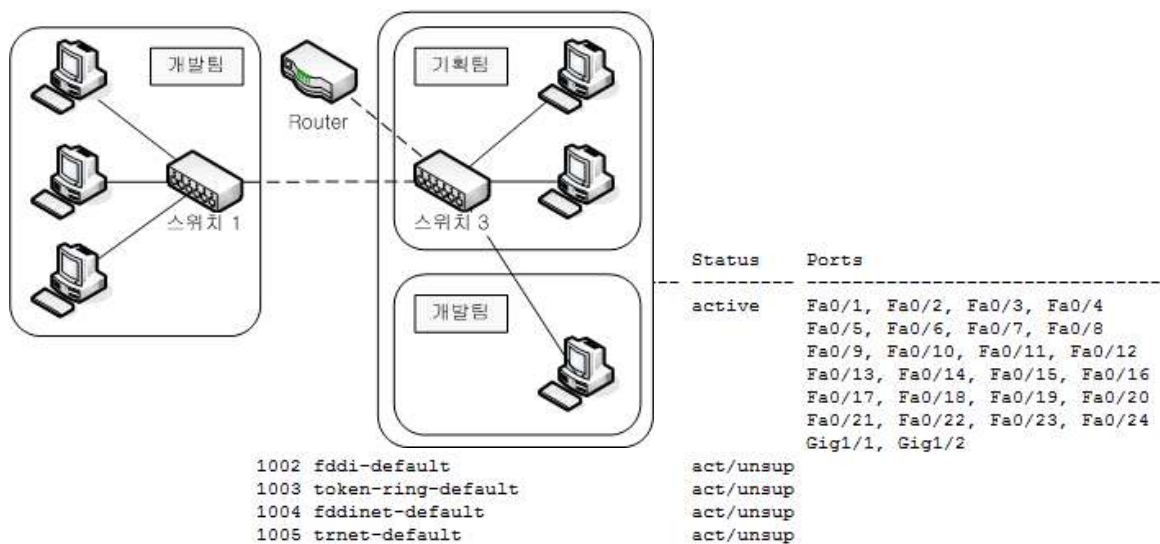


II

네트워크 기초(LAN)

06 LAN 구성 및 기본 프로토콜 이해

07 VLAN 구성

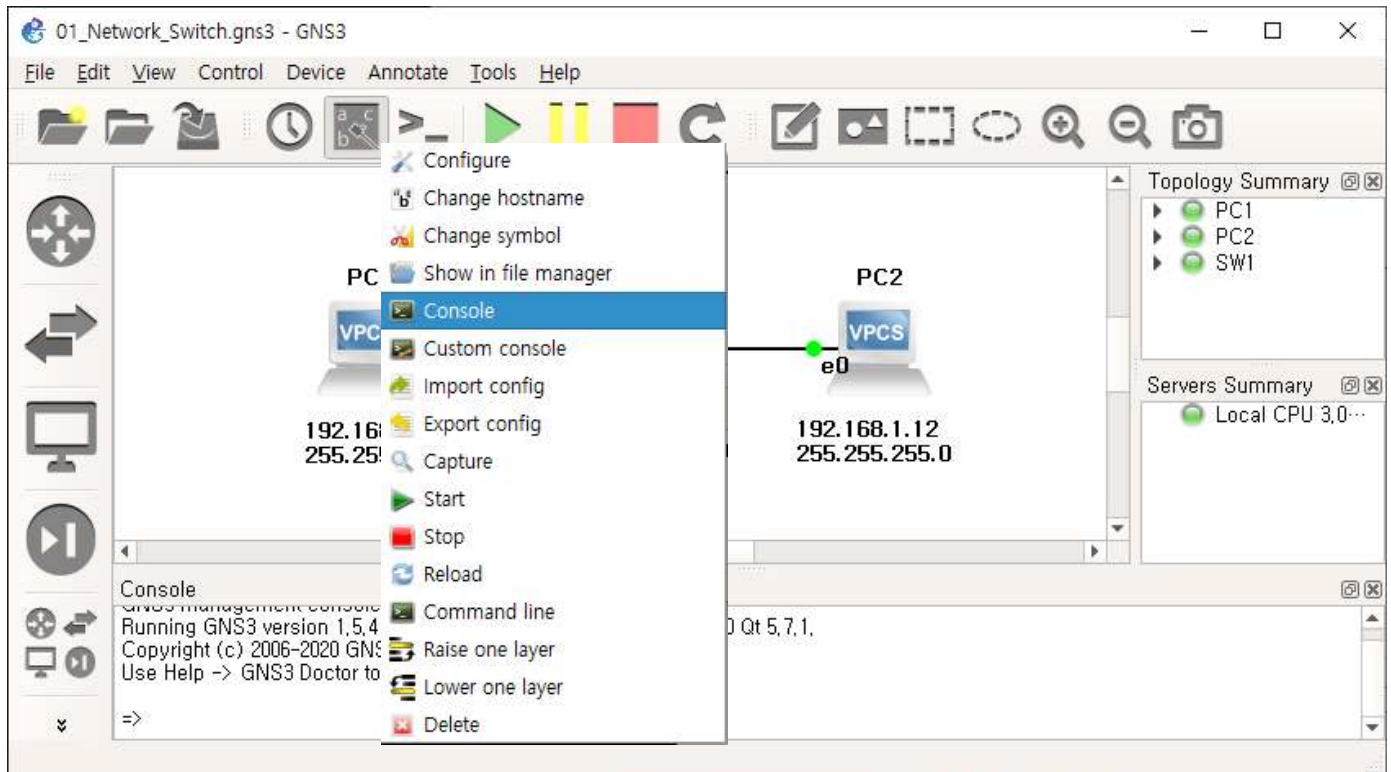


06 LAN 구성 및 기본 프로토콜 이해(IP주소, ARP, ICMP)

1. LAN(192.168.1.0) 구성하기

GNS의 VPCS와 스위치를 이용하여 다음 LAN을 구성한다.

| VPCS | IP주소 | 서브넷마스크 |
|------|--------------|---------------|
| PC1 | 192.168.1.11 | 255.255.255.0 |
| PC2 | 192.168.1.12 | 255.255.255.0 |



① VPCS의 **Console** 을 이용하여 PC1, PC2의 IP주소를 다음과 같이 설정하고 저장한다.

