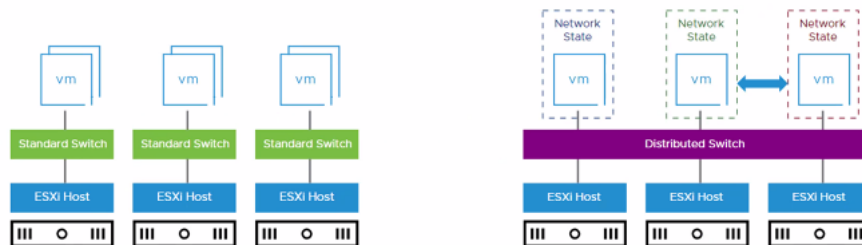


VM웨어 10일 (기술스택)

분산스위치란?

What Is a vSphere Distributed Switch?

vSphere Distributed Switch is a virtual switch that provides virtual networking for all ESXi hosts in a data center.



Whereas a standard switch is owned and managed by a single ESXi host, a distributed switch is owned and managed by vCenter Server.

- 3개의 스위치가 하나 처럼?
- 표준스위치는 vSwitch01 이런식이고 분산스위치는 표준 스위치를 분산스위치에 연결 그래서 하이퍼바이저는 분산스위치로 인식
- vCenter Server는 클러스터를 다루기 위해서 꼭 사용해야함. 분산스위치 핸들링할 때 도 필요
- 하나의 스위치만 관리하면 모든 호스트의 네트워크와 관련된 정책을 컨트롤할 수 있음
 - 관리포인트가 1개라서 유지보수에 편리함
 - 이 ESXi는 vCenter로 관리가능 ESXi 분산 스위치를 하나로 인식

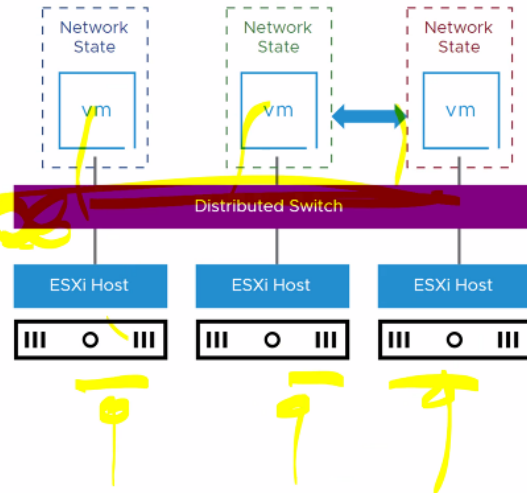
Benefits of Distributed Switches

A distributed switch provides the following benefits:

- **Consistent network configuration**
 - Virtual machines maintain a consistent network configuration as they migrate between hosts in the data center.
- **Central point of control**
 - Administrators have a central point of control for creating, administering, and monitoring the virtual networks.

vmware

© 2023 VMware, Inc.



- 하이퍼 바이저 위에는 vCenter가 관리하게 된다.
- DCNM, NDFC 관련 매니저 툴 사용 네트워크는 NSX Manager 사용
- vCenter에서 관리하는 가상스위치 분산스위치

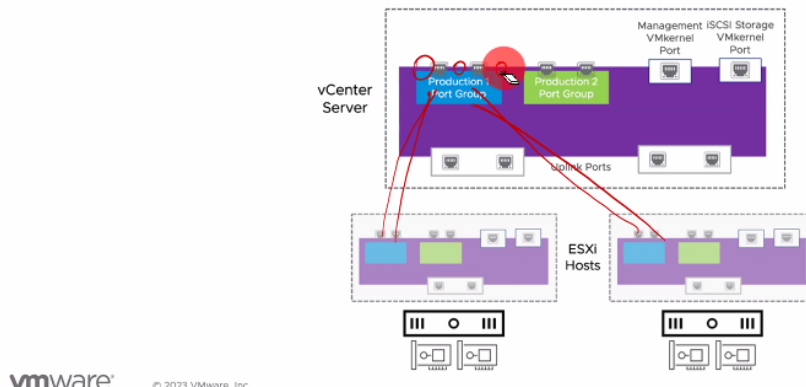
VM자료 찾는법

- GPT는 버전에 따라 다르게 답변하기 때문에 버전명시해서 영어로 구글링
 - vsphere 8.0 standard switch distributed switch
 - vsphere configure guide
 - esxi 8.0 configure guide

Distributed Switch Architecture

The distributed switch configuration is managed by vCenter Server:

- The port group and VMkernel port configuration is automatically pushed down to all connected ESXi hosts.
- Each ESXi host is responsible for managing their own uplink adapters and for forwarding packets from VMs to their destinations.

