

제20장 VLAN

VLAN(Virtual LAN)

사용자 증가로 인한 많은 양의 브로드캐스트 플러딩으로 대역폭이 저하되거나, 전송 장비 부하 발생은 LAN 구간에서 자리 잡고 있는 문제점 중에 하나이다. 그리고 스위치로 구성된 LAN 구간은 하나의 도메인으로 동작하기 때문에 상호간에 접근 자체가 허용되므로 보안적인 측면에서도 문제가 될 수 있다. 이런 문제들을 해결하기 위한 방법으로는 VLAN을 구성하여 논리적으로 분할된 스위치 네트워크, 즉 논리적인 브로드캐스트 도메인을 구성하여 브로드캐스트 접근 자체를 차단하는 것이다.

VLAN 구성 이점

- ① 논리적인 브로드캐스트 도메인을 분할하여 브로드캐스트 플러딩을 최소화한다.
- ② 서로 다른 VLAN 간에 브로드캐스트가 차단되므로 ARP 학습에 의한 유니캐스트 접근이 불가능하다.
- ③ Spanning-Tree 이중화 환경에서 VLAN 로드 분산이 가능하다.
- ④ 논리적인 브로드캐스트 도메인이기 때문에 위치상 제약이 없으며, 관리상 효율적이다.

VLAN 데이터베이스

VLAN 생성 정보와 스위치 포트 매핑 정보를 관리하는 테이블이다. 기본적으로 VLAN 1, VLAN 1002~1005가 관리되며, 이 5개의 VLAN은 수정 및 삭제가 불가능하다. VLAN은 1~4094 범위 내에서 사용할 수 있으며, 스위치에서 사용 가능한 VLAN은 최대 1005개로 제한된다. 이때, VLAN 1~1005까지를 Standard VLAN이라고 하며, VLAN 1006~4094까지를 Extended VLAN이라고 한다. [예제 20-1]은 초기화된 스위치의 VLAN 데이터베이스를 확인한 것이다.

[예제 20-1] 스위치 기본 VLAN 데이터베이스 내용

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

기본적으로 관리하는 VLAN 1, VLAN 1002~1005를 삭제, 또는 수정이 가능한지 확인하도록 하자.

[예제 20-2] 기본 VLAN 1, VLAN 1002~1005는 삭제 및 수정이 불가능함

```
Switch(config)#no vlan 1
Default VLAN 1 may not be deleted.
Switch(config)#
Switch(config)#vlan 1
Switch(config-vlan)#name TEST
Default VLAN 1 may not have its name changed.
```

VLAN 데이터베이스에서 관리할 수 있는 VLAN은 최대 1005개이다. 그럼 스위치에서 VLAN를 1005개 이상 생성이 가능한지 확인하도록 하자.

[예제 20-3] 스위치에서 생성 가능한 VLAN은 최대 1005개로 제한되어 있음

```
Switch(config)#vlan 2-1010
Switch(config-vlan)#end
%Proposed configuration exceeds the limit of 1005 VLANs that can be supported on
this platform. Reduce the number of VLANs proposed to be within this limit.
```

VLAN 데이터베이스는 NVRAM에 저장하여 관리되는 것이 아니라, 스위치 플래시 메모리에 'vlan.dat'라는 파일로 별도로 저장하여 관리된다. 그렇기 때문에 NVRAM에 저장된 설정 내용이 삭제되어도 VLAN 데이터베이스 내용은 영구적으로 보존된다. 단, 플래시 메모리에 저장된 'vlan.dat' 파일을 삭제한 다음, 스위치가 재부팅되면 VLAN 데이터베이스 내용은 초기화된다.

[예제 20-4] VLAN 데이터베이스 파일 확인

```
Switch(config)#vlan 11
Switch(config-vlan)#end
Switch#
Switch#show flash

System flash directory:
File Length Name/status
  1  8662192 c3560-advipservicesk9-mz.119-37.SE1.bin
  2   616    vlan.dat
[8662808 bytes used, 55353576 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

만약, VLAN 데이터베이스를 초기화하려면, 스위치 플래시 메모리에 저장되어 있는 'vlan.dat' 파일을 삭제한 다음, 스위치를 재부팅하면 된다. 이때, 'vlan.dat' 파일을 삭제할때에는 오타가 입력되지 않도록 주의해야 한다. 간혹 'vlan.dat' 파일을 삭제하려다가, Cisco IOS도 같이 삭제하는 경우가 있기 때문이다. 이럴때는 스위치를 재부팅하면 안된다. 왜냐하면 Cisco IOS가 로딩되어 동작하고 있을 경우, Cisco IOS를 업로드하기가 간편

하기 때문이다. 그러나 스위치를 재부팅하면 더 이상 Cisco IOS를 로딩할 수가 없기 때문에, 이때는 X-모뎀을 이용하여 장시간 동안 Cisco IOS를 업로드해야하는 문제가 발생한다. [예제 20-5]는 'vlan.dat' 파일을 삭제한 다음, 스위치를 재부팅하는 과정이다.

[예제 20-5] 'vlan.dat' 삭제 및 스위치 재부팅

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Switch#show flash

System flash directory:
File Length Name/status
  1  8662192 c3560-advipservicesk9-mz.119-37.SE1.bin
[8662192 bytes used, 55354192 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

Switch#reload
Proceed with reload? [confirm]
```

만약, Cisco IOS가 삭제된 경우, 스위치를 재부팅하면 [예제 20-6]과 같이 부트 로더 모드로 시작된다.

