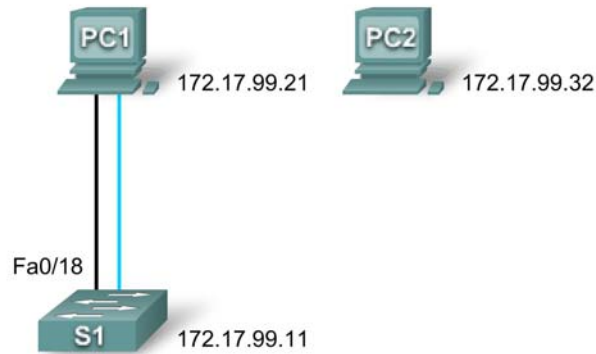


실습 2.5.1: 기본적인 스위치 설정

토폴로지



주소 테이블

장치	인터페이스	IP 주소	서브넷 마스크	디폴트 게이트웨이
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.1
PC2	NIC	172.17.99.32	255.255.255.0	172.17.99.1
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

학습 목표

이 실습을 마치면, 다음과 같은 것들이 가능하다.

- 토폴로지 다이어그램에 따라 네트워크 케이블링
- 스위치에 있는 기존 설정의 제거
- 기본 설정의 조사와 확인
- 이름과 IP 주소를 포함한 기본적인 스위치 설정의 생성
- CLI에 안전하게 액세스 하기 위해 패스워드를 설정
- 스위치의 포트 속도와 인터페이스에 대한 듀플렉스 속성을 설정
- 기본적인 스위치 포트 보안 설정
- MAC 주소 테이블 관리
- 정적 MAC 주소 할당
- 스위치에 호스트 추가 및 이동

시나리오

이 실습에서는 독립형 LAN 스위치를 설정하고 이를 살펴본다. 스위치가 정해진 상황에 대한 기본적인 기능을 수행하기는 하지만, 네트워크 관리자는 안전하고 최적화된 LAN을 보장하기 위해 다수의 파라미터들을 수정해야 한다. 이 실습은 스위치 설정의 기본을 설명하고 있다.

작업 1: 스위치의 케이블링, 삭제, 리로드

단계 1: 네트워크 케이블링.

토폴로지 다이어그램과 유사하게 네트워크 케이블링을 수행한다. 스위치로의 콘솔 연결을 생성한다. 필요한 경우, 콘솔 연결을 생성하는 방법에 대해서는 실습 1.3.1을 참조한다.

토폴로지에 도시한 바와 같은 필요 인터페이스를 가지고 있다면, 이 실습을 수행할 때 어떠한 스위치를 사용해도 상관없다. 이 실습에 나타나는 **결과 값**들은 2960 스위치를 기반으로 하고 있다. 다른 스위치를 사용할 경우, 인터페이스 설명과 스위치의 결과 값들이 다르게 나타날 수 있다.

노트: 처음에 PC2는 스위치에 연결되어 있지 않다. 이는 작업 5에서만 유일하게 사용된다.

단계 2: 스위치의 설정을 제거한다.

부록 1의 절차에 따라 스위치의 설정을 제거한다.

작업 2: 기본 스위치 설정 확인

단계 1: Privileged mode에 진입한다.

Privileged mode에서는 모든 스위치 명령어를 사용할 수 있다. 그러나, 많은 수의 특권 명령어들이 운영 파라미터들을 설정할 수 있기 때문에, privilege mode에 대한 액세스는 비인가된 사용을 방지하기 위해 패스워드로 보호되어야 한다. 패스워드 설정에 대한 내용은 작업 3에서 다룬다.

Privileged EXEC 명령어 집합은 다른 명령 모드로 진입해 액세스 할 수 있는 **configure** 명령어 뿐 아니라 user EXEC 모드와 관련된 명령어들도 포함하고 있다. **enable** 명령어를 입력하여 privileged EXEC 모드에 진입한다.

```
Switch>enable  
Switch#
```

설정 중에 Privileged EXEC 모드를 나타내기 위해 프롬프트가 변경된다는 것에 주의해야 한다.

