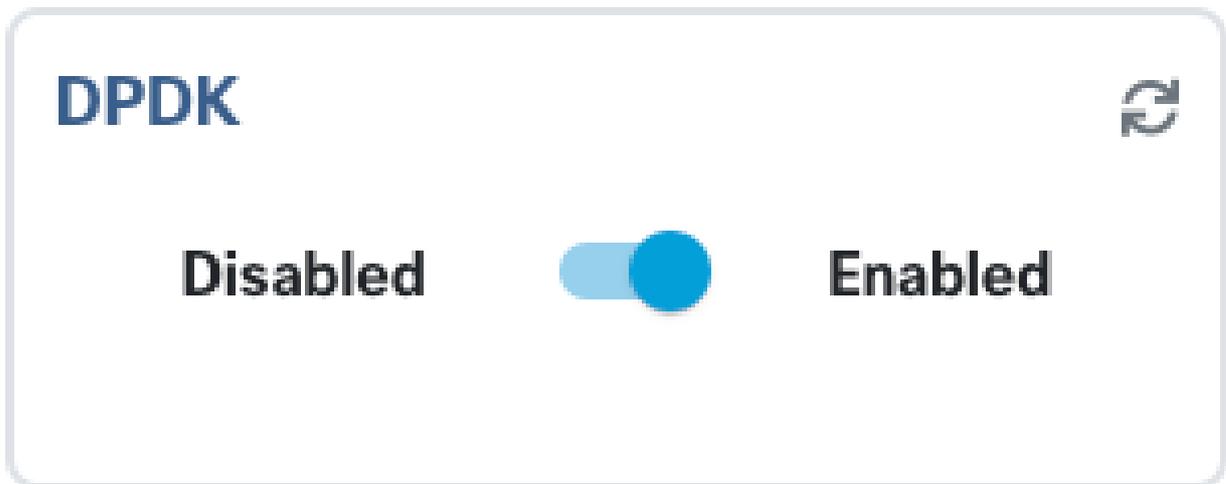
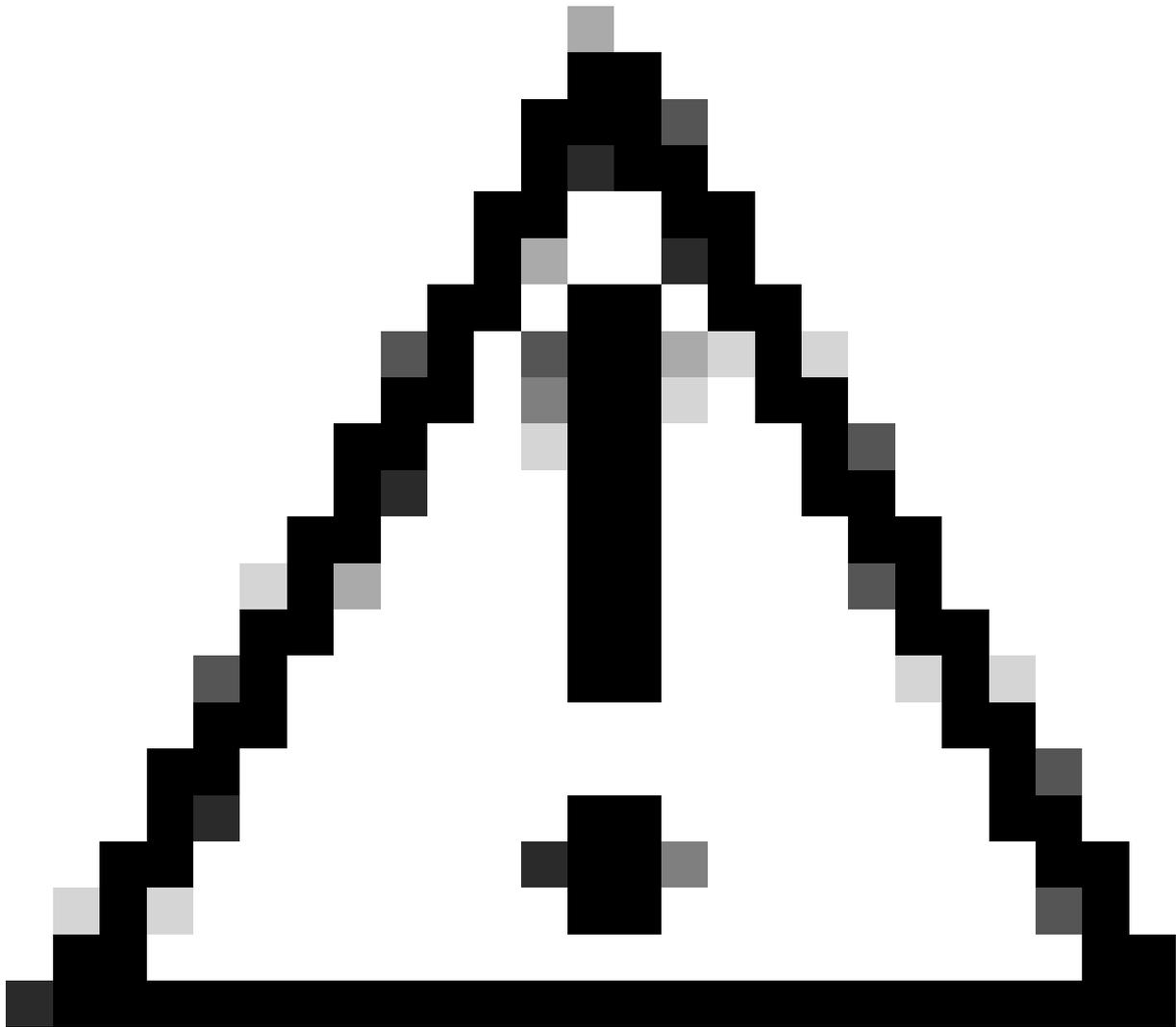