※ Console 창은 PC1 또는 PC2를 더블클릭하거나 마우스 오른쪽 버튼을 이용한 단축메뉴의 Console를 선택할 수 있다.

```
PC1> ip 192.168.1.11 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.1.11 255.255.255.0

PC1> save
Saving startup configuration to startup.vpc
. done

PC1>
```

```
PC2> ip 192.168.1.12 255.255.255.0
Checking for duplicate address...
PC2 : 192.168.1.12 255.255.255.0

PC2> save
Saving startup configuration to startup.vpc
. done

PC2>
```

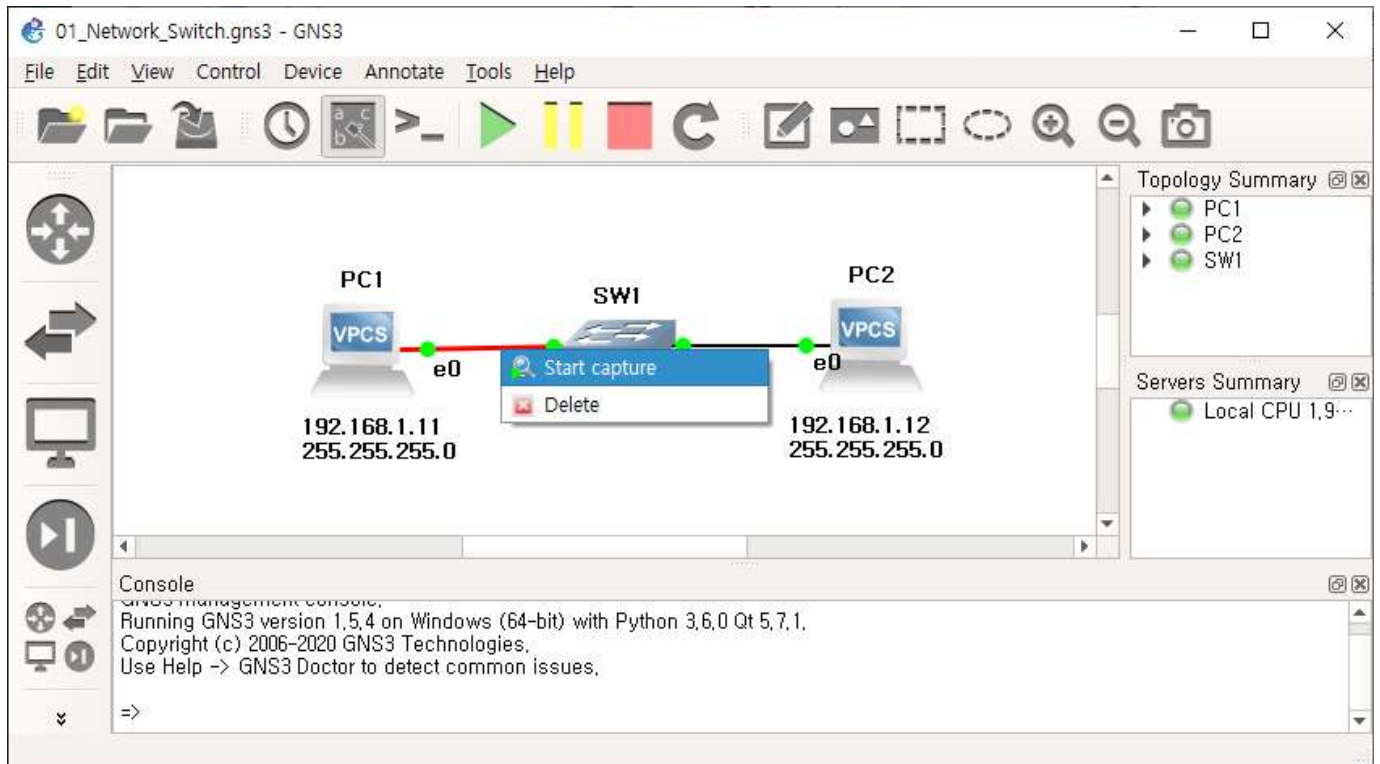
2. IP주소, ARP(Address Resolution Protocol), ICMP(Internet Control Message Protocol)

PC1, PC2에 192.168.1.11, 192.168.1.12와 같은 IP주소를 설정하여 192.168.1.0의 LAN(Local Area Network)을 구성하였다. LAN에 포함된 PC1, PC2는 192.168.1.11, 192.168.1.12와 같은 IP주소도 사용하지만, LAN에서 데이터를 전송하기 위해서는 서로의 MAC 주소(물리적 주소)를 파악해야 한다. 이 과정에서 IP를 보조하기 위한 수단으로 ARP(Address Resolution Protocol)가 사용된다.

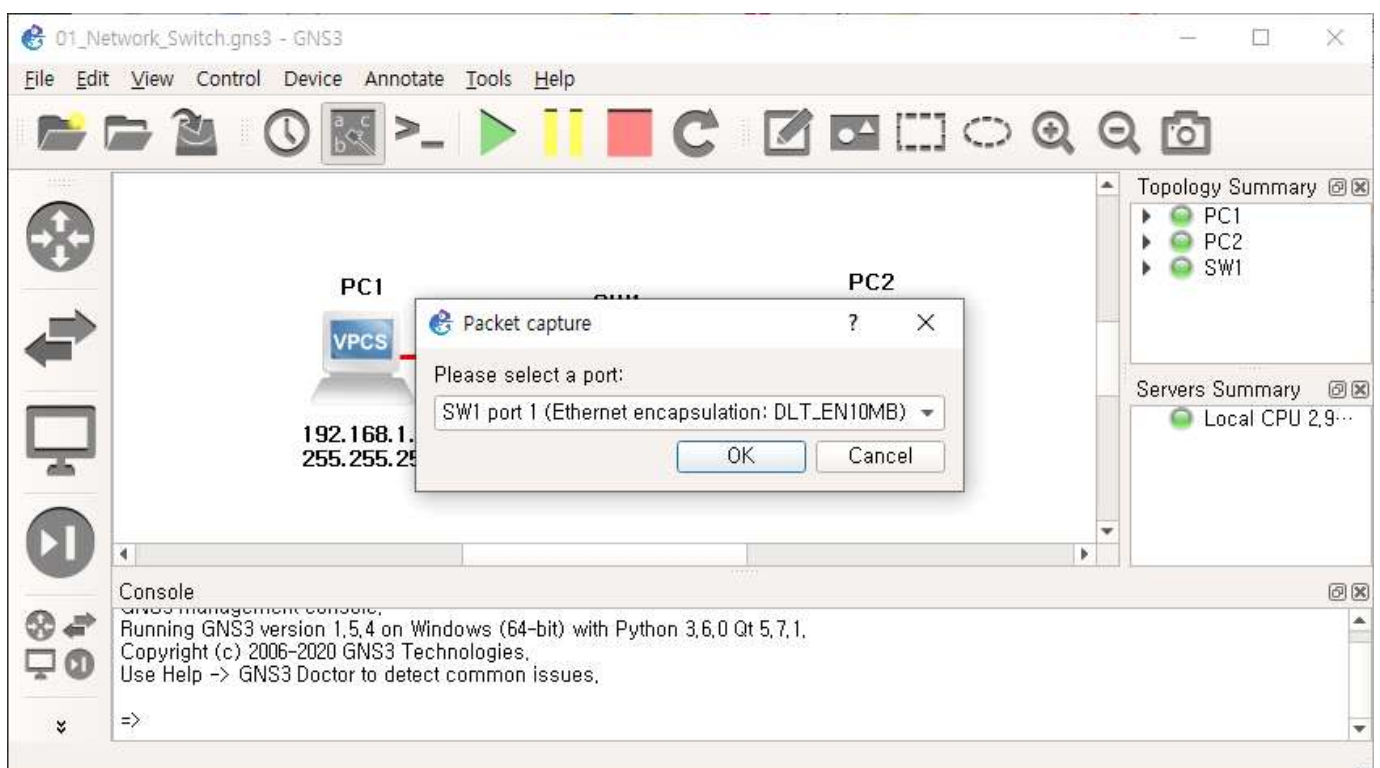
ICMP(Internet Control Message Protocol)는 네트워크에서 진단이나 제어에 주로 사용되는 프로토콜이다. ping, tracroute와 같은 명령을 이용하여 상대 호스트의 동작 여부, 목적지 호스트까지의 경로 등을 확인할 수 있다.