단계 2: 현재 스위치의 설정 조사

현재의 running configuration 파일을 조사한다.

```
Switch#show running-config
```

스위치가 가지고 있는 패스트이더넷 인터페이스는 몇 개인가? _____

스위치가 가지고 있는 기가비트 이더넷 인터페이스는 몇 개인가? _____

vtv 라인에 대해 나타나는 값의 범위는 얼마인가? _____

NVRAM의 현재 내용을 조사한다.

```
Switch#show startup-config
startup-config is not present
```

스위치가 이러한 결과를 나타내는 이유는 무엇인가?

가상 인터페이스 VLAN1의 특성을 조사한다.

```
Switch#show interface vlan1
```

스위치에 IP 주소가 설정되어 있는가? _____

가상 스위치 인터페이스의 MAC 주소는 무엇인가? _____

해당 인터페이스가 활성화 되어 있는가? _____

이제 해당 인터페이스의 IP 특성을 살펴보자.

```
Switch#show ip interface vlan1
```

어떠한 결과가 나타나는가? _____

단계 3: 시스코 IOS 정보의 표시

스위치가 보고하는 버전 정보를 조사한다.

```
Switch#show version
```

구동 중인 시스코 IOS 버전은 무엇인가? _____

시스템 이미지의 파일이름은 무엇인가? _____

스위치의 베이스 MAC 주소는 무엇인가? _____

단계 4: 패스트이더넷 인터페이스를 조사한다.

PC10이 사용하는 패스트이더넷 인터페이스의 기본 속성을 조사한다.

```
Switch#show interface fastethernet 0/18
```

인터페이스는 업 상태인가 다운 상태인가? _____

인터페이스를 업 상태로 만드는 이벤트는 무엇인가? _____

인터페이스의 MAC 주소는 무엇인가? _____

인터페이스의 속도와 듀플렉스 설정은 무엇인가? _____

단계 5: VLAN 정보 조사

스위치의 기본 VLAN 세팅을 조사한다.

```
Switch#show vlan
```

VLAN 1의 이름은 무엇인가? _____

이 VLAN의 포트는 어떤 것인가? _____

VLAN 1은 활성화 상태인가? _____

VLAN의 타입 중 디폴트 VLAN은 무엇인가? _____

단계 6 플래시 메모리를 조사한다.

플래시 디렉토리의 내용을 조사하기 위해 다음의 명령어 중 하나를 수행한다.

```
Switch#dir flash:
```

혹은

```
Switch#show flash
```

어떤 파일 혹은 디렉토리를 볼 수 있는가?

디렉토리는 파일 확장자를 갖지 않는다. 디렉토리 내의 파일들을 살펴보기 위해 출력결과에 파일이름이 화면에 표시될 수 있도록 다음과 같은 명령어를 수행한다.

```
Switch#dir flash:c2960-lanbase-mz.122-25.SEE3
```

출력결과가 이와 유사해야 한다.

```
Directory of flash:/c2960-lanbase-mz.122-25.SEE3/
 6  drwx      4480   Mar 1 1993 00:04:42 +00:00  html
618 -rwx     4671175   Mar 1 1993 00:06:06 +00:00  c2960-lanbase-mz.122-
25.SEE3.bin
619 -rwx        457   Mar 1 1993 00:06:06 +00:00  info
32514048 bytes total (24804864 bytes free)
```

시스코 IOS 이미지 파일의 이름은 무엇인가? _____

단계 7: startup configuration 파일을 조사한다.

startup configuration 파일의 내용을 살펴보기 위해, **show startup-config** 명령어를 privileged EXEC 모드에서 수행한다.

```
Switch#show startup-config
startup-config is not present
```

이러한 메시지가 나타나는 이유가 무엇인가?

스위치에서 하나의 설정을 변경한 후 이를 저장한다. 다음과 같은 명령어를 입력한다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname S1
S1(config)#exit
S1#
```

running configurationnon의 내용을 NVRAM (non-volatile RAM)에 저장하기 위해 **copy running-config startup-config**명령을 수행한다.

```
Switch#copy running-config startup-config
Destination filename [startup-config]? (enter).
Building configuration...
[OK]
```

노트: 이 명령어에 대한 입력을 좀 더 쉽게 하기 위해 **copy run start**로 축약하여 사용할 수 있다.

이제 **show startup-config** 명령을 사용하여 NVRAM의 내용을 화면에 표시한다.