[예제 20-6] Cisco IOS 로딩을 실패한 경우, 시작하는 부트 로더 모드

```
Switch#show flash

System flash directory:
File Length Name/status
[0 bytes used, 64016384 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

Switch#
Switch#reload
Proceed with reload? [confirm]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/8184K bytes of
memory.
3560-24PS starting...
Base ethernet MAC Address: 0002.171E.D3B6
Xmodem file system is available.
```

```
Initializing Flash...
flashfs[0]: 0 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 0
flashfs[0]: Bytes available: 64016384
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Boot process failed...

The system is unable to boot automatically. The BOOT
environment variable needs to be set to a bootable
image.
switch: <- Boot Loader 모드
switch:
```

스위치 포트들이 하나의 브로드캐스트 도메인으로 동작하여 브로드캐스트를 플러딩하는 이유는 [예제 20-7]과 같이 모든 스위치 포트가 기본적으로 VLAN 1 도메인에 소속되어 있기 때문이다. 예를 들어 F0/4로 브로드캐스트를 수신하면 VLAN 1에 속해 있는 모든 스위치 포트에 브로드캐스트가 플러딩되는 것이다.

[예제 20-7] 스위치 기본 VLAN 데이터베이스 내용

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN 구성 단계

VLAN을 구성하기 위해서는 가장 먼저 VLAN 도메인을 생성한 다음, VLAN 설계 기반으로 스위치 포트를 해당 VLAN으로 매핑해야 한다. 또한, 스위치가 다수인 경우에는 물리적인 연결 문제와 확장성에 대한 문제를 해결하기 위해서 스위치와 스위치 연결을 트렁크로 구성해야 한다.

VLAN 생성 및 삭제

vlan 11을 생성하면, 기본적으로 'VLAN0011'이라는 이름으로 생성된다. 이름을 변경하고자 한다면, 'name' 명령어를 이용하여 수정할 수 있으며, vlan 11을 삭제하고자 한다면, 'no' 명령어를 이용한다.

[예제 20-8] VLAN 생성 및 이름 변경

```
Switch(config)#vlan 11
Switch(config-vlan)#do show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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
11 VLAN0011	active	

~ 중간 생략 ~

```
Switch(config-vlan)#name VLAN_A
Switch(config-vlan)#do show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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
11 VLAN_A	active	

~ 중간 생략 ~

[예제 20-9] VLAN 삭제

```
Switch(config-vlan)#no vlan 11
Switch(config)#
Switch(config)#do show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

스위치 포트 매핑

VLAN 생성이 완료된 다음, VLAN 설계 내용을 기반으로 스위치 포트를 해당 VLAN으로 매핑한다. 이때, 스위치 포트를 Access Mode로 전환하여 단일 호스트 포트로 구성한 다음, 해당 VLAN 도메인으로 매핑시킨다. 이때, 동일한 VLAN에 이동되는 스위치 포트가 많은 경우, 'range', '-', ',' 옵션을 이용하면 설정이 간단해진다.

[예제 20-10] 스위치 포트 매핑

```
Switch(config)#vlan 11
Switch(config-vlan)#name VLAN_A
Switch(config-vlan)#vlan 12
Switch(config-vlan)#name VLAN_B
Switch(config-vlan)#
Switch(config-vlan)#int range fa0/2 , fa0/4 - 5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 11
Switch(config-if-range)#
Switch(config-if-range)#int range fa0/12 - 13
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 12
```

스위치 포트 매핑이 완료되었다면, VLAN 데이터베이스 내용을 확인하도록 한다.

[예제 20-11] 스위치 포트 매핑 이후, VLAN 데이터베이스 내용

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/3, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 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
11 VLAN_A	active	Fa0/2, Fa0/4, Fa0/5
12 VLAN_B	active	Fa0/12, Fa0/13
~ 중간 생략 ~		

[예제 20-11]을 보면, 앞으로 F0/5로 브로드캐스트를 수신하면, 같은 VLAN 11에 소속된 F0/2, F0/4으로만 브로드캐스트를 플러딩한다. 또한, ARP 요청에 의한 MAC 주소 학습도 같은 VLAN 11에 소속된 F0/2, F0/4, F0/5에 연결된 호스트들만 가능하기 때문에, VLAN 11에 소속된 호스트들만 유니케스트가 가능하다. 스위치 포트 상태를 확인하려면 [예제 20-12]와 같이 'show interface [Interface-Type] switchport'를 실시한다.

[예제 20-12] 스위치 포트 상태 확인

```
SW1#show interfaces fa0/2 switchport
```

```
Name: Fa0/2
```

```
Switchport: Enabled
```

```
Administrative Mode: static access
```

```
Operational Mode: static access
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: native
```

