

# IT 인프라 구축을 위한 VLAN & VPN

## 연구 및 구현

정지훈

# 목차

## 1. VLAN 개념

- 1) VLAN 작동 방식
- 2) VLAN 범위
- 3) VLAN 예
- 4) VLAN 특성
- 5) VLAN 유형
- 6) LAN과 VLAN의 차이점
- 7) VLAN 장/단점
- 8) VLAN 적용/목적

## 2. VLAN 구현

## 3. VPN 개념

- VPN 종류
  - L2TP, PPTP
  - IPSec
  - SSL/TLS
- VPN 구성방식
  - Remote Access VPN (=> SSL/신)
  - Site to Site VPN (=> IPsec)

## 4. VPN 구현

# 1. VLAN 개념

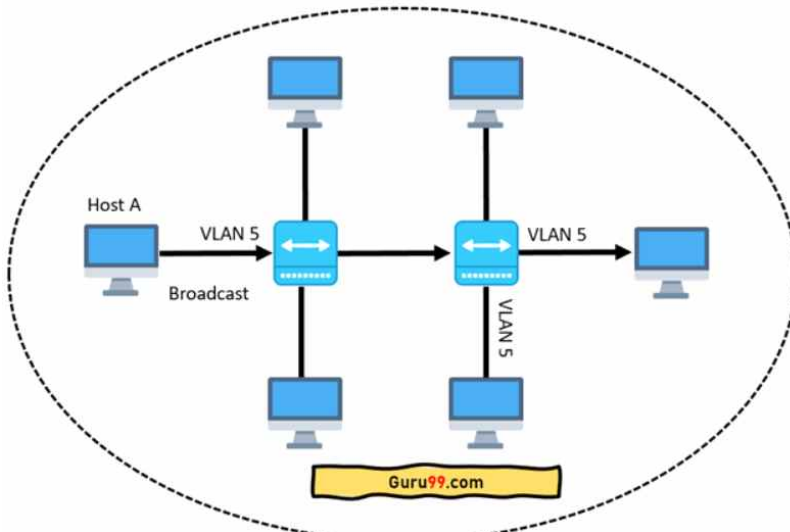
하나 이상의 근거리 통신망에서 생성된 사용자 지정 네트워크입니다. 여러 네트워크에서 사용 가능한 장치 그룹을 하나의 논리 네트워크로 결합할 수 있습니다. 그 결과 물리적 LAN처럼 관리되는 가상 LAN이 됩니다. VLAN의 전체 형태는 가상 근거리 통신망으로 정의됩니다.

아래 토폴로지는 동일한 가상 LAN 내부에 모든 호스트가 있는 네트워크를 나타냅니다.

동일한 VLAN 내에 모든 호스트가 있는 네트워크

VLAN이 없으면 호스트에서 보낸 브로드캐스트가 모든 네트워크 장치에 쉽게 도달할 수 있습니다. 각각의 모든 장치는 브로드캐스트 수신 프레임을 처리합니다. 이는 각 장치의 CPU 오버헤드를 증가시키고 전체 네트워크 보안을 감소시킬 수 있습니다.

두 스위치의 인터페이스를 별도의 VLAN에 배치하는 경우 호스트 A의 브로드캐스트는 동일한 VLAN 내에서 사용 가능한 장치에만 도달할 수 있습니다. VLAN의 호스트는 통신이 발생했는지조차 알지 못합니다.



호스트 A는 동일한 VLAN 내에서 사용 가능한 장치에만 연결할 수 있습니다.

네트워킹의 VLAN은 LAN의 가상 확장입니다. LAN은 학교, 연구실, 가정, 사무실 등 제한된 공간에서 연결된 컴퓨터 및 주변 장치의 그룹입니다. 파일, 프린터, 게임 및 기타 응용 프로그램과 같은 리소스를 공유하는 데 널리 유용한 네트워크입니다.

## 1) VLAN 작동 방식

네트워킹의 VLAN은 숫자로 식별됩니다.

유효한 범위는 1-4094입니다. VLAN 스위치에서 적절한 VLAN 번호로 포트를 할당합니다.

그런 다음 스위치는 동일한 VLAN을 가진 다양한 포트 간에 전송되어야 하는 데이터를 허용합니다.

거의 모든 네트워크가 단일 스위치보다 크기 때문에 두 스위치 간에 트래픽을 보낼 수 있는 방법이 있어야 합니다.

이를 수행하는 간단하고 쉬운 방법 중 하나는 VLAN이 있는 각 네트워크 스위치의 포트를 할당하고 그사이에 케이블을 연결하는 것입니다.

## 2) VLAN 범위

범위	설명
VLAN 0-4095	보거나 사용할 수 없는 예약된 VLAN입니다
VLAN 1	이것은 스위치의 기본 VLAN입니다. 이 VLAN은 삭제하거나 편집할 수 없지만 사용할 수는 있습니다.
VLAN 2-1001	정상적인 VLAN 범위입니다. 생성, 수정, 삭제할 수 있습니다
VLAN 1002-1005	이 범위는 토큰 링 및 FDDI에 대한 CISCO 기본값입니다. 이 VLAN은 삭제할 수 없습니다.
VLAN 1006-4094	VLAN의 확장된 범위입니다.