그림 10. DPDK 활성화를 위해 GUI에서 사용할 수 있는 슬라이드 버튼
CLI의 경우 컨피그레이션 모드의 전역 시스템 설정에서 활성화해야 합니다.

```
nfvis(config)# system settings dpdk enable
```



주의: NFVIS에서 공장 재설정을 수행하지 않으면 DPDK를 비활성화할 수 없습니다.

새 네트워크 생성 및 새 OVS 브리지에 연결

Configuration(컨피그레이션) > Virtual Machine(가상 머신) > Networking(네트워킹) > Networks(네트워크)로 이동합니다. Networks 페이지에서 Networks 테이블의 왼쪽 위에 더하기 기호(+)를 클릭합니다.



Networks								Total Record: 3	search in all record	
#	Network	Mode	Vlan	Vlan-Range	Native Vlan	Bridge	Interface	Action		
1	wan-net	trunk				wan-br	GE0-0			
2	wan2-net	trunk				wan2-br	GE0-1			
3	lan-net	trunk				lan-br	GE0-2			

그림 11. NFVIS GUI의 네트워크 테이블 보기

네트워크의 이름을 지정하고 새 브리지에 연결합니다. VLAN 및 인터페이스 바인딩 옵션은 네트워크 인프라 요구 사항에 따라 달라질 수 있습니다.