```
Negotiation of Trunking: On
```

```
Access Mode VLAN: 11 (VLAN_A)
```

```
Trunking Native Mode VLAN: 1 (default)
```

```
Voice VLAN: none
```

```
~ 중간 생략 ~
```

```
Trunking VLANs Enabled: ALL
```

```
Pruning VLANs Enabled: 2-1001
```

```
Capture Mode Disabled
```

```
Capture VLANs Allowed: ALL
```

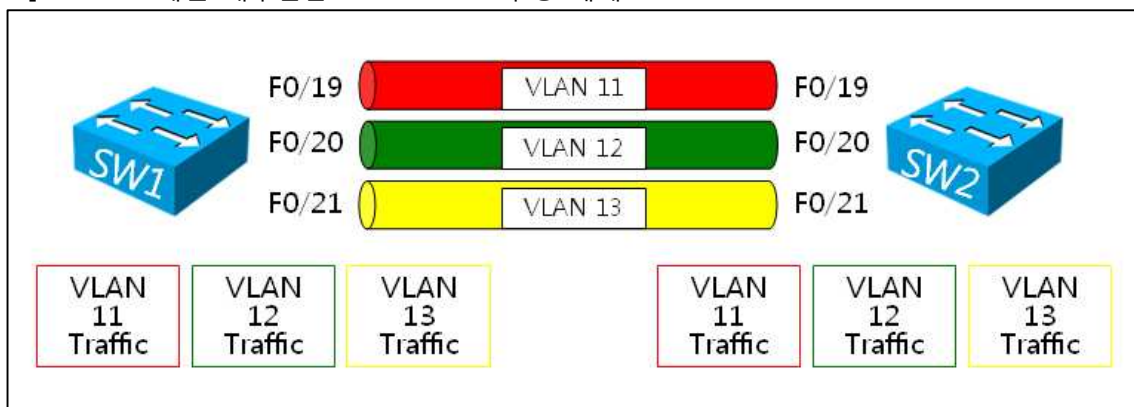
```
Protected: false
```

```
Appliance trust: none
```


트렁크 포트 구성

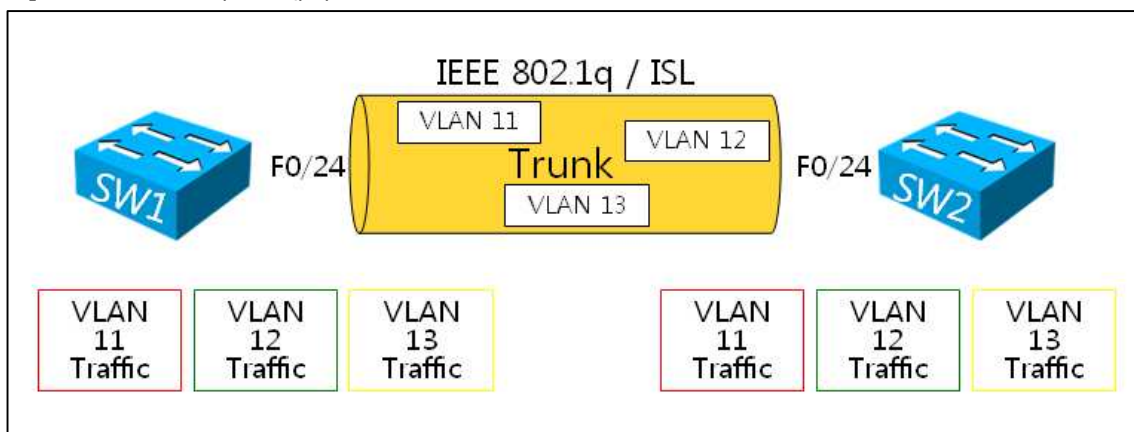
스위치와 스위치 간에 VLAN 개수만큼 연결하여 Access 포트에 설정할 경우, 확장성에 대한 문제점이 발생된다. 만약, SW1과 SW2 간에 VLAN 11, 12, 13을 연결하기 위해서 [그림 20-1]과 같이 크로스오버 케이블을 VLAN 개수만큼 3개를 연결한 다음, 각각 VLAN 11, 12, 13에 대한 Access 포트에 설정하면, 나중에 VLAN 개수가 증가될 경우 스위치 포트 개수가 부족하거나, 물리적인 연결에 대한 번거로움이 발생된다.

[그림 20-1] VLAN 도메인 개수만큼 Access 포트 구성 예제



[그림 20-1]과 같이 스위치와 스위치 간에 VLAN 개수만큼 연결하여 Access 포트에 구성하는 방법은 가장 신뢰적인 방법이지만, 앞서서도 언급했듯이 확장성에 대한 문제점과 물리적인 연결에 대한 번거로움이 있기 때문에 일반적으로 [그림 20-2]와 같이 트렁크 포트를 구성하여 이더넷 프레임에 VLAN-ID를 태깅하여 프레임 전송하는 방법을 주로 사용한다.

[그림 20-2] 트렁크 포트 구성 예제