## 3) VLAN의 예



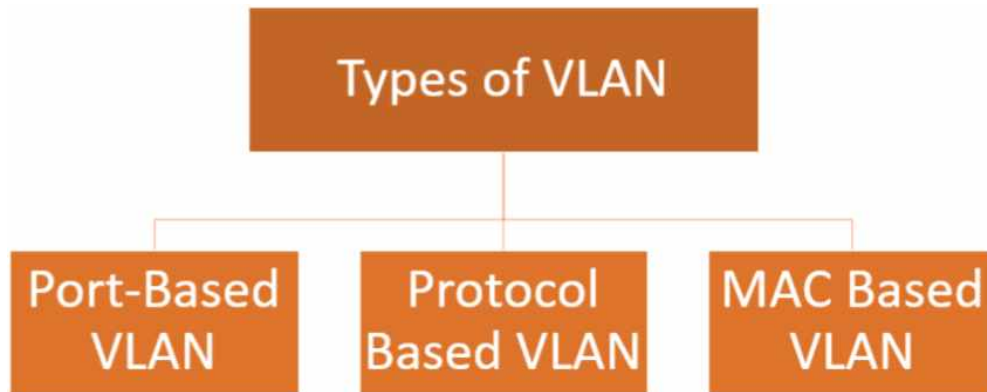
서로 다른 VLAN을 가진 6개의 스위치에 6개의 호스트가 있습니다. 스위치를 함께 연결하려면 6개의 포트가 필요합니다. 즉, 24개의 다양한 VLAN이 있는 경우 45개의 포트 스위치에 24개의 호스트만 있습니다.

## 4) VLAN의 특성

- 가상 LAN은 네트워크가 다른 경우에도 장치 그룹을 만들기 위한 구조를 제공합니다.
- LAN에서 가능한 브로드캐스트 도메인을 늘립니다.
- VLAN을 구현하면 브로드캐스트 도메인에 연결되는 호스트 수가 줄어들기 때문에 보안 위험이 줄어듭니다.
- 이는 민감한 정보가 있는 호스트에 대해서만 별도의 가상 랜을 설정하여 수행합니다.
- 네트워크 위치 대신 부서에 따라 사용자를 그룹화하는 유연한 네트워킹 모델이 있습니다.
- VLAN에서 호스트/사용자를 변경하는 것은 비교적 쉽습니다. 새로운 포트 수준 구성만 있으면 됩니다.
- 개별 VLAN이 별도의 LAN으로 작동하므로 트래픽을 공유하여 혼잡을 줄일 수 있습니다.
- 워크스테이션은 각 포트에서 전체 대역폭으로 사용할 수 있습니다.
- 터미널 재배치가 쉬워집니다.

- VLAN은 여러 스위치에 걸쳐 있을 수 있습니다.
- 트렁크 링크는 여러 LAN에 대한 트래픽을 전달할 수 있습니다.

## 5) VLAN 유형



### \* 포트 기반 VLAN

포트 기반 VLAN은 가상 LAN을 포트별로 그룹화합니다. 이러한 유형의 가상 LAN에서는 스위치 포트를 VLAN의 구성원으로 수동으로 구성할 수 있습니다.

이 포트에 연결된 장치는 다른 모든 포트가 유사한 VLAN 번호로 구성되어 있기 때문에 동일한 브로드캐스트 도메인에 속합니다.

이러한 유형의 네트워크의 과제는 각 VLAN에 적합한 포트를 아는 것입니다. VLAN 구성원은 스위치의 물리적 포트만 보고 알 수 없습니다. 구성 정보를 확인하여 결정할 수 있습니다.

### \* 프로토콜 기반 VLAN

이 유형의 VLAN은 태그가 지정되지 않은 패킷인 태그에 대한 필터링 기준을 정의하는 데 사용할 수 있는 프로토콜을 기반으로 트래픽을 처리합니다.

이 가상 근거리 통신망에서 계층 3 프로토콜은 VLAN 구성원을 결정하기 위해 프레임에 의해 전달됩니다. 다중 프로토콜 환경에서 작동합니다. 이 방법은 주로 IP 기반 네트워크에서 실용적이지 않습니다.

### \* MAC 기반 VLAN

MAC 기반 VLAN을 사용하면 태그가 지정되지 않은 수신 패킷에 가상 LAN을 할당할 수 있으므로 패킷 소스 주소에 따라 트래픽을 분류할 수 있습니다. MAC의 항목을 VLAN 테이블에 매핑하도록 구성하여 VLAN 매핑에 대한 Mac 주소를 정의합니다.

이 항목은 소스 Mac 주소 적절한 VLAN ID를 사용하여 지정됩니다. 테이블 구성은 모든 장치 포트에서 공유됩니다.