```
S1#show startup-config
Using 1170 out of 65536 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
<output omitted>
```

현재의 설정을 NVRAM에 저장한다.

작업 3: 기본적인 스위치 설정 생성

단계 1: 스위치에 이름을 할당한다.

이전 작업의 마지막 단계에서는 호스트이름이 설정되어 있었다. 여기에서는 이러한 명령어가 사용되었던 방법에 대해 다시 살펴본다.

```
S1#configure terminal
S1(config)#hostname S1
S1(config)#exit
```

단계 2: 액세스 패스워드의 설정

콘솔에서 config-line 모드로 진입한다. 로그인 패스워드는 **cisco**로 설정한다. vty 라인 0 ~ 15까지의 패스워드도 **cisco**로 설정한다.

```
S1#configure terminal
```

각 라인 당 하나씩 설정 명령어를 입력한다. 입력을 끝났을 경우, global configuration 모드로 되돌아 가기 위해 **exit** 명령을 입력하거나 Ctrl-Z를 누른다.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

login 명령어가 필요한 이유는 무엇인가? _____

단계 3. 명령어 모드 패스워드를 설정한다.

enable secret 패스워드를 class로 설정한다. 이 패스워드는 privileged EXEC 모드에 대한 액세스를 보호한다.

```
S1(config)#enable secret class
```

단계 4. 스위치에 3계층 주소를 설정한다.

PC1에서 원격으로 S1을 관리하기 전에, 스위치에 IP 주소를 할당해야 한다. 스위치의 기본 설정은 VLAN 1을 통해 스위치를 제어할 수 있도록 되어 있다. 그러나 기본적인 스위치 설정의 가장 좋은 방법은 VLAN 1이 아닌 다른 VLAN으로 매니지먼트 VLAN을 변경하는 것이다. 이렇게 변경하는 이유는 다음 챕터에서 설명한다.

앞으로 VLAN 99가 관리를 위한 목적으로 사용될 것이다. VLAN 99는 임의로 선택된 것이기 때문에, 항상 VLAN 99가 사용되어야 한다는 것을 의미하지 않는다.

먼저, 스위치에 VLAN 99를 새롭게 생성한다. 이 후, 스위치의 내부 가상 인터페이스인 VLAN 99에 172.17.99.11의 IP 주소와 255.255.255.0의 서브넷 마스크를 세팅한다.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state
to down
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#
```

no shutdown 명령어를 입력했다고 하더라도 VLAN 99 인터페이스가 다운 상태라는 것에 주의해야 한다. VLAN 99에 할당된 스위치 포트가 없기 때문에 해당 인터페이스는 현재 다운 상태이다.

모든 사용자 포트를 VLAN 99에 할당한다.

```
S1(config)#interface range fa0/1 - 24
S1(config-if-range)#switchport access vlan 99
S1(config-if-range)#exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
```

VLAN에 대한 전체적인 내용은 이 실습의 범위를 벗어난다. 이 주제에 대한 좀 더 상세한 내용은 다음 챕터에서 다룬다. 그러나 호스트와 스위치 간의 연결성 확립을 위해, 호스트에서 사용되는 포트는 반드시 스위치와 동일한 VLAN 내에 있어야 한다. VLAN 1에 대한 상기의 출력결과에서는 VLAN 1에 할당된 포트가 없기 때문에 다운 상태라는 것에 주의해야 한다. 일정 시간이 흐른 후, 적어도 하나의 포트가 VLAN 99에 할당되었기 때문에 VLAN 99는 업 상태가 된다.

단계 5: 스위치의 기본 게이트웨이 설정

S1은 2계층 스위치이기 때문에, 2계층 헤더를 기반으로 포워딩을 결정한다. 스위치에 다수의 네트워크가 연결되어 있는 경우, 경로가 3계층에서 결정되기 때문에 스위치가 인터네트워킹 프레임들을 어떻게 포워딩 할 것인지에 대해 지정해야 한다. 이는 라우터 혹은 3계층 스위치를 가리키는 기본 게이트웨이 주소를 지정함으로써 간단히 해결된다. 이 실습에서는 외부의 IP 게이트웨이에 대한 내용은 포함하고 있지 않지만, 결과적으로는 외부 액세스를 위해 LAN을 라우터에 연결해야 한다는 것을 알 수 있을 것이다. 라우터의 LAN 인터페이스가 172.17.99.1이라고 가정하고, 스위치의 기본 게이트웨이로 설정한다.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

단계 6: 매니지먼트 LAN 세팅을 확인한다.