이처럼 스위치와 스위치 간에 트렁크를 구성하면, 이더넷 프레임에 VLAN-ID를 태깅하여 전송 처리가 가능하기 때문에, VLAN 개수만큼 Access 포트를 구성할 필요가 없다. 이러한 트렁크 기법은 VLAN 환경뿐만 아니라, 일반 PSTN 전화 서비스에서도 볼 수 있다. 예를 들어 사무실 내에 전화기들은 회사 내부에 위치해 있는 사설 PBX 교환기에 개별적인 회선으로 연결되고, 사설 PBX 교환기는 전화국 CO 스위치와 하나의 트렁크 회선을 통하여 음성 신호를 전달한다. 그렇기 때문에 사무실 내부 전화기들과 전화국 CO 스위치 간에 개별적인 연결을 할 필요가 없기 때문에 확장성과 회선 비용 절감이라는 장점을 갖게된다.

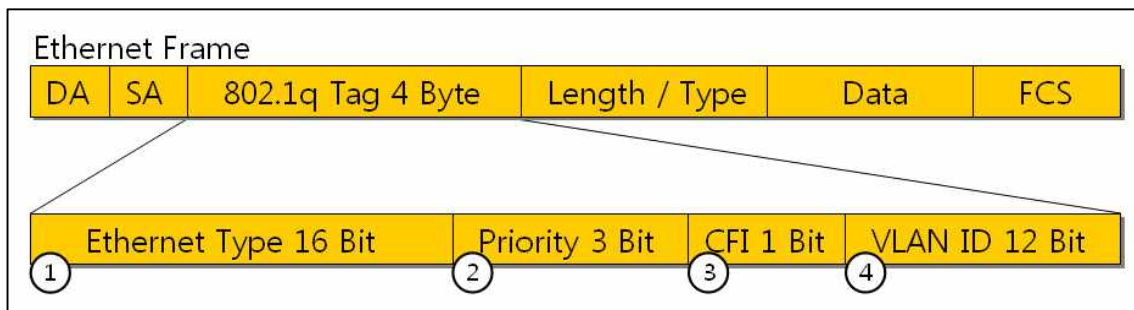
트렁크 프로토콜

트렁크란 하나의 회선에서 다수의 VLAN 프레임을 전달하는 구간을 말한다. 즉, 하나에 스위치에서 다른 스위치로 다수의 VLAN 프레임을 전달하기 위해서 VLAN-ID를 기록하여 전달하는 구간을 의미한다. 이때, VLAN-ID를 기록하는 작업을 태깅이라고 하며, VLAN-ID를 태깅하기 위해서는 트렁크 프로토콜이 필요하다.

IEEE 802.1q 트렁크 프로토콜

IEEE 802.1q는 IEEE 기관에서 정의한 표준 트렁크 프로토콜로서 여러 벤더 제품과 호환이 가능하기 때문에 가장 많이 사용되고 있다. IEEE 802.1q 트렁크 프로토콜은 12Bit의 VLAN-ID를 사용하기 때문에 VLAN 1~4094까지 지원할 수 있다. [그림 20-3]은 IEEE 802.1q 헤더 내용을 보여주고 있다.

[그림 20-3] IEEE 802.1q 헤더 내용



- ① 802.1q와 802.1p 태그 정보이며 고정값인 0x8100을 사용한다.
- ② 802.1p 트래픽 우선순위 값이며, 3Bit이기 때문에 8개의 우선순위를 설정할 수 있다.
- ③ 이더넷에서는 0으로 설정되며, 토큰링에서는 1로 설정되어 사용된다.
- ④ VLAN-ID 필드이며, 12Bit를 사용하기 때문에 VLAN을 최대 4094까지 지원한다. 또한, VLAN-ID가 없을 경우에는 Native VLAN으로 인식한다.

스위치 포트를 IEEE 802.1q 트렁크 포트 구성하는 방법은 다음과 같다.

[예제 20-13] IEEE 802.1q 트렁크 포트 구성