3. ARP(Address Resolution Protocol) 동작 확인

- ① 토폴로지 상의 PC1과 SW1 사이의 링크를 선택하고 마우스 오른쪽을 클릭하여 [Start Capture]를 선택한다.



- ① 패킷을 캡처하고자 하는 대상 포트를 선택하여 와이어샤크를 실행한다.



- ③ PC1의 IP주소를 192.168.1.20으로 변경한다. IP주소를 변경하면 호스트는 LAN 상에서 동일한 IP주소를 사용하는 다른 호스트가 있는지 확인하는 과정을 먼저 수행하며, 이 과정을 위한 패킷을 송신하게 된다.

```

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.1.11/24
GATEWAY    : 255.255.255.0
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 10001
RHOST:PORT : 127.0.0.1:10002
MTU       : 1500

PC1> ip 192.168.1.20
Checking for duplicate address...
PC1 : 192.168.1.20 255.255.255.0

PC1>
  
```

- ④ 실행중인 와이어샤크에 PC1이 IP주소 중복을 확인하기 ARP의 일종인 GARP를 전송한 것을 확인할 수 있다. GARP는 주로 IP주소 충돌을 감지하기 위해 사용한다. ARP와는 다르게 자신의 IP주소를 타겟 주소로 ARP 요청을 보내게 되고, 이에 응답하는 호스트가 있다면 이 IP주소는 누군가에게 사용되고 있다는 의미가 된다.

Capturing from - [SW1 1 to PC1 Ethernet0]

| No. | Source | Destination | Protocol | Length | Info |
|-----|------------------|-------------|----------|--------|---|
| 1 | Private_66:68:00 | Broadcast | ARP | 64 | Gratuitous ARP for 192.168.1.20 (Request) |
| 2 | Private_66:68:00 | Broadcast | ARP | 64 | Gratuitous ARP for 192.168.1.20 (Request) |
| 3 | Private_66:68:00 | Broadcast | ARP | 64 | Gratuitous ARP for 192.168.1.20 (Request) |

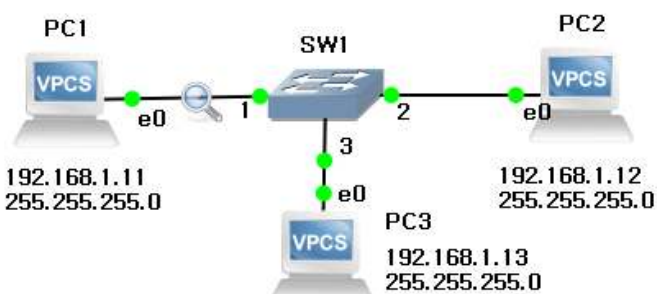
Protocol size: 4
 Opcode: request (1)
 [Is gratuitous: True]
 Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
 Sender IP address: 192.168.1.20
 Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
 Target IP address: 192.168.1.20

0010 08 00 06 04 00 01 00 50 79 66 68 00 c0 a8 01 14P yfh.....
 0020 ff ff ff ff ff ff c0 a8 01 14 00 00 00 00 00 00

Opcode (arp.opcode), 2 bytes | Packets: 3 · Displayed: 3 (100.0%) | Profile: Default

- ※ 위의 패킷의 Sender IP address와 Target IP address가 192.168.1.20으로 모두 같음을 확인할 수 있다. GARP 패킷이 3번 전송되는 동안 어떤 호스트에서도 응답(Reply) 패킷을 전송하지 않았으므로 192.168.1.20을 사용하는 호스트는 없는 것으로 판단하고, PC1의 IP주소는 192.168.1.20으로 변경된다.

직접 해보기 - 1

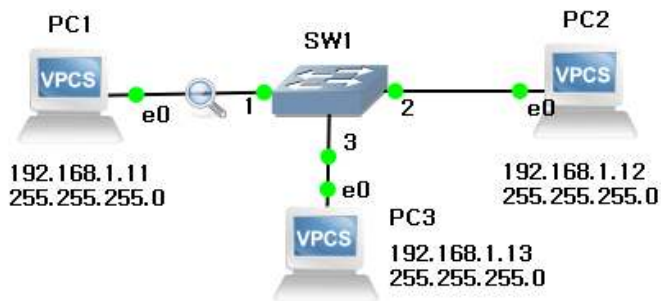


왼쪽과 같이 PC3를 추가하고 IP주소를 192.168.1.13으로 설정한다.

그 과정에서 전송되는 GARP 패킷을 확인하여 IP주소 중복을 감지하는 과정을 확인한다.

과제 - 1

GARP를 통한 IP주소 중복 확인 과정 이해하기



왼쪽과 같이 PC3이 추가된 토폴로지에서 PC3의 IP주소를 192.168.1.11 또는 192.168.1.12로 변경한다.