VLAN 99의 인터페이스 세팅을 확인한다.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.5302.4ec1 (bia 001b.5302.4ec1)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:03:23, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    4 packets input, 1368 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

이 인터페이스의 대역폭은 얼마인가? _____

VLAN 상태는 무엇인가? VLAN99는 _____ 이다. 라인 프로토콜은 _____ 이다.

큐잉 전략은 무엇인가? _____

단계 7: PC1에 대한 IP 주소와 기본 게이트웨이를 설정한다.

PC1의 IP 주소는 172.17.99.21, 서브넷 마스크는 255.255.255.0로 설정한다. 기본 게이트웨이는 172.17.99.1로 설정한다. (필요한 경우, 실습 1.3.1을 참조하여 PC의 NIC를 설정한다.)

단계 8: 연결성을 검사한다.

호스트와 스위치가 올바르게 설정되었는지 확인하기 위해, PC1에서 스위치의 IP 주소(172.17.99.11)로 ping을 수행한다.

핑이 성공적이었는가? _____

그렇지 않은 경우, 스위치와 호스트 설정에 대한 트러블슈팅을 수행한다. 다수의 시도를 수행해야만 pings에 성공 할 수 있다.

단계 9: 패스트이더넷 인터페이스의 포트 속도와 듀플렉스 세팅을 설정한다.

패스트이더넷 0/18 에서 듀플렉스 와 속도를 세팅한다. 작업이 끝난 후 end 명령을 사용하여 privileged EXEC 모드로 돌아간다.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

패스트이더넷 0/18 인터페이스와 VLAN 99 인터페이스 모두에서 라인 프로토콜이 일시적으로 다운 상태가 될 것이다.

스위치의 이더넷 인터페이스는 기본적으로 자동-감지 (auto-sensing) 기능을 가지고 있기 때문에, 자동적으로 최적화된 세팅값을 협상한다. 확실한 속도와 듀플렉스 모드로 작동하기 위해서는 수동으로 설정해야 한다. 수동으로 설정된 포트는 듀플렉스의 불일치를 야기할 수 있으며, 이는 심각한 성능 저하를 일으킬 수 있다.

패스트이더넷 인터페이스의 새로운 듀플렉스와 속도 세팅을 확인한다.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is FastEthernet, address is 001b.5302.4e92 (bia 001b.5302.4e92)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
```

```

ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:01, output hang never
All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights
reserved. This document is Cisco Public Information. Page 7 of 15 CCNA
Exploration LAN Switching and Wireless: Basic Switch Concepts and
Configuration Lab 2.5.1: Basic Switch Configuration
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  265 packets input, 52078 bytes, 0 no buffer
    Received 265 broadcasts (0 multicast)
      0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 32 multicast, 0 pause input
    0 input packets with dribble condition detected
  4109 packets output, 342112 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out

```

단계 10: 설정을 저장한다.

이제 스위치의 기본적인 설정이 완료되었다. 시스템이 리부팅되거나 전원이 공급되지 않을 경우에 변경된 설정 값들을 잃지 않기 위해 running configuration 파일을 NVRAM으로 백업한다.

```

S1#copy running-config startup-config
Destination filename [startup-config]?[Enter] Building configuration...
[OK]
S1#

```

단계 11: startup configuration 파일을 조사한다.

NVRAM에 저장된 설정을 보기 위해서는 privileged EXEC 모드에서 show startup-config 명령어를 사용해야 한다.

```
S1#show startup-config
```

입력했던 모든 변경사항들이 해당 파일 내에 기록되어 있는가? _____

작업 4: MAC 주소 테이블의 관리

단계 1: 호스트의 MAC 주소를 기록한다.

다음과 같은 명령을 사용하여 PC 네트워크 인터페이스 카드의 2계층 (물리적) 주소를 기록하고 확인한다.

Start > Run > cmd > ipconfig /all

PC1: _____

PC2: _____

단계 2: 스위치가 학습한 MAC 주소를 확인한다.

MAC 주소를 화면에 표시하기 위해 `show mac-address-table` 명령어를 privileged EXEC 모드에서 수행한다.