```
SW1(config)#int fa0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
```

만약, IEEE 802.1q 트렁크 프로토콜만 지원하는 스위치인 경우, 트렁크 포트 구성은 다음과 같다.

[예제 20-14] IEEE 802.1q 트렁크 포트 구성

```
SW1(config)#int fa0/24
SW1(config-if)#switchport mode trunk
```

트렁크 포트 구성이 완료되었다면, 다음과 같이 트렁크 정보 확인을 실시하도록 한다.

[예제 20-15] IEEE 802.1q 트렁크 포트 구성

```
SW1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/24    on        802.1q         trunking    1
          ①          ②          ③          ④

Port      Vlans allowed on trunk ⑤
Fa0/24    1-4094

Port      Vlans allowed and active in management domain ⑥
Fa0/24    1,11-12

Port      Vlans in spanning tree forwarding state and not pruned ⑦
Fa0/24    1,11-12

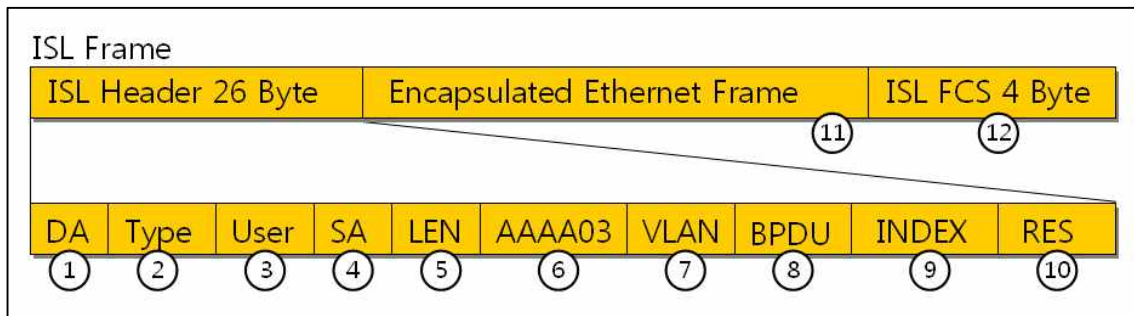
SW1#show interfaces fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
~ 중간 생략 ~
```

- ① on, auto, desirable이라는 3가지 유형의 트렁크 구성 모드이며, 이때 on 모드는 DTP 프로토콜을 이용하지 않고 트렁크를 수동으로 구성한 것을 의미한다. 만약, DTP 프로토콜을 이용하여 트렁크가 구성되면 Desirable 모드로 출력된다.
- ② 사용중인 트렁크 프로토콜을 의미한다. 만약, n-802.1q, n-isl로 출력되면 DTP 프로토콜을 이용하여 상대방과 협의하여 트렁크를 구성한 것이다.
- ③ F0/24 포트가 트렁크 포트로 동작하는 것을 알 수 있다.
- ④ VLAN-ID가 태깅되지 않는 Untagged 프레임을 수신하면, 해당 프레임을 처리하는 VLAN을 의미한다.
- ⑤ 트렁크 포트는 기본적으로 VLAN 1~4094까지 모든 VLAN들에 대해서 트렁크 사용을 허용한다.
- ⑥ 현재 VLAN 데이터베이스에 등록되어 사용 가능한 VLAN을 태깅한다는 의미이다.
- ⑦ Spanning-Tree 환경에서 프레임 전송이 가능한 VLAN 도메인과 VTP Pruning에 적용되지 않는 VLAN을 의미한다.

Cisco ISL 트렁크 프로토콜

ISL(Inter-Switch Link)는 시스코에서 개발한 트렁크 프로토콜이며 시스코 장비간에서만 호환된다. 스위치에서 프레임을 트렁크 포트를 통해 전송할 경우 이더넷 프레임에 ISL 26Byte의 헤더와 FCS를 캡슐화하여 전송한다. ISL은 10M 이더넷 포트에서는 동작하지 않으며, 시스코 카탈리스트 2950 스위치에는 지원하지 않는다. [그림 20-4]는 Cisco ISL 헤더 내용을 보여주고 있다.

[그림 20-4] Cisco ISL 헤더 내용



- ① 프레임이 전송될 목적지 MAC 주소이다. 48Bit 중 40Bit 멀티캐스트 주소로 ISL 프레임 시작을 표기한다.
- ② 4Bit의 프레임 타입이다. 타입은 이더넷(0000), 토큰링(0001), FDDI(0010), ATM(0011)가 있다.
- ③ 이더넷 프레임의 우선순위 값이다.
- ④ 프레임을 전송하는 출발지 MAC 주소이다.
- ⑤ DA, Type, User, SA, LEN, FCS 필드를 제외한 길이이다.
- ⑥ IEEE 802.3 SNAP 필드이다.
- ⑦ 프레임의 VLAN-ID이며, 15Bit로 구성된다. 이때, 10bit만 사용되므로 VLAN 1024개만 지원한다.
- ⑧ 이 프레임이 BPDU이거나 CDP인 경우 1로 설정된다.
- ⑨ 프레임을 전송하는 스위치의 포트 번호로 16Bit로 구성된다.
- ⑩ 일반적인 이더넷은 0x0000 필드로 설정되고, 토큰링인 경우 AC, FC 필드값이 설정된다. 그리고 FDDI인 경우에는 FC 필드가 설정된다.
- ⑪ 액세스 링크상으로 송수신되는 원본 이더넷 프레임이다.
- ⑫ ISL 헤더와 Encapsulated 프레임에 대한 FCS 프레임이다.

스위치 포트를 ISL 트렁크 포트 구성하는 방법은 다음과 같다.

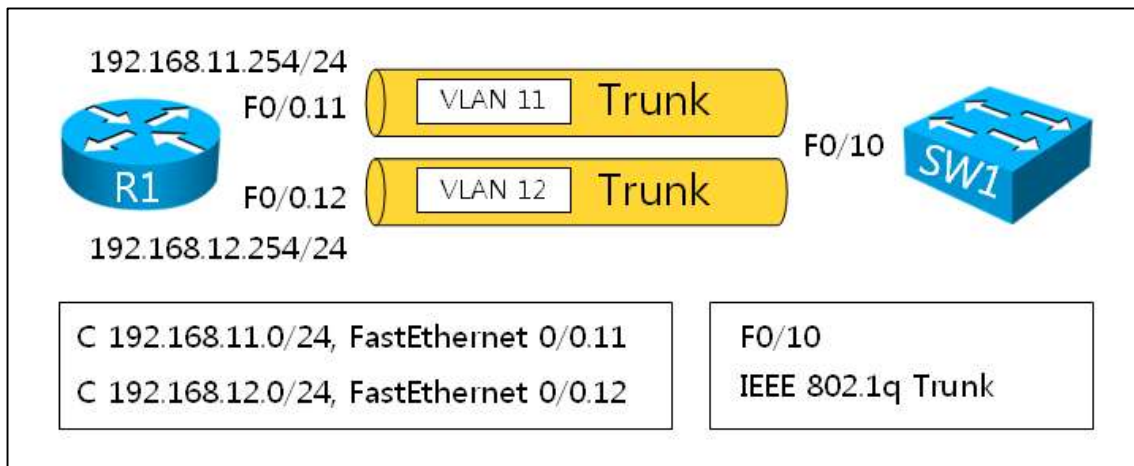
[예제 20-16] ISL 트렁크 포트 구성

```
SW1(config)#int fa0/24
SW1(config-if)#switchport trunk encapsulation isl
SW1(config-if)#switchport mode trunk
```

Inter-VLAN

서로 다른 VLAN 간에 유니캐스트 프레임을 전송하기 위해서 라우터를 이용한 VLAN 라우팅을 의미한다. 이때, 확장성과 물리적인 연결 문제를 해결하기 위해서 라우터와 스위치는 트렁크로 구성하며, 라우터는 서브-인터페이스를 이용하여 각각의 VLAN 도메인에 대한 게이트웨이를 수행하도록 한다. [그림 20-5]를 참조하여 Inter-VLAN 구성 방법을 알아보도록 하자.

[그림 20-5] Inter-VLAN 구성



SW1 F0/10를 트렁크 포트 구성하며, R1은 VLAN 도메인에 대한 게이트웨이를 수행하는 서브-인터페이스를 이용하여 IP 주소 설정과 VLAN-ID를 태깅할 수 있도록 트렁크 설정을 실시한다.

[예제 20-16] R1에서 Inter-VLAN 설정