그 과정에서 전송되는 GARP 패킷을 확인하고, IP주소 변경 결과와 그 결과에 대한 해석을 아래에 작성하시오.

PC3의 콘솔 화면 캡처

```
PC3
PC3> ip 192.168.1.13 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.1.13 255.255.255.0

PC3> ip 192.168.1.11 255.255.255.0
Checking for duplicate address...
192.168.1.11 is being used by MAC 00:50:79:66:68:00
Address not changed

PC3>
```

PC3의 콘솔 화면 설명

PC3의 IP주소를 192.168.1.11로 변경하려 했으나 해당 IP주소를 사용하는 호스트가 있는 것으로 확인되었고, IP주소는 192.168.1.11로 변경되지 못했다.

와이어샤크 화면 캡처

• 와이어샤크 창의 패킷 중 이번 과정의 패킷만 보이게 캡처하세요.

Capturing from - [SW1 1 to PC1 Ethernet0]

File

Edit

View

Go

Capture

Analyze

Statistics

Telephony

Wireless

Tools

Help

</

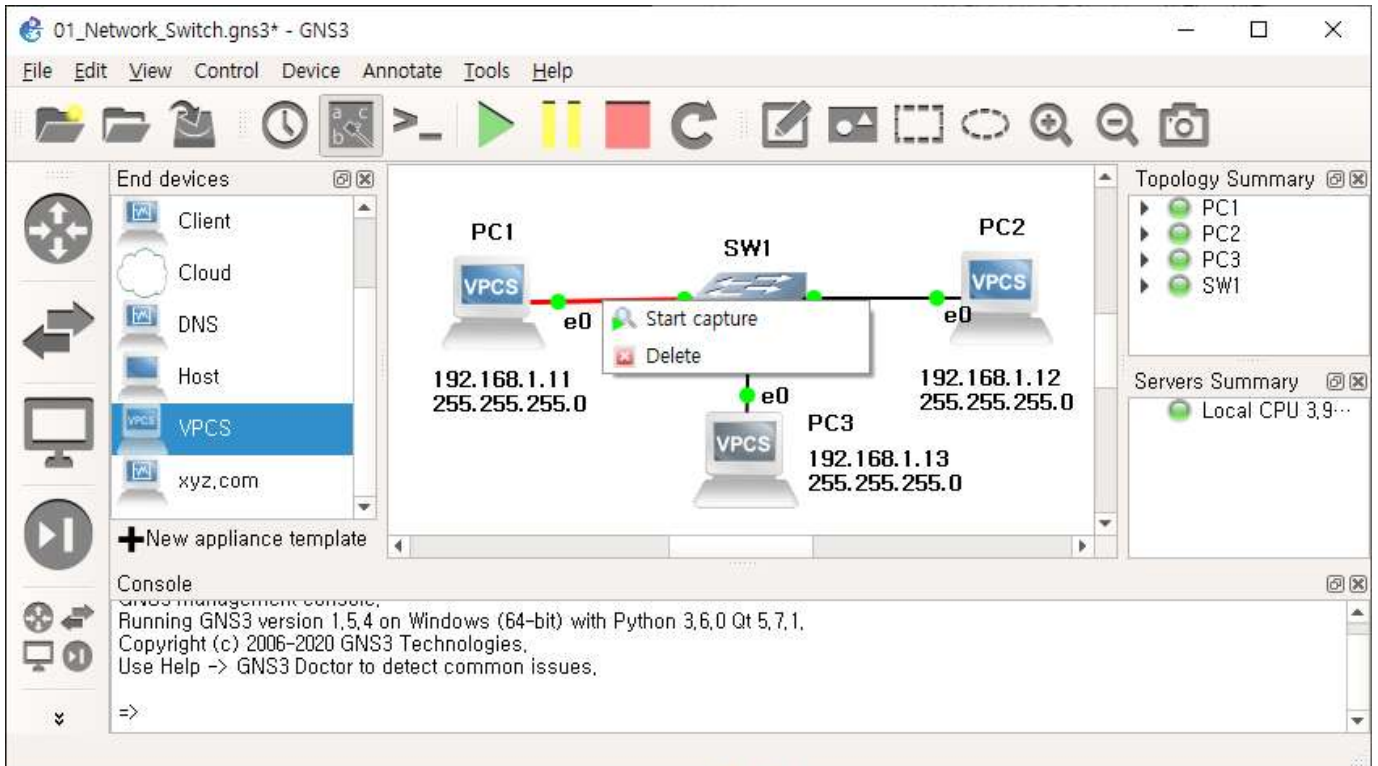
패킷에 대한 설명

• 캡처된 패킷의 번호(No.)를 포함하여 설명하시오.