## 6) LAN과 VLAN의 차이점

LAN	VLAN
LAN은 제한된 영역에서 연결된 컴퓨터 및 주변 장치의 그룹으로 정의할 수 있습니다.	VLAN은 하나 이상의 근거리 통신망에서 생성된 사용자 지정 네트워크로 정의할 수 있습니다.
LAN의 전체 형태는 근거리통신망입니다.	VLAN의 전체 형태는 가상 근거리 통신망입니다.
LAN의 대기 시간이 높습니다.	VLAN의 대기 시간은 더 적습니다.
LAN 비용이 높습니다.	VLAN 비용은 더 적습니다.
LAN에서 네트워크 패킷은 모든 장치에 보급됩니다.	VLAN에서 네트워크 패킷은 특정 브로드캐스트 도메인으로만 전송됩니다.
링을 사용하며 FDDI(Fiber Distributed Data Interface)가 프로토콜입니다.	ISP와 VTP를 프로토콜로 사용합니다.

## 7) VLAN의 장/단점

### VLAN 장점

- VLAN은 브로드캐스트 도메인의 크기를 줄입니다.
- VLAN을 사용하면 보안 계층을 추가할 수 있습니다.
- 그것은 장치 관리를 간단하고 쉽게 만들 수 있습니다.
- 위치가 아닌 기능별로 장치를 논리적으로 그룹화할 수 있습니다.
- 이를 통해 자체 네트워크에 있는 것처럼 작동하는 논리적으로 연결된 장치 그룹을 만들 수 있습니다.
- 부서, 프로젝트 팀 또는 기능을 기반으로 네트워크를 논리적으로 분할할 수 있습니다.
- VLAN은 성장하는 회사를 지원하기 위해 네트워크를 지리적으로 구성하는 데 도움이 됩니다.
- 더 높은 성능과 감소된 대기 시간.
- VLAN은 향상된 성능을 제공합니다.
- 사용자는 다른 사용자가 볼 수 없는 민감한 정보에 대해 작업할 수 있습니다.
- VLAN은 물리적 경계를 제거합니다.
- 네트워크를 쉽게 분할할 수 있습니다.
- 네트워크 보안을 강화하는 데 도움이 됩니다.
- VLAN으로 호스트를 분리할 수 있습니다.
- 추가 하드웨어와 케이블이 필요하지 않으므로 비용을 절감할 수 있습니다.
- 소프트웨어에서 사용자의 IP 서브넷을 변경하기 때문에 운영상의 이점이 있습니다.
- 특정 네트워크 토폴로지의 장치 수를 줄입니다.
- VLAN은 물리적 장치 관리를 덜 복잡하게 만듭니다.

## **VLAN의 단점**

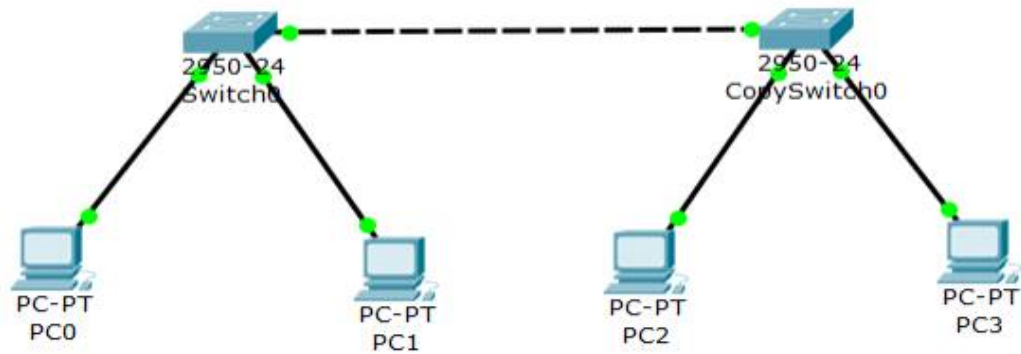
- 패킷은 한 VLAN에서 다른 VLAN으로 누출될 수 있습니다.
- 주입된 패킷은 사이버 공격으로 이어질 수 있습니다.
- 단일 시스템의 위협은 전체 논리 네트워크를 통해 바이러스를 퍼뜨릴 수 있습니다.
- 대규모 네트워크에서 워크로드를 제어하려면 추가 라우터가 필요합니다.
- 상호 운용성 문제에 직면할 수 있습니다.
- VLAN은 네트워크 트래픽을 다른 VLAN으로 전달할 수 없습니다.

## **8) VLAN의 적용/목적**

- VLAN은 LAN에 200개 이상의 장치가 있을 때 사용됩니다.
- LAN에 트래픽이 많을 때 유용합니다.
- VLAN은 사용자 그룹이 더 많은 보안을 필요로 하거나 많은 브로드캐스트로 인해 속도가 느려질 때 이상적입니다.
- 사용자가 하나의 브로드캐스트 도메인에 있지 않을 때 사용됩니다.
- 하나의 스위치를 여러 개의 스위치로 만드십시오.