```
R1(config)#int fa0/0
R1(config-if)#no shutdown
R1(config-if)#int fa0/0.11
R1(config-subif)#encapsulation dot1q 11
R1(config-subif)#ip address 192.168.11.254 255.255.255.0
R1(config-subif)#int fa0/0.12
R1(config-subif)#encapsulation dot1q 12
R1(config-subif)#ip address 192.168.12.254 255.255.255.0
```

R1에서 Inter-VLAN 구성이 완료되었다면, R1은 서브-인터페이스로 수신하는 프레임을 라우팅하여 해당 VLAN 도메인으로 프레임을 전송한다. 이때, IEEE 802.1q 트렁크 프로토콜을 이용하여 VLAN-ID를 태깅하여 전송한다. [예제 20-17]은 VLAN 도메인을 라우팅하기 위한 R1 라우팅 테이블 내용이다.

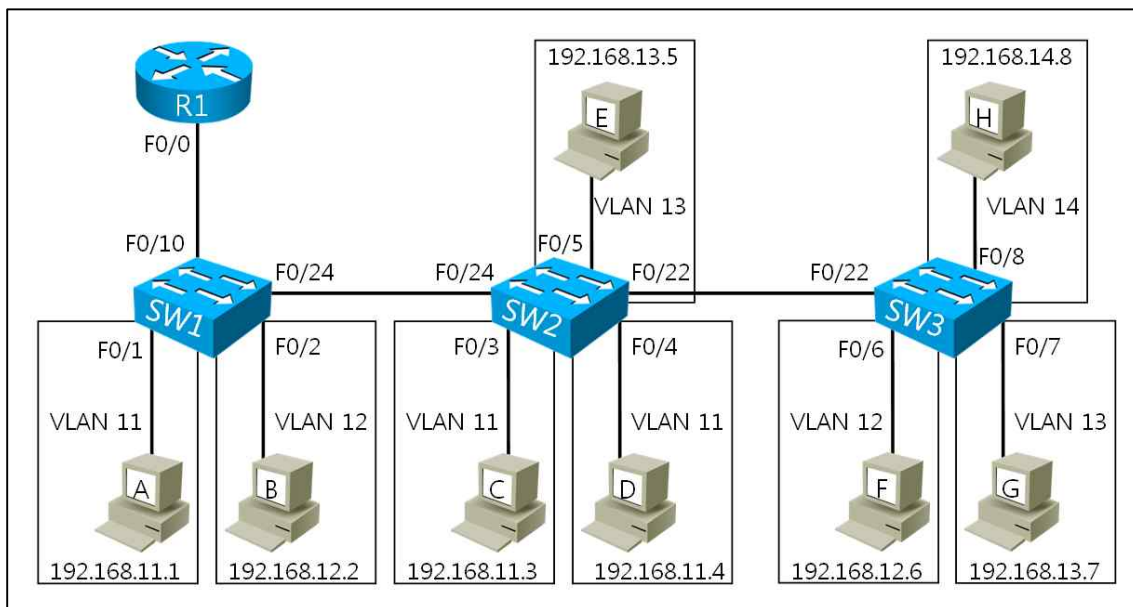
[예제 20-17] R1 라우팅 테이블 확인

```
R1#show ip route connected
C 192.168.11.0/24 is directly connected, FastEthernet0/0.11
C 192.168.12.0/24 is directly connected, FastEthernet0/0.12
```

VLAN 구성 예제

SW1을 VTP 서버로 설정하여, SW2와 SW3에 VLAN 11~14가 공유되도록 한 다음, [그림 20-6]을 참조하여 VLAN 구성을 실시하도록 하자. 또한, VLAN 구성이 완료되었다면, R1을 이용하여 VLAN 라우팅이 가능하도록 Inter-VLAN을 구성하도록 하자.

[그림 20-6] VLAN 실습 토폴로지



① 트렁크 설정

[예제 20-18] SW1, SW2, SW3에서 트렁크 설정

```
SW1(config)#int fa0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk

SW2(config)#int range fa0/22 , fa0/24
SW2(config-if-range)#switchport trunk encapsulation dot1q
SW2(config-if-range)#switchport mode trunk

SW3(config)#int fa0/22
SW3(config-if)#switchport trunk encapsulation dot1q
SW3(config-if)#switchport mode trunk
```

② VTP 관련 설정

[예제 20-19] SW1, SW2, SW3에서 VTP 관련 설정

```
SW1(config)#vtp domain CCNP
SW1(config)#vtp password cisco
SW1(config)#vtp mode server

SW2(config)#vtp domain CCNP
SW2(config)#vtp password cisco
SW2(config)#vtp mode client

SW3(config)#vtp domain CCNP
SW3(config)#vtp password cisco
SW3(config)#vtp mode client
```

③ VLAN 생성

[예제 20-20] SW1에서 VLAN 생성