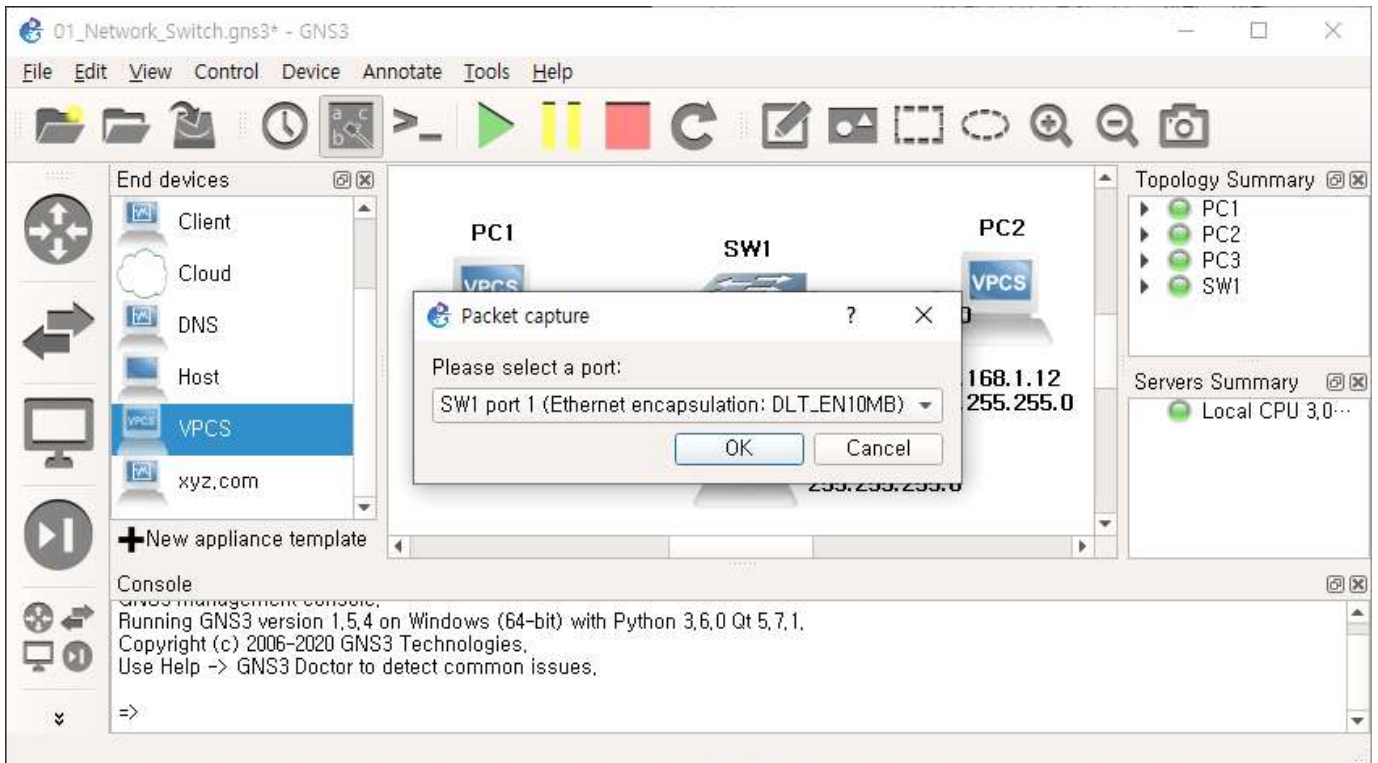
24번 ~26번 패킷은 PC3가 192.168.1.11을 사용하는 호스트가 있는지 확인하기 위한 GARP 요청(Request) 패킷이며, 27번 패킷은 PC1이 PC3에게 192.168.1.11을 자신이 사용하고 있음을 알려주는 응답(Reply) 패킷이다.
이 패킷을 수신한 PC3는 192.168.1.11이 이미 사용되고 있음을 알 수 있게 된다.

4. ICMP(Internet Control Message Protocol) 동작 확인

- ① 토폴로지 상의 PC1과 SW1 사이의 링크를 선택하고 마우스 오른쪽쪽을 클릭하여 [Start Capture]를 선택한다.



- ② 패킷을 캡처하고자 하는 대상 포트를 선택하여 와이어샤크를 실행한다.



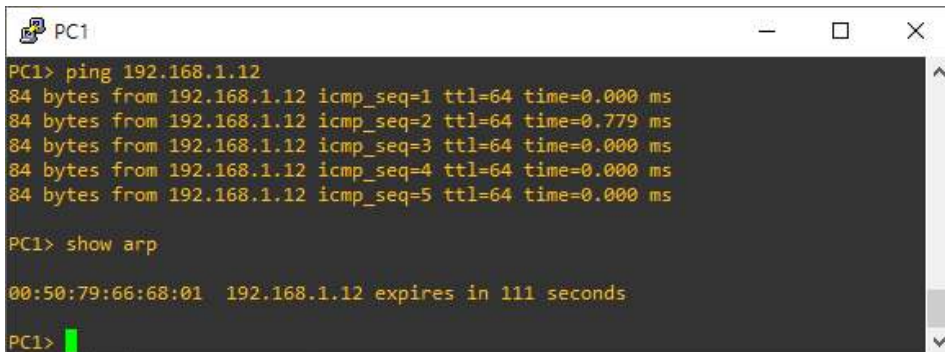
- ③ PC1에서 show arp 명령을 이용해 PC1의 arp table을 확인한다.



```
PC1> show arp
arp table is empty
PC1>
```

※ PC1의 arp table은 현재 비어 있다. arp table은 해당 호스트가 부팅된 이후 인식한 IP주소와 MAC 주소의 쌍을 저장한 테이블로 LAN에서 호스트간의 통신을 위해 사용된다. 즉, PC1(192.168.1.11)이 PC2(192.168.1.12)로 데이터를 보내고자 한다면 먼저 arp table을 확인하여 192.168.1.12에 대응되는 MAC 주소를 확인하는 과정을 거친다.

- ④ PC1에서 ping 192.168.1.12 명령을 통해 PC2의 응답을 확인한다.

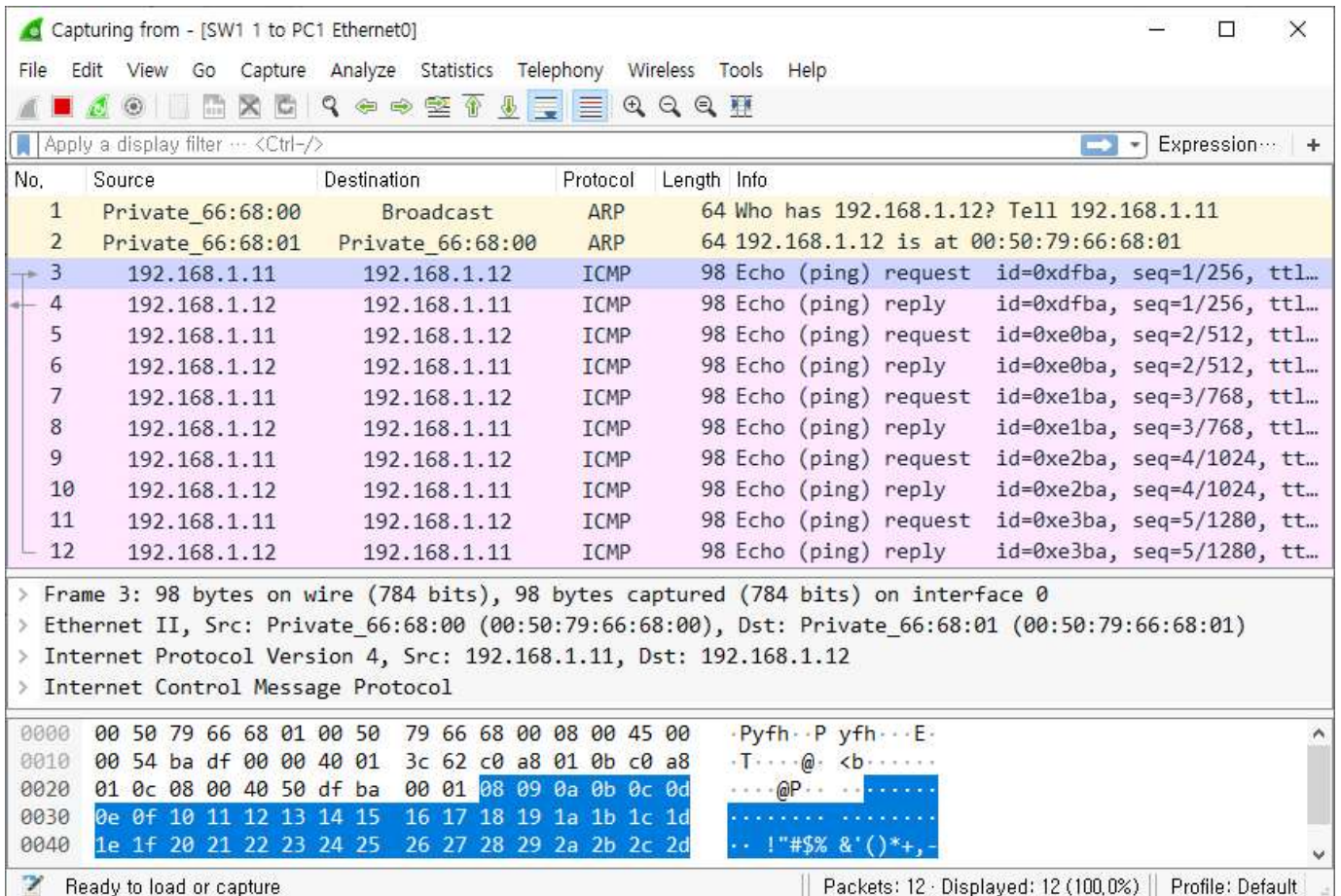


```
PC1> ping 192.168.1.12
84 bytes from 192.168.1.12 icmp_seq=1 ttl=64 time=0.000 ms
84 bytes from 192.168.1.12 icmp_seq=2 ttl=64 time=0.779 ms
84 bytes from 192.168.1.12 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 192.168.1.12 icmp_seq=4 ttl=64 time=0.000 ms
84 bytes from 192.168.1.12 icmp_seq=5 ttl=64 time=0.000 ms

PC1> show arp
00:50:79:66:68:01 192.168.1.12 expires in 111 seconds
PC1>
```