```
S1#show mac-address-table
```

존재하는 동적 주소는 몇 개인가? _____

존재하는 전체 MAC 주소는 몇 개인가? _____

동적 MAC 주소가 PC1의 MAC 주소와 일치하는가? _____

단계 3: `show mac-address-table` 옵션을 나타낸다.

```
S1#show mac-address-table
```

얼마나 많은 수의 옵션이 `show mac-address-table` 명령어에서 사용가능한가? _____

동적으로 학습된 테이블에서 MAC 주소만을 나타낸다.

```
S1#show mac-address-table address dynamic
```

존재하는 동적 주소는 몇 개인가? _____

PC1에 대한 MAC 주소 엔트리를 살펴본다.

```
S1#show mac-address-table address <PC1 MAC here>
```

단계 4: MAC 주소 테이블을 제거한다.

존재하는 MAC 주소를 제거하기 위해 `clear mac-address-table` 명령을 privileged EXEC 모드에서 수행한다.

```
S1#clear mac-address-table dynamic
```

단계 5: 결과 확인

MAC 주소 테이블이 정리되었는지 확인한다.

```
S1#show mac-address-table
```

존재하는 정적 MAC 주소는 몇 개인가? _____

존재하는 동적 주소는 몇 개인가? _____

단계 6: MAC 주소 테이블을 다시 조사한다.

PC1에서 구동 중인 애플리케이션은 이미 S1으로 프레임을 송신하였다. S1이 PC1에 대한 MAC 주소를 학습했는지 살펴보기 위해 privileged EXEC 모드에서 MAC 주소 테이블을 다시한번 관찰한다.

```
S1#show mac-address-table
```

존재하는 동적 주소는 몇 개인가? _____

마지막으로 화면에 표시된 것에서 이와 같이 변경된 이유는 무엇인가?

S1이 아직 PC1에 대한 MAC 주소를 재학습하지 못했을 경우, PC1에서 스위치의 VLAN 99 IP 주소로 ping을 수행한 후 단계 6을 반복한다.

단계 7: 정적 MAC 주소를 셋업한다.

호스트가 어떤 포트에 연결하는지 지정하기 위한 하나의 옵션은 포트에 대한 호스트 MAC 주소의 정적 매핑을 생성하는 것이다.

이 작업의 단계 1에 있는 PC1에 대한 주소를 사용하여 패스트이더넷 인터페이스 0/18의 정적 MAC 주소를 셋업한다. MAC 주소인 **00e0.2917.1884**는 단지 하나의 예일 뿐이다. 여기에 주어진 예제에 있는 것과는 다른, PC1의 MAC 주소를 반드시 사용해야 한다.

```
S1(config)#mac-address-table static 00e0.2917.1884 vlan 99 interface  
fastethernet 0/18
```

단계 8: 결과를 확인한다.

MAC 주소 테이블의 엔트리를 확인한다.

```
S1#show mac-address-table
```

존재하는 전체 MAC 주소는 몇 개인가? _____

존재하는 정적 주소는 몇 개인가? _____

단계 9: MAC 주소 테이블의 엔트리를 확인한다.

다음 작업을 완료하기 위해서는 정적 MAC 주소 테이블 엔트리의 제거가 필요하다. 설정 모드로 진입하여 no를 명령어 문자열의 앞에 입력하여 해당 명령을 제거한다.

노트: MAC 주소인 00e0.2917.1884는 하나의 예일 뿐이다. PC1의 MAC 주소를 사용해야 한다.

```
S1(config)#no mac-address-table static 00e0.2917.1884 vlan 99 interface  
fastethernet 0/18
```

단계 10: 결과 확인

정적 MAC 주소가 제거되었는지 확인한다.