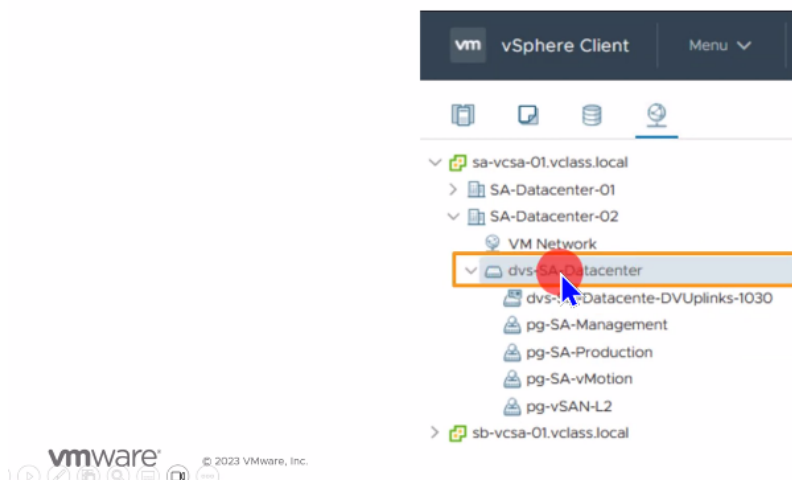


- 분산스위치 아키텍처
- vCenter 서버에서 포트그룹이 있는데 거기서 호스트의 1의 lan 포트 2개, 호스트2 lan 2개 각각 분산스위치로 연결

Viewing a Distributed Switch Configuration

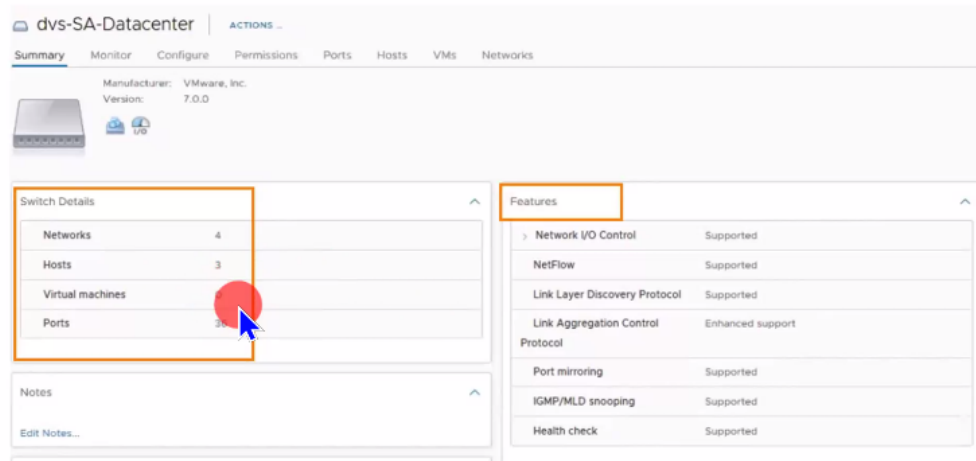
You can view details about the configuration of a distributed switch in the vSphere Client.

You select the distributed switch in the Networking view of the navigation pane.



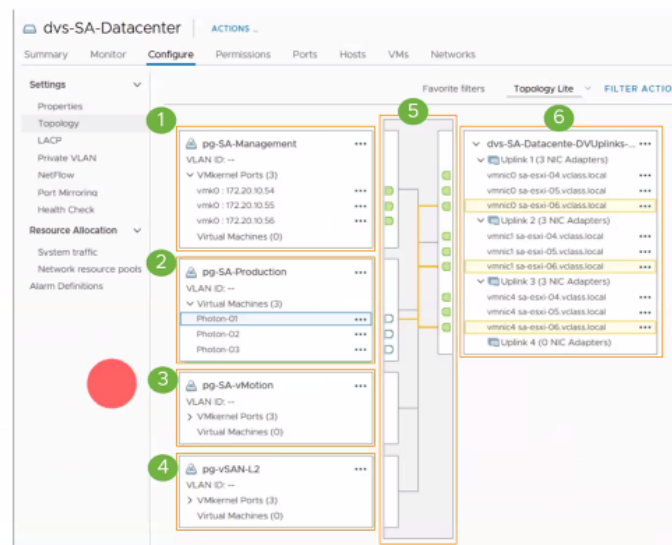
Distributed Switch: Summary Tab

The **Summary** tab shows switch details and supported features of the distributed switch.