```
SW1(config)#vlan 11
SW1(config-vlan)#name VLAN_A
SW1(config-vlan)#vlan 12
SW1(config-vlan)#name VLAN_B
SW1(config-vlan)#vlan 13
SW1(config-vlan)#name VLAN_C
SW1(config-vlan)#vlan 14
SW1(config-vlan)#name VLAN_D
```

④ 스위치 포트 매핑

[예제 20-21] 스위치 포트 액세스 설정 및 VLAN 매핑

```
SW1(config)#int fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 11
SW1(config-if)#
SW1(config-if)#int fa0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 12
SW1(config-if)#
```



```
SW2(config)#int range fa0/3 - 4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 11
SW2(config-if-range)#
SW2(config-if-range)#int fa0/5
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 13

SW3(config)#int fa0/6
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 12
SW3(config-if)#
SW3(config-if)#int fa0/7
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 13
SW3(config-if)#
SW3(config-if)#int fa0/8
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 14
```

⑤ VLAN 데이터베이스 정보 확인

[예제 20-22] SW1~SW3에서 확인한 VLAN 데이터베이스 내용

```
SW1#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, 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
                                Gig0/1, Gig0/2
11   VLAN_A                  active    Fa0/1
12   VLAN_B                  active    Fa0/2
13   VLAN_C                  active
14   VLAN_D                  active

SW2#show vlan brief
```


VLAN Name		Status	Ports

1	default	active	Fa0/1, Fa0/2, 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, Fa0/23, Gig0/1 Gig0/2
11	VLAN_A	active	Fa0/3, Fa0/4
12	VLAN_B	active	
13	VLAN_C	active	Fa0/5
14	VLAN_D	active	
SW3#show vlan brief			
VLAN Name		Status	Ports

1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, 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, Fa0/23, Fa0/24 Gig0/1, Gig0/2
11	VLAN_A	active	
12	VLAN_B	active	Fa0/6
13	VLAN_C	active	Fa0/7
14	VLAN_D	active	Fa0/8

⑥ VLAN 서브넷 할당

[표 20-1] VLAN 11, 12, 13, 14 서브넷 정보

VLAN 11		VLAN 12		VLAN 13		VLAN 14	
A	192.168.11.1	B	192.168.12.2	E	192.168.13.5	H	192.168.14.8
C	192.168.11.3	F	192.168.12.6	G	192.168.13.7		
D	192.168.11.4						
GW	192.168.11.254	GW	192.168.12.254	GW	192.168.13.254	GW	192.168.14.254

⑦ 동일한 VLAN 간에 Ping 테스트

[예제 20-23] 호스트 A(192.168.11.1)에서 호스트 C(192.168.11.3)로 Ping 테스트 내용

```
PC>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time=172ms TTL=128
Reply from 192.168.11.3: bytes=32 time=62ms TTL=128
Reply from 192.168.11.3: bytes=32 time=93ms TTL=128
Reply from 192.168.11.3: bytes=32 time=94ms TTL=128

Ping statistics for 192.168.11.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 62ms, Maximum = 172ms, Average = 105ms

PC>arp -a
```

Internet Address	Physical Address	Type
192.168.11.3	0002.16ac.3482	dynamic

[예제 20-24] 호스트 B(192.168.12.2)에서 호스트 F(192.168.12.6)로 Ping 테스트 내용

```
PC>ping 192.168.12.6

Pinging 192.168.12.6 with 32 bytes of data:

Reply from 192.168.12.6: bytes=32 time=234ms TTL=128
Reply from 192.168.12.6: bytes=32 time=94ms TTL=128
Reply from 192.168.12.6: bytes=32 time=109ms TTL=128
Reply from 192.168.12.6: bytes=32 time=125ms TTL=128

Ping statistics for 192.168.12.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 94ms, Maximum = 234ms, Average = 140ms

PC>
PC>arp -a
```

Internet Address	Physical Address	Type
192.168.12.6	000c.cf24.ee4b	dynamic

⑧ 서로 다른 VLAN 간에 Ping 테스트

[예제 20-25] 호스트 A(192.168.11.1)에서 호스트 F(192.168.12.6)로 Ping 테스트 내용

```
PC>ping 192.168.12.6

Pinging 192.168.12.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.12.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

⑨ Inter-VLAN을 구성하기 위한 SW1에서 트렁크 설정

[예제 20-26] SW1에서 트렁크 설정

```
SW1(config)#int fa0/10
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 11,12,13,14
```

⑩ Inter-VLAN을 구성하기 위한 R1에서 VLAN 라우팅 설정

[예제 20-27] R1에서 VLAN 라우팅 설정

```
R1(config)#int fa0/0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#int fa0/0.1
R1(config-subif)#encapsulation dot1q 11
R1(config-subif)#ip address 192.168.11.254 255.255.255.0
R1(config-subif)#int fa0/0.2
R1(config-subif)#encapsulation dot1q 12
R1(config-subif)#ip address 192.168.12.254 255.255.255.0
R1(config-subif)#int fa0/0.3
R1(config-subif)#encapsulation dot1q 13
R1(config-subif)#ip address 192.168.13.254 255.255.255.0
```

```
R1(config-subif)#int fa0/0.4
R1(config-subif)#encapsulation dot1q 14
R1(config-subif)#ip address 192.168.14.254 255.255.255.0
```

⑪ R1 라우팅 테이블 확인

[예제 20-28] R1에서 확인한 라우팅 테이블 내용

```
R1#show ip route connected
C    192.168.11.0/24 is directly connected, FastEthernet0/0.1
C    192.168.12.0/24 is directly connected, FastEthernet0/0.2
C    192.168.13.0/24 is directly connected, FastEthernet0/0.3
C    192.168.14.0/24 is directly connected, FastEthernet0/0.4
```