```
S1#show mac-address-table
```

존재하는 전체 정적 MAC 주소는 몇 개인가? _____

작업 5: 포트 보안 설정

단계 1: 두 번째 호스트를 설정한다.

이 작업을 수행하기 위해서는 두 번째 호스트가 필요하다. PC2의 IP 주소를 172.17.99.22 (서브넷 마스크: 255.255.255.0)로 설정하고, 기본 게이트웨이는 172.17.99.1로 설정한다. 이 PC는 아직까지 스위치에 연결하면 안된다.

단계 2: 연결성을 확인한다.

호스트에서 스위치의 VLAN 99 IP 주소로 ping 테스트를 수행하여 PC1과 스위치가 여전히 올바르게 설정되어 있는지 확인한다.

Ping이 성공적으로 수행되었는가? _____

이에 대한 답이 아니오라면, 호스트와 스위치 설정에 대한 트러블슈팅을 수행한다.

단계 3: 호스트의 MAC 주소를 복사한다.

작업4, 단계1에서의 MAC 주소를 기록한다.

PC1_____

단계 3: 연결을 확인한다.

단계 4: 스위치가 학습한 MAC 주소를 확인한다.

Privileged EXEC 모드에서 **show mac-address-table** 명령어를 사용하여 학습된 MAC 주소들을 화면에 표시한다.

```
S1#show mac-address-table
```

존재하는 동적 주소는 몇 개인가? 단계 4: MAC 주소 테이블을 제거하라.

해당 MAC 주소 엔트리와 PC1의 MAC 주소가 일치하는가? _____

단계 5: 포트 보안 옵션 목록을 살펴본다.

인터페이스 패스트이더넷 0/18의 포트 보안을 세팅하기 위한 옵션들을 살펴보자.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security violation mode
<cr>
S1(config-if)#switchport port-security
```

단계 6: 액세스 포트에 대한 포트 보안을 설정한다.

위반 사항이 발생했을 경우 유효하지 않은 호스트들의 트래픽의 블로킹, 디바이스들에 대한 동적인 MAC 주소 학습, 오직 2개의 디바이스만 접속할 수 있도록 하기 위해 스위치의 패스트이더넷 0/18 포트를 설정한다.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation protect
S1(config-if)#end
```

단계 7: 결과 확인

포트 보안 세팅을 나타낸다.

```
S1#show port-security
```

패스트이더넷 0/18에서 허용되는 안전한 주소는 몇 개나 되는가? _____

이 포트에 대한 보안 기능은 무엇인가? _____

단계 8: running configuration을 조사한다.

```
S1#show running-config
```

running configuration의 보안 적용을 직접적으로 반영하고 있는 문장이 목록에 존재하는가?

단계 9: 포트에서 포트 보안 세팅을 수정한다.

패스트이더넷 0/18 인터페이스에서 위반사항이 발생했을 경우 셧 다운 시키기 위해 포트 보안의 최대 MAC 주소 개수를 1로 변경한다.

```
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security violation shutdown
```

단계 10: 결과 확인

포트 보안 세팅을 나타낸다.

```
S1#show port-security
```

포트 보안 세팅에 단계 9에서 변경한 사항들이 반영되어 있는가? _____

연결성을 확인하고 MAC 주소 테이블을 갱신하기 위해 PC1에서 스위치의 VLAN 99 주소로 ping 테스트를 수행한다. PC1에 대한 MAC 주소가 running configuration에 "stuck" 되었음을 볼 수 있을 것이다.

```
S1#show run
Building configuration...
<output omitted>
!
interface FastEthernet0/18
switchport access vlan 99
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 00e0.2917.1884
speed 100
duplex full
!
<output omitted>
```

단계 11: 로우그 (rogue) 호스트 소개

PC1에 대한 연결을 해제하고 PC2를 패스트이더넷 0/18 포트에 연결한다. 새로운 호스트에서 VLAN 99의 주소인 172.17.99.11로 ping을 수행한다. 주황색 링크 상태 표시등이 녹색으로 변경될때까지 기다린다. 녹색으로 변경된 뒤와 거의 동시에 꺼져야 한다.

관찰 결과 기록: _____

단계 12: 포트 설정 정보를 나타낸다.

패스트이더넷 포트 0/18에 대한 설정 정보를 보기 위해, privileged EXEC 모드에서 다음과 같은 명령어를 실행한다.