- 첫번째 사진은 분산스위치
- 그 안에는 분산 스위치의 정보와 전에 배웠던 네트워크 프로토콜 방식 등이 기록되어 있다.
- -각 프로토콜 다시 복습

Topology Diagram

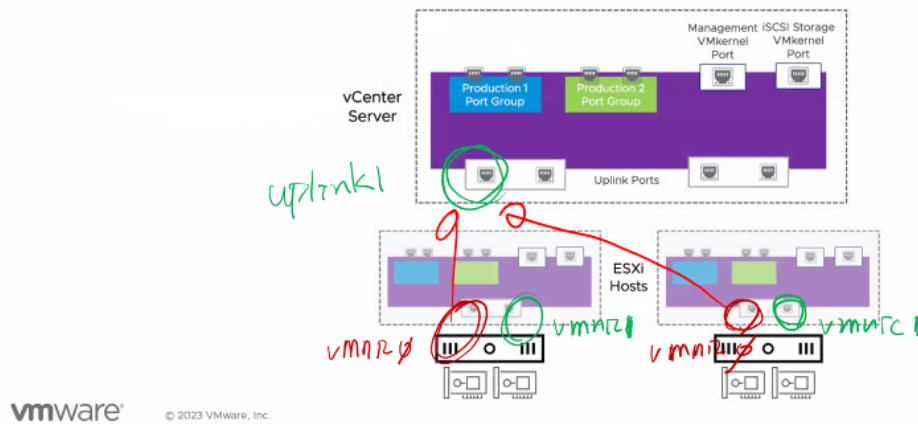


The topology diagram provides useful information for troubleshooting networking problems.

Distributed Switch Architecture

The distributed switch configuration is managed by vCenter Server:

- The port group and VMkernel port configuration is automatically pushed down to all connected ESXi hosts.
- Each ESXi host is responsible for managing their own uplink adapters and for forwarding packets from VMs to their destinations.



- 오른쪽 업링크
- 왼쪽 커널포트, 가상머신 포트그룹, vMotion 포트그룹, vSan 포트그룹
- vnic 0, 0 그룹이 uplink1에 묶인다.
- 6번 업링크를 보면 어떻게 묶여있는지 확인가능

스위치 네트워크 정책

About Networking Policies

As an administrator, you set networking policies on virtual switches to configure virtual network properties, such as security, performance, and availability.

Depending on the virtual switch type, networking policies can be applied at different levels of the virtual switch.

Virtual Switch Type	Set Default Policy At	Override Default Policy At
vSphere Standard Switch	Virtual switch level	Port group level
vSphere Distributed Switch	Port group level	Individual port level

The following networking policies are available for a virtual switch:

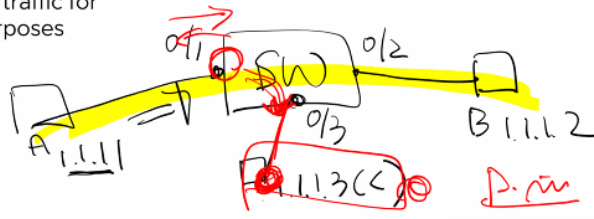
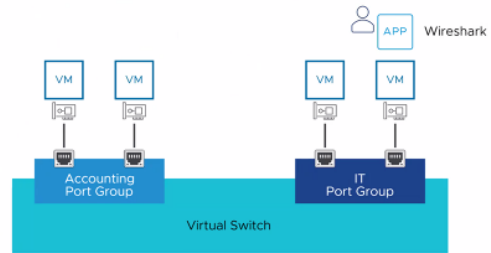
- Security
- Traffic shaping
- NIC teaming and failover