Add Network

Network *

inter-vnf-net

Mode *

trunk

Vlan

Vlan-Range

Native Vlan

1

Bridge *

Existing Create New

Bridge

inter-vnf-br

Interface

Submit

Cancel

Reset

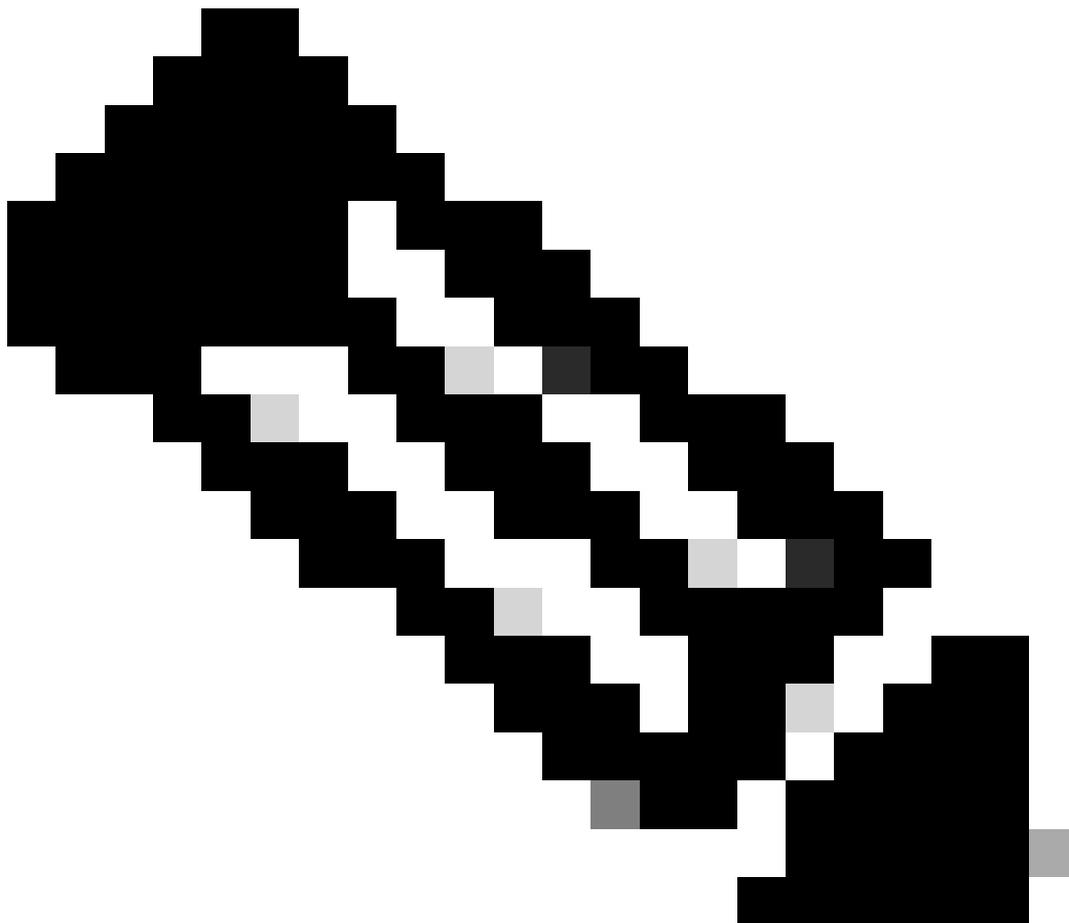
그림 12. NFVIS GUI에서 가상 네트워크를 생성하기 위한 "Add Network" 모달

제출 버튼을 클릭한 후에는 Networks(네트워크) 테이블에 추가된 새로 생성된 네트워크를 검토할 수 있어야 합니다.



#	Network	Mode	Vlan	Vlan-Range	Native Vlan	Bridge	Interface	Action
1	wan-net	trunk				wan-br	GE0-0	 
2	wan2-net	trunk				wan2-br	GE0-1	 
3	lan-net	trunk				lan-br	GE0-2	 
4	inter-vnf-net	trunk			1	inter-vnf-br		 

그림 13. 오른쪽 상단 모서리에 "Refresh Icon(새로 고침 아이콘)"이 있는 NFVIS GUI의 네트워크 테이블 보기(빨간색으로 강조 표시됨)



참고: 새 네트워크가 테이블에 표시되지 않으면 오른쪽 상단 새로 고침 버튼을 클릭하거나 전체 페이지를 새로 고치십시오.

CLI에서 수행하는 경우 모든 네트워크 및 브리지가 컨피그레이션 모드에서 생성되며 워크플로는 GUI 버전과 동일합니다.

1. 새 브리지를 생성합니다.