```
S1#show interface fastethernet 0/18
```

이 인터페이스의 상태는 무엇인가?

패스트이더넷0/18은 _____ 이다. 라인 프로토콜은 _____ 이다.

단계 13: 포트를 재활성화 시킨다.

보안 위반사항이 발생하여 포트가 셧 다운 되었을 경우, **no shutdown** 명령을 통해 이를 다시 재활성화 시킨다. 그러나, 로우그(rogue) 호스트가 패스트이더넷 0/18에 부착되어 있는 한, 해당 호스트로부터의 어떤 트래픽도 해당 포트를 비활성화 시킨다. PC1을 패스트이더넷 0/18에 재연결하고, 스위치에서 다음과 같은 명령어들을 입력한다.

```
S1#configure terminal
```

```
S1(config)#interface fastethernet 0/18
```

```
S1(config-if)#no shutdown
```

```
S1(config-if)#exit
```

노트: 일부 IOS 버전에서는 **no shutdown** 명령어를 입력하기 전에 **shutdown** 명령어를 수동으로 입력해야 할 수도 있다.

단계 14: 정리

다른 지시사항이 없는 한, 해당 스위치의 설정을 제거하고, 호스트 컴퓨터와 스위치의 전원을 끄고, 케이블을 분리하여 잘 보관하도록 한다.

부록 1

스위치의 삭제 및 리로딩

Exploration 3 과정의 대부분의 실습은 설정되지 않은 스위치를 가지고 시작한다. 설정이 되어있는 스위치의 사용은 예기치 않은 결과를 만들 수도 있다. 이러한 지침들은 실습을 시작하기 전에 스위치를 어떻게 준비해야 하는지를 알려준다. 이러한 지침들은 2960 스위치에 대한 것이다. 그러나, 2900과 2950 스위치에 대한 절차도 이와 동일하다.

단계 1: enable 명령어를 입력하여 privileged EXEC 모드로 진입한다.

패스워드에 대한 프롬프트가 나타나는 경우, class를 입력한다. 패스워드를 정확히 입력했음에도 불구하고 제대로 동작하지 않는 경우, 감사에게 도움을 요청한다.

```
Switch>enable
```

단계 2: VLAN 데이터베이스 정보 파일을 삭제한다.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] <ENTER>
```

VLAN 파일이 없는 경우, 이러한 메시지가 화면에 표시된다.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

단계 3: NVRAM에서 스위치의 startup configuration 파일을 제거한다.

```
Switch#erase startup-config
```

이에 대한 라인 프롬프트는 다음과 같을 것이다:

```
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
Press Enter to confirm.
```

응답은 다음과 같아야 한다:

```
Erase of nvram: complete
```

단계 4: VLAN 정보가 삭제되었는지 체크한다.

VLAN 정보가 단계 2에서 삭제되었는지 확인하기 위해 **show vlan** 명령을 수행한다.

VLAN 정보가 단계 2에서 성공적으로 삭제되었을 경우, 단계 5로 가서 **reload** 명령을 수행하여 스위치를 재시작 시킨다.

이전의 VLAN 정보가 여전히 존재하는 경우 (기본 매니지먼트 VLAN 1 이외의 것), **reload** 명령어를 수행하지 말고 전원을 차단했다가 다시 공급한다 (하드웨어 재시작). 스위치의 전원을 차단했다가 다시 공급하려면 스위치의 뒷면에 있는 전원 코드를 뽑다가 다시 끼운다.

단계 5: 소프트웨어를 재시작한다.

노트: 스위치가 하드웨어 재시작 방법을 통해 재시작되었을 경우, 이 단계는 필요하지 않다.

privileged EXEC 모드 프롬프트에서 **reload** 명령어를 입력한다.

```
Switch(config)#reload
```

이에 대한 라인 프롬프트는 다음과 같을 것이다.

```
System configuration has been modified. Save? [yes/no]:
```

다음과 같이 **n**을 입력하고 **Enter**키를 누른다.

이에 대한 라인 프롬프트는 다음과 같을 것이다.

```
Proceed with reload? [confirm] [ENTER]
```

응답의 첫번째 라인은 다음과 같을 것이다.

```
Reload requested by console.
```

스위치가 리로드된 후, 라인 프롬프트는 다음과 같을 것이다.

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

다음과 같이 **n**을 입력하고 **Enter**키를 누른다.

이에 대한 라인 프롬프트는 다음과 같을 것이다:

```
Press RETURN to get started! [ENTER]
```