⑫ SW1 F0/10 트렁크 포트 확인

[예제 20-29] SW1에서 확인한 F0/10 트렁크 포트 내용

```
SW1#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/10    on        802.1q         trunking      1
Fa0/24    on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/10    11-14
Fa0/24    1-1005

Port      Vlans allowed and active in management domain
Fa0/10    11,12,13,14
Fa0/24    1,11,12,13,14

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/10    11,12,13,14
Fa0/24    1,11,12,13,14
```

⑬ 서로 다른 VLAN 간에 Ping 테스트

[예제 20-30] 호스트 A(192.168.11.1)에서 호스트 H(192.168.14.8)로 Ping 테스트 내용

```
PC>ping 192.168.14.8

Pinging 192.168.14.8 with 32 bytes of data:

Request timed out.
Reply from 192.168.14.8: bytes=32 time=187ms TTL=127
Reply from 192.168.14.8: bytes=32 time=128ms TTL=127
Reply from 192.168.14.8: bytes=32 time=172ms TTL=127

Ping statistics for 192.168.14.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 128ms, Maximum = 187ms, Average = 162ms
```

⑭ Inter-VLAN 경로 확인

[예제 20-31] 호스트 A(192.168.11.1)에서 호스트 H(192.168.14.8)에 대한 Inter-VLAN 경로 내용

```
PC>tracert 192.168.14.8

Tracing route to 192.168.14.8 over a maximum of 30 hops:

  1  38 ms    47 ms    63 ms    192.168.11.254
  2  156 ms   187 ms   172 ms    192.168.14.8

Trace complete.
```

정보 확인이 완료되었다면, 다음 내용을 알아보기 위해서 SW1 F0/10 인터페이스를 'shutdown' 하도록 하자.

[예제 20-32] SW1에서 F0/10 'shutdown' 실시

```
SW1(config)#int fa0/10
SW1(config-if)#shutdown
```

L3 스위치를 이용한 VLAN 라우팅

L3 스위치는 라우팅 기능이 보장되며, VLAN 개수만큼 Management VLAN 인터페이스를 사용할 수 있기 때문에 각각의 VLAN 도메인에 대한 게이트웨이 수행이 가능하다. 그럼 SW1에서 L3 스위치를 이용한 VLAN 라우팅을 설정하도록 하자. (참고 : L3 스위치는 Cisco 카탈리스트 스위치 중에는 3550, 3560, 3750 시리즈가 있다.)

[예제 20-33] SW1에서 VLAN 라우팅 설정

```
SW1(config)#ip routing
SW1(config)#
SW1(config)#int vlan 11
SW1(config-if)#ip address 192.168.11.254 255.255.255.0
SW1(config-if)#int vlan 12
SW1(config-if)#ip address 192.168.12.254 255.255.255.0
SW1(config-if)#int vlan 13
SW1(config-if)#ip address 192.168.13.254 255.255.255.0
SW1(config-if)#int vlan 14
SW1(config-if)#ip address 192.168.14.254 255.255.255.0
```

설정이 완료되었다면, SW1에서 라우팅 테이블을 확인하도록 하자.

[예제 20-34] SW1에서 확인한 라우팅 테이블

```
SW1#show ip route connected
C    192.168.11.0/24   is directly connected, Vlan11
C    192.168.12.0/24   is directly connected, Vlan12
C    192.168.13.0/24   is directly connected, Vlan13
C    192.168.14.0/24   is directly connected, Vlan14
```

정보 확인 결과, 라우터에서 사용하는 라우팅 테이블이 SW1에서도 사용되는 것을 알 수 있다. 그럼 호스트 A(192.168.11.1)에서 호스트 H(192.168.14.8)로 Ping이 가능한지 확인하도록 하자.

[예제 20-35] 호스트 A(192.168.11.1)에서 호스트 H(192.168.14.8)로 Ping 테스트 내용

```
PC>ping 192.168.14.8

Pinging 192.168.14.8 with 32 bytes of data:

Reply from 192.168.14.8: bytes=32 time=93ms TTL=127
Reply from 192.168.14.8: bytes=32 time=94ms TTL=127
Reply from 192.168.14.8: bytes=32 time=111ms TTL=127
Reply from 192.168.14.8: bytes=32 time=125ms TTL=127

Ping statistics for 192.168.14.8:
```

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 93ms, Maximum = 125ms, Average = 105ms

Ping 테스트 결과, VLAN 11에 속해있는 호스트 A에서 VLAN 14에 속해있는 호스트 H로 Ping이 되는 것을 알 수 있다. 그럼 호스트 A(192.168.11.1)에서 호스트 H(192.168.14.8)로 데이터가 전송될 때, VLAN 라우팅 경로를 확인하도록 하자.

[예제 20-36] 호스트 A(192.168.11.1)에서 호스트 H(192.168.14.8)에 대한 VLAN 라우팅 경로 내용

```
PC>tracert 192.168.14.8

Tracing route to 192.168.14.8 over a maximum of 30 hops:

  1  31 ms    16 ms    32 ms    192.168.11.254
  2  125 ms   94 ms   125 ms   192.168.14.8

Trace complete.
```

이처럼 Inter-VLAN를 구성할 경우, L3 스위치가 존재한다면 라우터 없이 바로 스위치에서 VLAN 라우팅을 구성할 수 있다.

(빈 페이지입니다.)