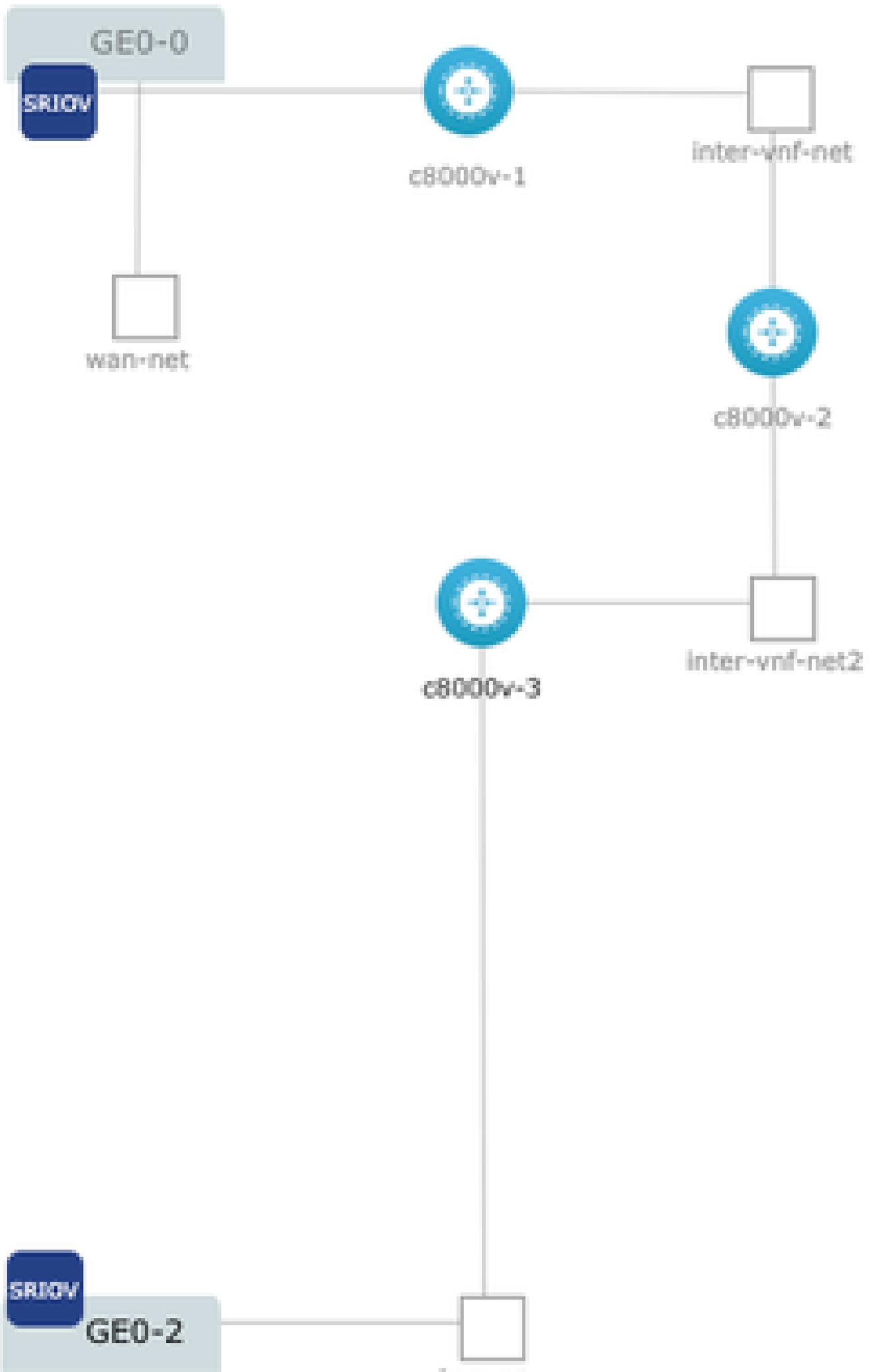
```
nfvis(config)# bridges bridge inter-vnf-br2
nfvis(config-bridge-inter-vnf-br2)# commit
```

2. 새 네트워크를 생성하고 이전에 생성한 브리지와 연결합니다

```
nfvis(config)# networks network inter-vnf-net2 bridge inter-vnf-br2 trunk true native-vlan 1
nfvis(config-network-inter-vnf-net2)# commit
```

VNF 연결

네트워크 토폴로지 또는 단일 VFN 구축으로 시작하려면 Configuration(컨피그레이션) > Deploy(구축)로 이동해야 합니다. VM 또는 컨테이너를 선택 목록에서 토폴로지 작성 영역으로 끌어서 가상 인프라 생성을 시작할 수 있습니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.