※ 192.168.1.12에서의 응답을 5번 수신한 것을 확인할 수 있다. 또한 show arp 명령을 통해 arp table에 192.168.1.12에 대응되는 MAC 주소가 저장된 것을 확인할 수 있다. arp table은 호스트의 설정에 따라 호스트가 켜져 있는 동안 유지되거나 일정 시간 이후에 삭제되기도 한다.

- ⑤ 와이어샤크에서 PC1에서 ping 192.168.1.12 명령을 수행하는 과정의 패킷을 확인한다.



Capturing from - [SW1 1 to PC1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| No. | Source | Destination | Protocol | Length | Info |
|-----|------------------|------------------|----------|--------|---|
| 1 | Private_66:68:00 | Broadcast | ARP | 64 | Who has 192.168.1.12? Tell 192.168.1.11 |
| 2 | Private_66:68:01 | Private_66:68:00 | ARP | 64 | 192.168.1.12 is at 00:50:79:66:68:01 |
| 3 | 192.168.1.11 | 192.168.1.12 | ICMP | 98 | Echo (ping) request id=0xdfba, seq=1/256, ttl=... |
| 4 | 192.168.1.12 | 192.168.1.11 | ICMP | 98 | Echo (ping) reply id=0xdfba, seq=1/256, ttl=... |
| 5 | 192.168.1.11 | 192.168.1.12 | ICMP | 98 | Echo (ping) request id=0xe0ba, seq=2/512, ttl=... |
| 6 | 192.168.1.12 | 192.168.1.11 | ICMP | 98 | Echo (ping) reply id=0xe0ba, seq=2/512, ttl=... |
| 7 | 192.168.1.11 | 192.168.1.12 | ICMP | 98 | Echo (ping) request id=0xe1ba, seq=3/768, ttl=... |
| 8 | 192.168.1.12 | 192.168.1.11 | ICMP | 98 | Echo (ping) reply id=0xe1ba, seq=3/768, ttl=... |
| 9 | 192.168.1.11 | 192.168.1.12 | ICMP | 98 | Echo (ping) request id=0xe2ba, seq=4/1024, tt=... |
| 10 | 192.168.1.12 | 192.168.1.11 | ICMP | 98 | Echo (ping) reply id=0xe2ba, seq=4/1024, tt=... |
| 11 | 192.168.1.11 | 192.168.1.12 | ICMP | 98 | Echo (ping) request id=0xe3ba, seq=5/1280, tt=... |
| 12 | 192.168.1.12 | 192.168.1.11 | ICMP | 98 | Echo (ping) reply id=0xe3ba, seq=5/1280, tt=... |

> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)

> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12

> Internet Control Message Protocol

0000 00 50 79 66 68 01 00 50 79 66 68 00 08 00 45 00 Pyfh..P yfh...E.

0010 00 54 ba df 00 00 40 01 3c 62 c0 a8 01 0b c0 a8 .T....@. <b.....

0020 01 0c 08 00 40 50 df ba 00 01 08 09 0a 0b 0c 0d ...@P.....

0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d

0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ..!"#\$%&'()*+,-

Ready to load or capture | Packets: 12 · Displayed: 12 (100.0%) | Profile: Default

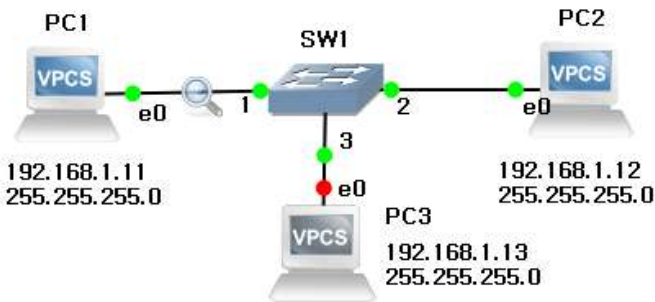
※ PC1에서 192.168.1.12로의 ping을 보내기 전에 ARP를 통해 192.168.1.12에 해당하는 MAC 주소를 확인한다. 그 이후에 ping request를 보내고 ping request를 수신한 것을 알 수 있다. PC1의 콘솔 화면에서는 reply 패킷에 대한 정보만 표시하고 있음을 확인할 수 있다.

직접 해보기 - 2

1. ping request, ping reply 패킷 중 하나를 선택하여 [Internet Control Message Protocol] 항목에서 [Data]의 크기가 몇 bytes이며, Data의 형태는 어떠한지 확인하시오.
2. ping request, ping reply 패킷의 Sequence number(BE), Sequence number(LE)가 어떻게 증가하는지 확인하시오.