## 2. VLAN 구현

### 네트워크 구성



### 실습 과정

#### -IP 설정

IP Configuration	
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	

PC0: 192.168.10.100/24 , PC1: 192.168.20.100/24

PC2: 192.168.10.200/24 , PC3: 192.168.20.200/24

SW1

SW2

1) 192.168.10.1

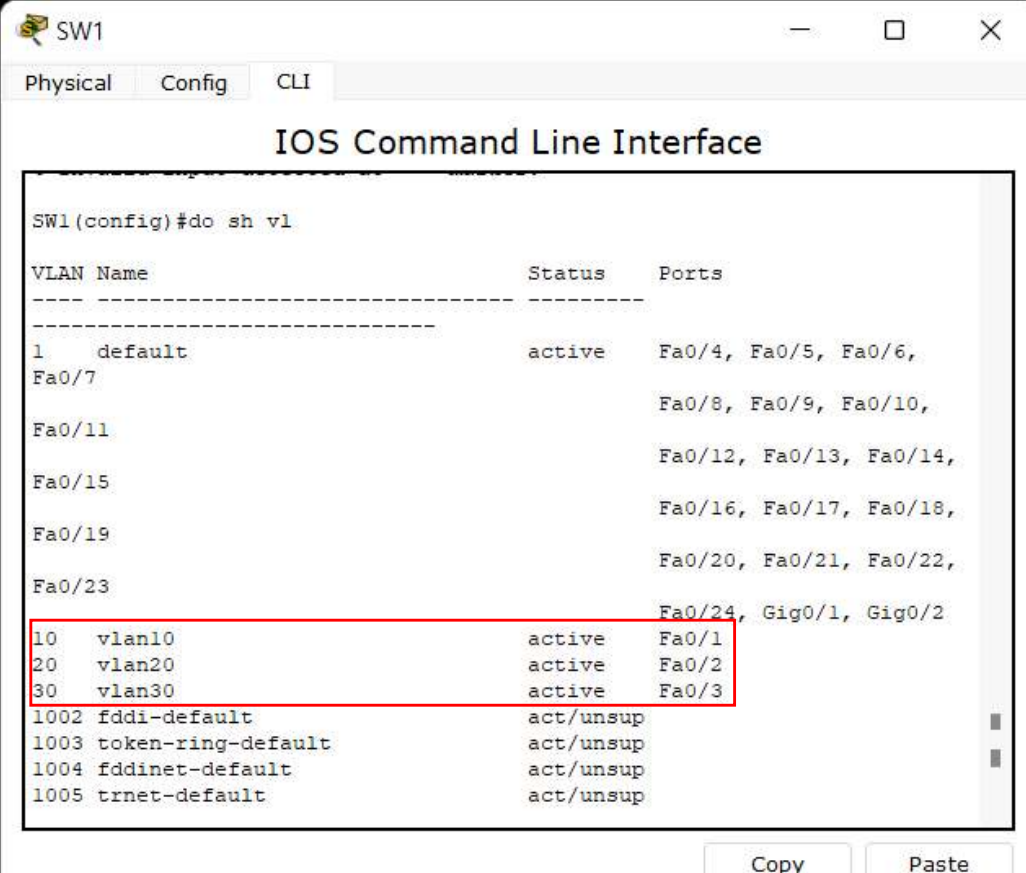
2) 192.168.10.2

1) 192.168.20.1

2) 192.168.20.2



-VLAN 조회(vlan10, vlan20, vlan30)



SW1

Physical Config CLI

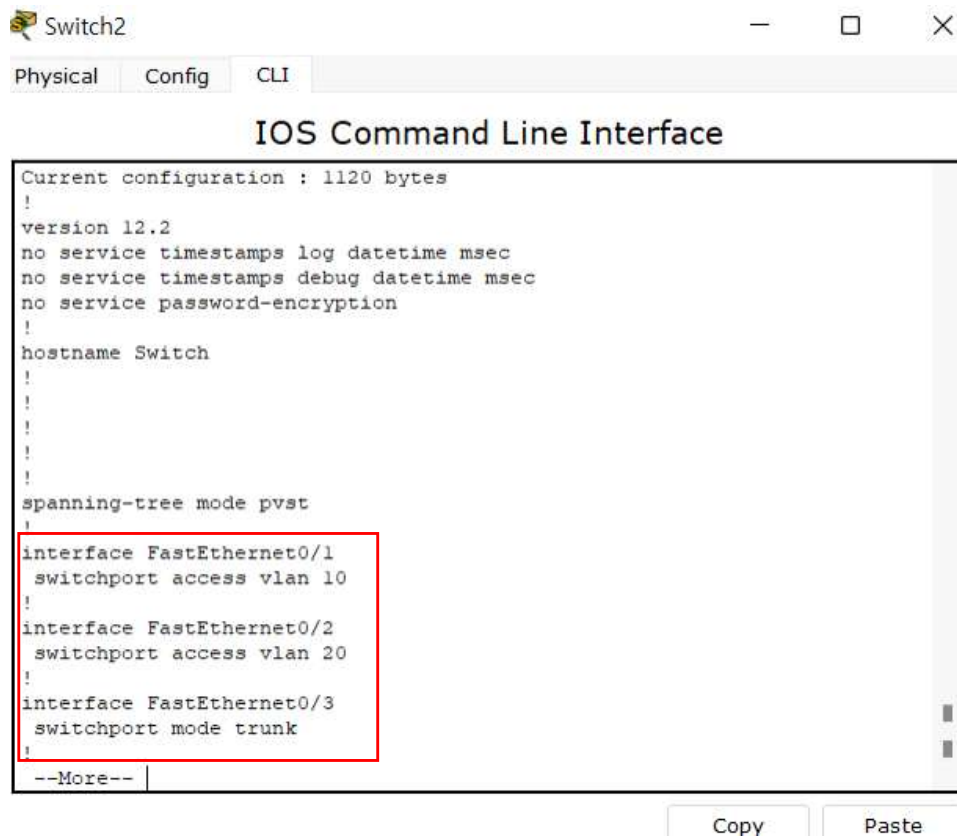
### IOS Command Line Interface

```
SW1(config)#do sh vl
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 vlan10	active	Fa0/1
20 vlan20	active	Fa0/2
30 vlan30	active	Fa0/3
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Copy Paste

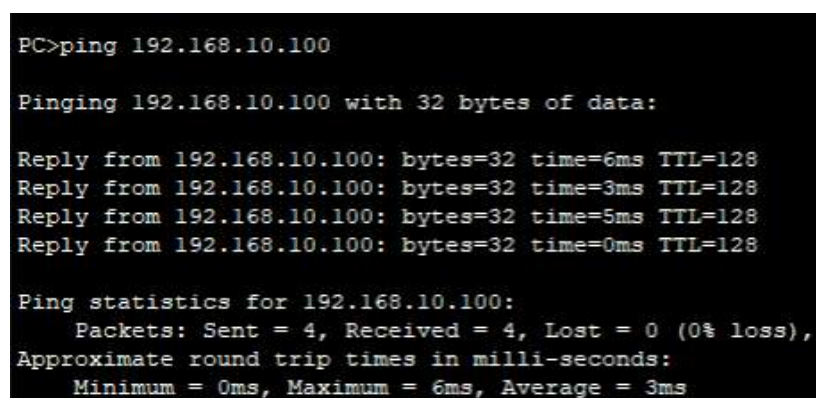
-VLAN 조회(trunk 확인)