- 분산 스위치는 설정에 대한 유연성이 생긴다
- 단일 스위치는 1:1 매핑 분산 스위치는 그룹 매핑
- Nic teaming and failover
- 트래픽의 대역폭을 조절하는게 Traffic shaping
 - 20 60 40이면 줄여서 100 맞춤
- port aggregation이 이더넷 채널 (묶어버리는거)
 - 분산스위치로 사용하려고 그룹으로 묶는거 이는 액티브/스탠바이 형으로 사용가능
 - 액티브 액티브를 사용해서 로드 밸런서로 사용하는것도 가능
 - failover 시키고 싶으면 액티브 스탠바이형으로 사용

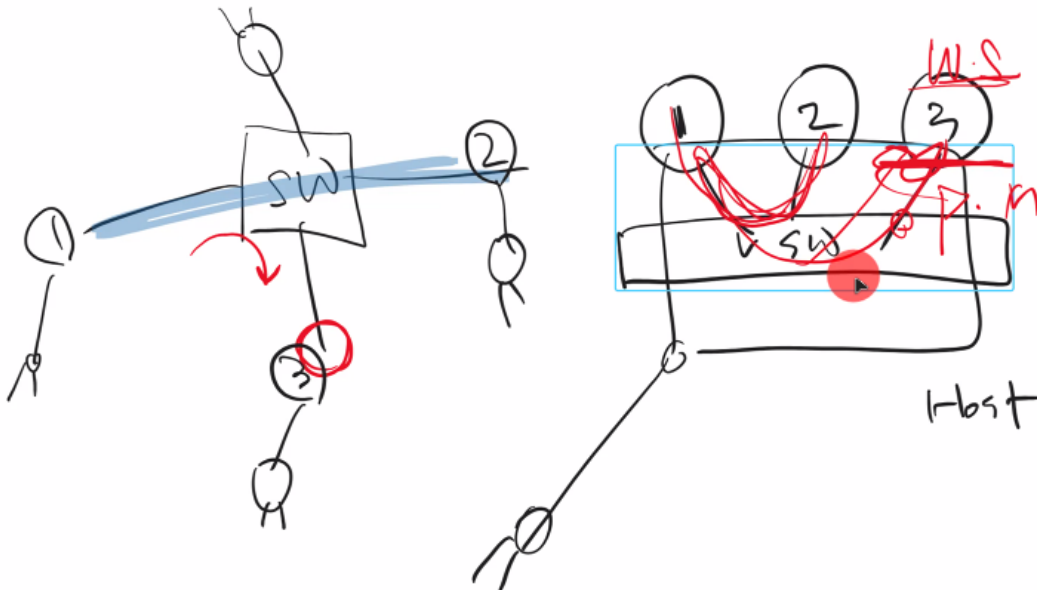
Promiscuous Mode

When promiscuous mode is enabled, the virtual NIC on a VM receives all the traffic that flows through the virtual switch. Virtual NICs see all network packets, even packets intended for other VMs.

- Why is allowing promiscuous mode a security concern?
 - Unauthorized access to confidential data
- When is allowing promiscuous mode necessary?
 - To analyze network traffic for troubleshooting purposes



- Promiscuous mode를 활성화시키면 포트 미러링이 가능
 - A → B로 주고받는 트래픽 모니터링 가능
- 분산스위치에서 지원하는 기능이다.

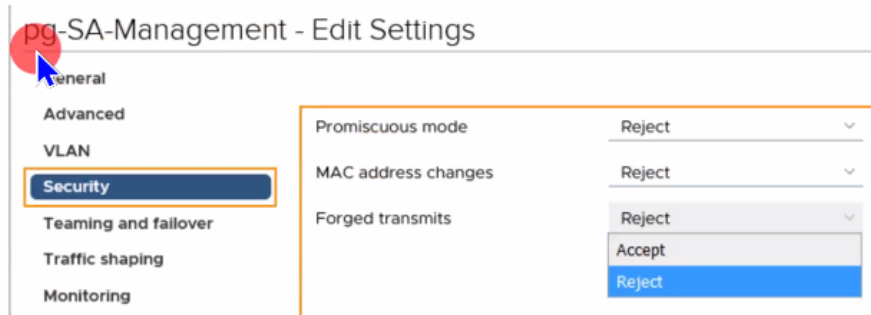


ARP 스푸핑 막기

Configuring the Security Policy

The security policy has three options. The value for each option is either Reject or Accept:

- Reject: Do not enable the option.
- Accept: Enable the option.