과제 - 2

ICMP 메시지 확인하기



왼쪽과 같이 PC3을 마우스 오른쪽으로 클릭하여 **Stop** 을 선택한다.

PC1의 콘솔에서 ping 192.168.1.13을 수행하고, 콘솔 화면과 와이어샤크를 통해 결과를 확인하고, 결과에 대한 해석을 아래에 작성하시오.

PC1의 콘솔 화면 캡처

```
PC1
PC1> ping 192.168.1.13
host (192.168.1.13) not reachable
PC1>
```

PC3의 콘솔 화면 설명

192.168.1.13에 도달할 수 없음을 표시한다.

와이어샤크 화면 캡처

- 와이어샤크 창의 패킷 중 이번 과정의 패킷만 보이게 캡처하세요.

패킷에 대한 설명

- 캡처된 패킷의 번호(No.)를 포함하여 설명하시오.

13번 ~25번 패킷은 PC1이 192.168.1.13을 사용하는 호스트가 있는지 확인하기 위한 ARP 요청(Request) 패킷을 LAN에 브로드캐스트 한 과정이다. 이에 대한 응답(Reply) 패킷을 수신하지 못했으므로 PC1은 192.168.1.13에 도달할 수 없다는 메시지를 콘솔 화면에 표시한다.

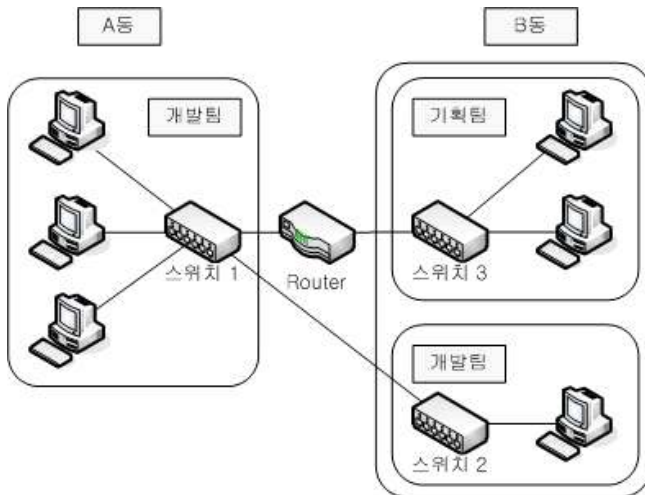
07 VLAN 구성

1. VLAN(Virtual LAN)

VLAN은 스위치에 연결된 하나의 네트워크를 여러 개의 논리적인 네트워크로 분할하는 기술을 말한다. 이는 하나의 스위치를 여러 개의 스위치로 분할하여 사용하는 것으로 생각하면 된다.

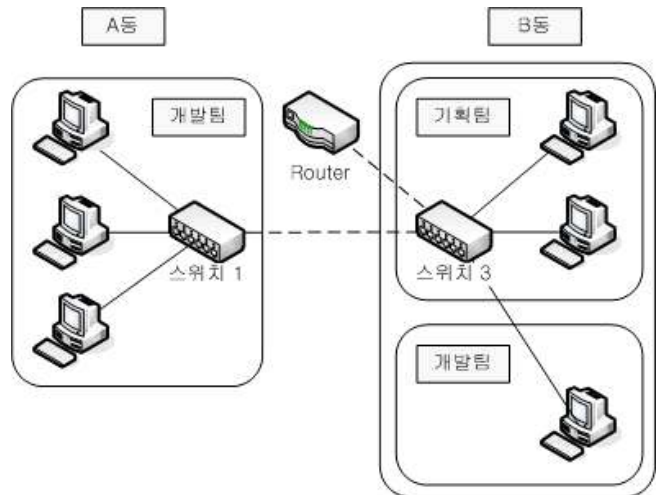
각각의 VLAN은 독립적인 스위치같이 동작하며, 여러 스위치에 동일한 방식으로 VLAN을 설정하여 다양한 형태로 네트워크를 구성할 수 있다.

■ VLAN이 없는 경우



개발팀의 컴퓨터가 건물 A동과 B동에 모두 위치했을 때에는 스위치1과 스위치2가 직접 연결되어야만 같은 개발팀이 동일한 네트워크를 유지할 수 있다.

■ VLAN을 사용한 경우



VLAN을 이용하면 1개의 스위치로 여러 개의 네트워크를 구성할 수 있다. 좌측의 네트워크 구성에서는 스위치가 3개 필요하지만 VLAN을 활용한다면 스위치 2개로 동일한 네트워크를 구성할 수 있다.

스위치에 PC, 프린터 등과 같은 많은 장치가 연결되어 네트워크의 규모가 커진다면 브로드캐스트 프레임도 증가하여 네트워크의 성능이 저하될 수 있다. VLAN은 브로드캐스트 도메인을 분할하여 브로드캐스트 트래픽으로 인한 네트워크의 성능 저하를 막을 수 있다.

또한 스위치로 구성된 네트워크에서는 별다른 제약 없이 특정 장치에 접속할 수 있어 보안상 취약한데, VLAN은 독립적인 네트워크를 구성하므로 서로 다른 VLAN에 속해 있는 장치들은 서로 통신이 불가능하여 보안성을 높일 수 있다.

■ VLAN 기본 정보

```
Switch#show vlan
```

| 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 Gig1/1, Gig1/2 |
| 1002 fddi-default | act/unsup | |
| 1003 token-ring-default | act/unsup | |
| 1004 fddinet-default | act/unsup | |
| 1005 trnet-default | act/unsup | |

기본적으로 스위치의 모든 포트는 VLAN 1에 속해있다. 또한 VLAN은 번호로 구분하며, 할당할 수 있는 번호는 1번부터 1005번까지이다. 이 중에서 예약된 1번, 1002~1005를 제외한 2번부터 1001번까지 사용자가 할당할 수 있다.

```
Switch#show flash
```

```
Directory of flash:/
```

| | | | | |
|---|------|---------|-----------|--------------------------------|
| 1 | -rw- | 4414921 | <no date> | c2960-lanbase-mz.122-25.FX.bin |
| 2 | -rw- | 616 | <no date> | vlan.dat |