```
Switch2
Physical Config CLI
IOS Command Line Interface

Current configuration : 1120 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 20
!
interface FastEthernet0/3
 switchport mode trunk
!
--More--
```

-Ping 테스트(PC에서 결과확인)



```
PC>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time=6ms TTL=128
Reply from 192.168.10.100: bytes=32 time=3ms TTL=128
Reply from 192.168.10.100: bytes=32 time=5ms TTL=128
Reply from 192.168.10.100: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 3ms
```

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:

Reply from 192.168.20.100: bytes=32 time=5ms TTL=128
Reply from 192.168.20.100: bytes=32 time=0ms TTL=128
Reply from 192.168.20.100: bytes=32 time=6ms TTL=128
Reply from 192.168.20.100: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 3ms
```

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.200

Pinging 192.168.10.200 with 32 bytes of data:

Reply from 192.168.10.200: bytes=32 time=1ms TTL=128
Reply from 192.168.10.200: bytes=32 time=3ms TTL=128
Reply from 192.168.10.200: bytes=32 time=0ms TTL=128
Reply from 192.168.10.200: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.10.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 4ms
```

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.200

Pinging 192.168.20.200 with 32 bytes of data:

Reply from 192.168.20.200: bytes=32 time=0ms TTL=128
Reply from 192.168.20.200: bytes=32 time=3ms TTL=128
Reply from 192.168.20.200: bytes=32 time=5ms TTL=128
Reply from 192.168.20.200: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.20.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 3ms
```

### 3. VPN 개념

VPN(영어: virtual private network)은 공중 네트워크를 통해 한 회사나 몇몇 단체가 내용을 바깥 사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망이다. 가상사설망에서 메시지는 인터넷과 같은 공공망 위에서 표준 프로토콜을 써서 전달되거나, 가상사설망 서비스 제공자와 고객이 서비스 수준 계약을 맺은 후 서비스 제공자의 사설망을 통해 전달된다.



#### -VPN 종류

##### L2TP(Layer 2 Tunneling Protocol)

가상사설망(VPN)을 지원하거나 ISP에서 제공하는 서비스 일부로 사용되는 터널링 프로토콜이다. 자체 제어 메시지(선택사항인 사전 공유 비밀 사용)에 대해서만 암호화('숨김')를 사용하며 자체적으로 콘텐츠의 암호화 또는 기밀성을 제공하지 않는다. 그보다는 계층 2(암호화될 수 있음)에 대한 터널을 제공하고 터널 자체는 IPsec과 같은 계층 3 암호화 프로토콜을 통해 제공될 수 있다.

##### PPTP(Point to Point Tunneling)

쉽게 말하자면 컴퓨터가 일련의 규칙을 따라서 서로 통신하는 언어입니다. 사용자는 이러한 통신 규칙을 사용해서 VPN 역할을 하는 공공 네트워크를 통해 "터널링"을 진행하여 개인 네트워크를 확장할 수 있습니다. 작동 방식은 IP를 통과하거나 데이터를 캡슐화하는 모든 데이터를 암호화, 인증, PPP 무효화합니다. 데이터가 캡처되면 "터널"을 통해 이동합니다. 데이터가 통과하는 모든 라우터나 기기 장치는 IP 패킷으로 처리됩니다. 이러한 터널은 LAN 또는 WAN 사용에 알맞는 안전한 통신을 제공합니다. 심지어 공용 네트워크를 사용해도 안전하게 정보를 전달합니다.