Note: To change the security policy, you must have the correct network configuration privileges.

- 분산스위치 관리용 인터페이스 들어가서 시큐리티 들어가면
- Forged 활성화 시키면 mac 스푸핑 막기 가능
- 그외 미러링도 활성화 지원

이중화

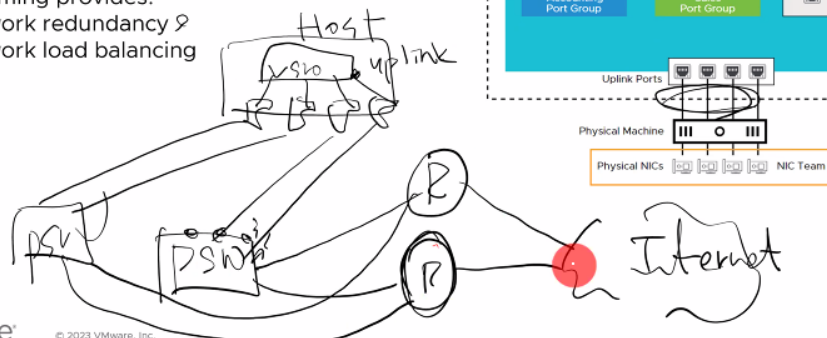
What Is NIC Teaming?

NIC teaming occurs when multiple physical NICs are associated with a virtual switch.

This group of NICs is called a NIC team.

NIC teaming provides:

- Network redundancy
- Network load balancing



- 라우터 이중화, 스위치 이중화 각각의 다른 스위치에 묶인 SW1 e/1, SW2 e/1을 각각 하나의 호스트에 연결함. 이것을 그룹화해서 가상의 분산스위치로 사용
- 가능한 모든것을 이중화하여 안정성을 확보하는게 이게 네트워크 redundancy 라고말 함
- 로드밸런싱은 xor 연산하기 때문에 균등하게 나갈 일은 없다.
 - IP해시방식 알고리즘
 - 그래도 어느정도 균등하게 트래픽을 분산시키려면 IP해시를 쓰자
- 라운드로빈 맥 add 사용방식도 있음

기술스택

기술 (Cisco IOS)

스위치 : STP, ETH, vlan/trunk

라우터: static, ospf, v2/v3

VMware

서버 가상화(vSphere v7.0) : VM, vSS, vDS, teaming, vMotion, VM 리소스 관리, HA, DRS, FT

네트워크 가상화(NSX 4.0) : NSX Manager 관리, NSX 프로그램 설치, segment 구성, gateway 구성

현업에서 사용하는 구성과 유사한 구성으로 테스트(클러스터 환경)

도커, 쿠버

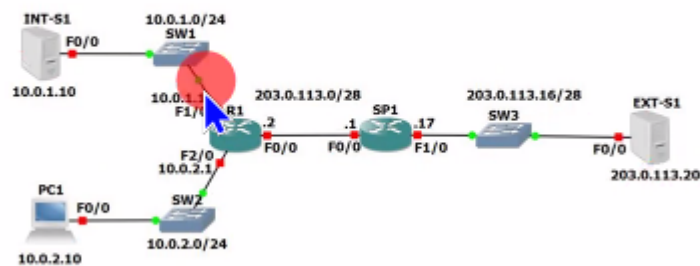
**** 네트워크 가상화 구현 순서 ****

1. NSX Manager 배포
2. 호스트에 NSX 프로그램 설치
3. Edge 노드 배포

4. L2 논리 스위치 구성(segment)
 5. L3 논리 라우터 구성(tier-0 gateway, tier-1 gateway)
-

NAT 실습

Lab Topology



1. static NAT
2. dynamic NAT
3. PAT (port address translation)

** 설정순서 **

1. 인터페이스 설정(inside/outside)
 - a. int f0/1 → ip nat inside
2. nat 설정
 - a. ip nat inside source 사설, 공인



참고 : 각 라우터에 WIC-1ENET 추가해야함

```
R1(config)#ip nat inside source list 1 int f0/0 overload
R1(config)#access-list 1 permit 10.0.1.0 0.0.0.255
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
```

- 사설망 → 공인아이피 변환
- R1 라우터 기준