##### IPsec(Internet Protocol Security)

통신 세션의 각 IP패킷을 암호화하고 인증하는 안전한 인터넷 프로토콜(IP) 통신을 위한 인터넷 프로토콜 스위트이다. 이 보안은 통신 세션의 개별 IP 패킷을 인증하고 암호화함으로써 처리된다. IPsec은 세션의 시작에서 에이전트들 사이에서 상호 인증을 확립하거나 세션을 맺는 중에 사용될 암호화 키의 협상을 위한 프로토콜을 포함한다. IPsec은 호스트 한쌍 사이(Host와 host), 보안 게이트웨이 사이(네트워크와 네트워크), 보안 게이트웨이와 호스트 사이(네트워크와 호스트)에 데이터 흐름을 보호하기 위해 사용된다. Internet Protocol security (IPsec)

은 Internet Protocol 네트워크 사이에 통신을 지키기 위해 암호의 보안 서비스를 사용한다.

IPsec 보안 구조 : 인증헤더(AH), 보안 페이로드 캡슐화(ESP), 보안 연관(SA)

IPsec 동작 방식: 전송모드(Transpot mode), 터널모드(Tunnel Mode)

## SSL/TLS

SSL(Secure Socket Layer)



암호화 기반 인터넷 보안 프로토콜이다. 전달되는 모든 데이터를 암호화하고 특정한 유형의 사이버 공격도 차단한다. SSL은 TLS(Transport Layer Security) 암호화의 전신이기도 한다.

SSI/TLS를 사용하는 웹사이트 URL은 HTTP 대신 HTTP가 사용된다.

## TLS

SSL의 업데이트 버전으로 SSL의 최종버전인 3.0과 TLS의 최초버전의 차이는 크지않으며, 이름이 바뀐것은 SSL을 개발한 Netscape가 업데이트에 참여하지 않게 되어 소유권 변경을 위해서였다고 한다.

결과적으로 TLS는 SSL의 업데이트 버전이며 명칭만 다르다고 볼 수 있다.

## - VPN 구성방식

Remote Access VPN (=> SSL/TLS)

출장 혹은 재택근무 중인 직원이 원격지에서 본사 내부 자원에 접근하려는 경우 안전하게 접근하기 위한 목적으로 구성되는 VPN 서비스

Site-to-Site IPsec VPN과의 차이점

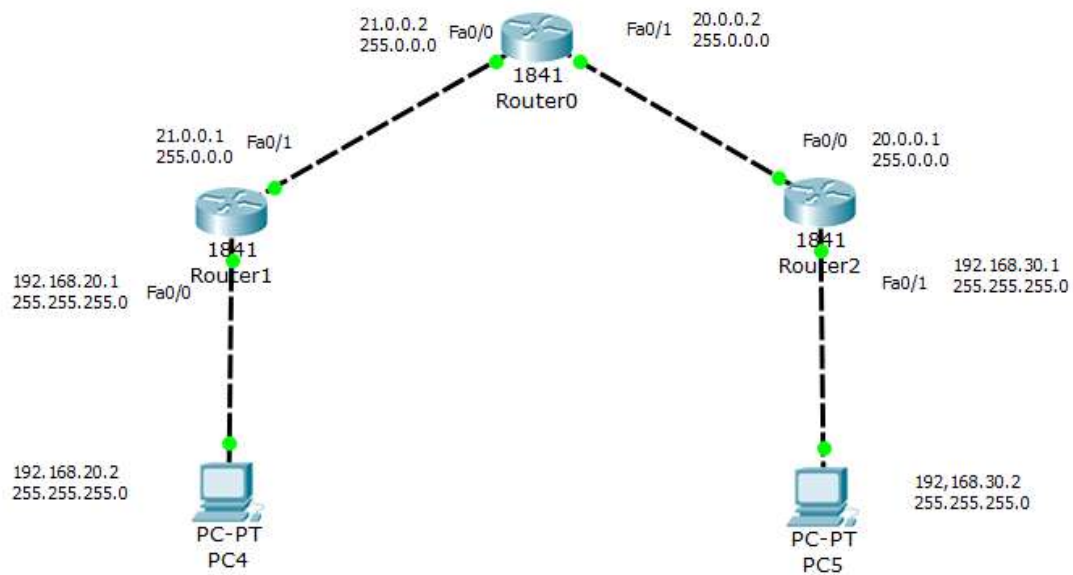
- H(암호화 X) 방식은 불가능하고 ESP(암호화 O) 방식만 사용이 가능하다.
- Transport 모드는 사용이 불가능하고 Tunnel 모드만 사용이 가능하다.
- Diffie-Hellman 협상 과정에서 Group 1(768bit)은 지원안되고, Group 2(1024bit)부터 사용가능하다.

Site to Site VPN (=> IPsec)

Site-to-Site VPN을 설정하면 두 개의 중복 IPsec 터널이 있습니다. Oracle은 두 터널을 모두 사용하도록 CPE 장치를 구성할 것을 권장합니다(장치가 지원하는 경우). 과거에 Oracle은

최대 4개의 IPSec 터널이 있는 IPSec 연결을 만들었습니다..

#### 4. VPN 구현



#### 실습순서

- 라우터 연결 확인
- VPN 터널 생성 및 구성
- 라우터 간 연결 체크
- 결과 (PC4, PC5 핑 테스트 및 터널링 확인)

#### 실습 과정

## -라우터 연결 확인

Router1

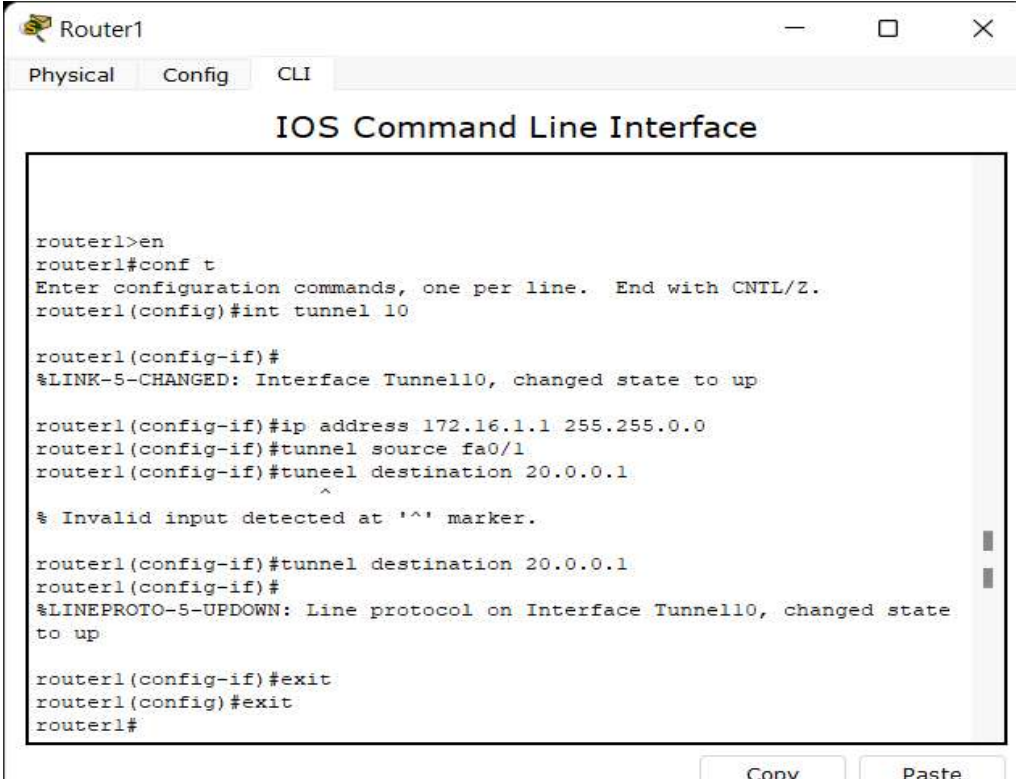
```
router1#ping 20.0.0.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
```

Router2

```
router2#ping 21.0.0.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 21.0.0.1, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms
```

## -VPN 터널 생성 및 구성





Router1

Physical Config CLI

### IOS Command Line Interface

```
router1>en
router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#int tunnel 10

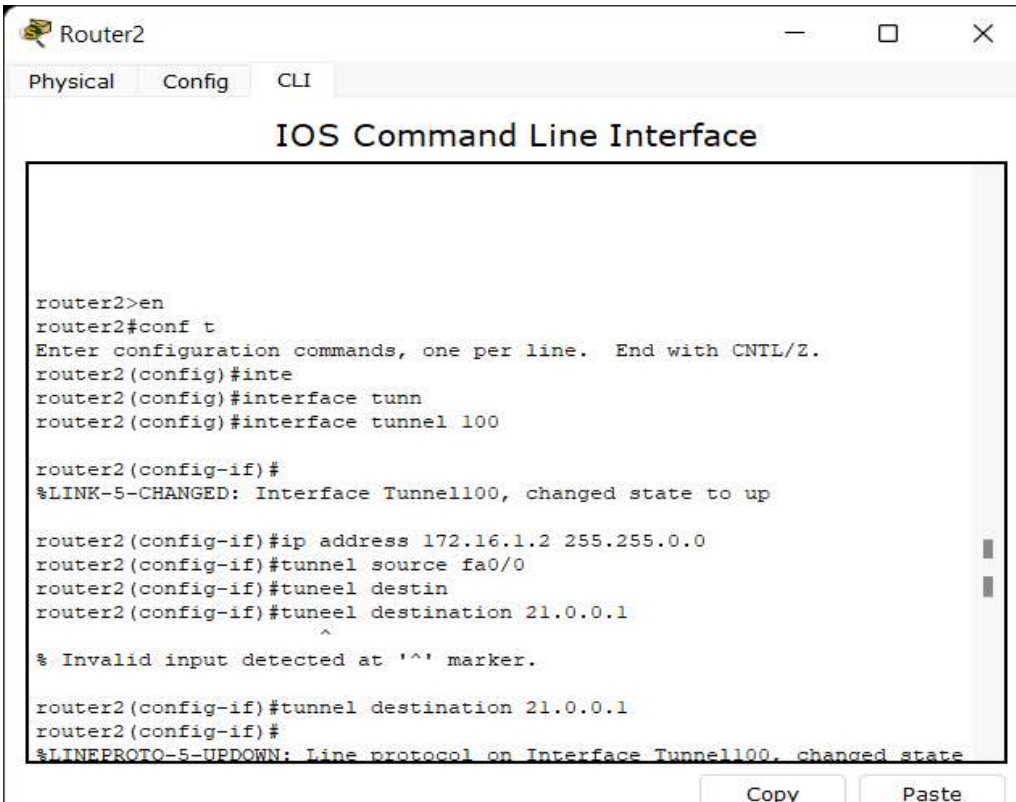
router1(config-if)#
%LINK-5-CHANGED: Interface Tunnel10, changed state to up

router1(config-if)#ip address 172.16.1.1 255.255.0.0
router1(config-if)#tunnel source fa0/1
router1(config-if)#tunnel destination 20.0.0.1
^
% Invalid input detected at '^' marker.

router1(config-if)#tunnel destination 20.0.0.1
router1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state
to up

router1(config-if)#exit
router1(config)#exit
router1#
```

Copy Paste



Router2

Physical Config CLI

### IOS Command Line Interface

```
router2>en
router2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router2(config)#inte
router2(config)#interface tunn
router2(config)#interface tunnel 100

router2(config-if)#
%LINK-5-CHANGED: Interface Tunnel100, changed state to up

router2(config-if)#ip address 172.16.1.2 255.255.0.0
router2(config-if)#tunnel source fa0/0
router2(config-if)#tunnel destin
router2(config-if)#tunnel destination 21.0.0.1
^
% Invalid input detected at '^' marker.

router2(config-if)#tunnel destination 21.0.0.1
router2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed state
```

Copy Paste

-라우터 간 연결 체크



A screenshot of a network simulator window titled "Router1". It has tabs for "Physical", "Config", and "CLI", with "CLI" selected. The main area is titled "IOS Command Line Interface" and contains a terminal window. The terminal shows the following commands and output:

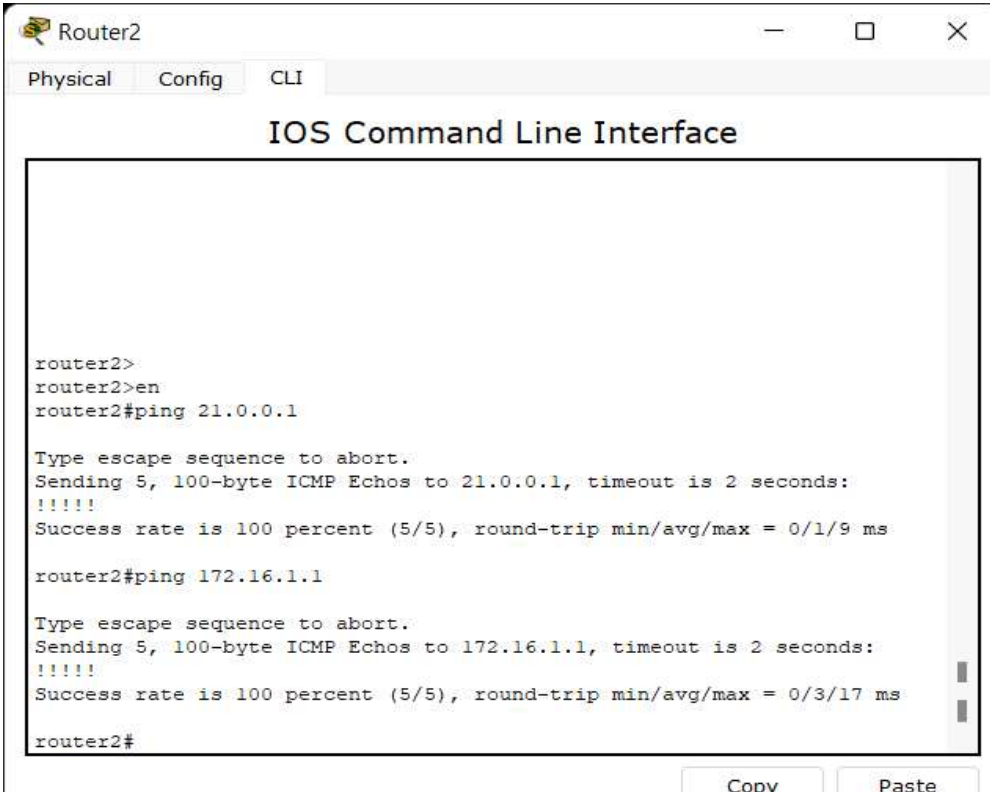
```
router1>
router1>en
router1#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

router1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

router1#
```

At the bottom right of the window are "Copy" and "Paste" buttons.A screenshot of a network simulator window titled "Router2". It has tabs for "Physical", "Config", and "CLI", with "CLI" selected. The main area is titled "IOS Command Line Interface" and contains a terminal window. The terminal shows the following commands and output:

```
router2>
router2>en
router2#ping 21.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 21.0.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/9 ms

router2#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/17 ms

router2#
```

At the bottom right of the window are "Copy" and "Paste" buttons.

결과 (PC4, PC5 핑 테스트 및 터널링 확인)