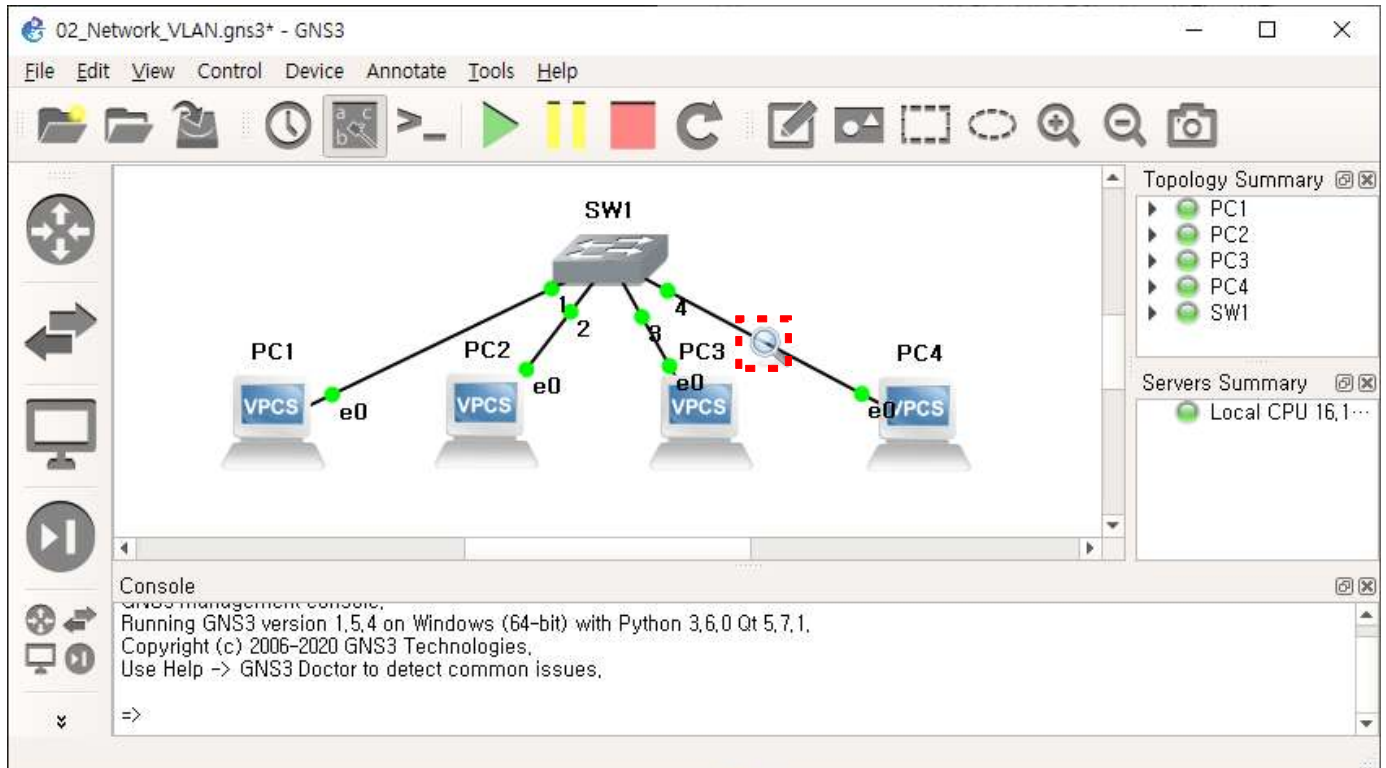
VLAN의 정보는 기본적으로 vlan.dat에 저장된다.

```
64016384 bytes total (59600847 bytes free)
```

2. 브로드캐스트 도메인 확인

스위치에 추가적인 VLAN이 설정되지 않은 경우 스위치의 모든 포트는 하나의 브로드캐스트 도메인으로 설정된다. 각 호스트의 IP주소와 서브넷 마스크를 이용한 설정은 가능하나 물리적으로 하나의 브로드캐스트 도메인인 것에는 변함이 없다. 다음 과정을 통해 스위치의 브로드캐스트 도메인에 대해 확인한다.

- ① GNS에서 VPCS PC1, PC2, PC3, PC4과 스위치 SW1을 추가하고, 각 VPCS와 스위치를 순서대로 연결한다. SW1과 PC4 사이의 링크를 선택하고 Start capture를 클릭한다.



- ② GNS에서 VPCS PC1, PC2, PC3, PC4과 스위치 SW1을 추가하고, 각 VPCS와 스위치를 순서대로 연결한다.

```
PC1> ip 192.168.1.10 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0
PC1>
```

| VPCS | IP주소 | 서브넷 마스크 | 게이트웨이 |
|------|--------------|---------------|---------------|
| PC1 | 192.168.1.10 | 255.255.255.0 | 192.168.1.254 |
| PC2 | 192.168.1.20 | 255.255.255.0 | 192.168.1.254 |
| PC3 | 192.168.2.10 | 255.255.255.0 | 192.168.2.254 |
| PC4 | 192.168.2.20 | 255.255.255.0 | 192.168.2.254 |

※ PC1, PC2는 192.168.1.0 네트워크, PC3, PC4는 192.168.2.0 네트워크로 설정되었다.

IP주소와 서브넷 마스크를 이용하여 서로 다른 네트워크로 분리되었으나, 물리적으로는 하나의 스위치에 연결된 상태이다.

- ③ PC1에서 192.168.2.20으로 ping을 보낸다.

```
PC1> ping 192.168.2.20
host (255.255.255.0) not reachable
PC1>
```

※ PC1은 192.168.1.0 네트워크, PC4는 192.168.2.0 네트워크로 서로 다른 네트워크에 속하기 때문에 통신할 수 없는 상태이다.

④ 실행중인 와이어샤크의 패킷을 확인한다.

Capturing from [SW1 4 to PC4 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| No. | Source | Destination | Protocol | Length | Info |
|-----|------------------|-------------|----------|--------|--|
| 1 | Private_66:68:00 | Broadcast | ARP | 64 | Who has 255.255.255.0? Tell 192.168.1.10 |
| 2 | Private_66:68:00 | Broadcast | ARP | 64 | Who has 255.255.255.0? Tell 192.168.1.10 |
| 3 | Private_66:68:00 | Broadcast | ARP | 64 | Who has 255.255.255.0? Tell 192.168.1.10 |

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 50 79 66 68 00 08 06 00 01  .....P yfh.....
0010  08 00 06 04 00 01 00 50 79 66 68 00 c0 a8 01 0a  .....P yfh.....
0020  ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00  .....
  
```

Ready to load or capture | Packets: 6 · Displayed: 6 (100.0%) | Profile: Default

※ PC1과 PC4는 서로 다른 네트워크에 속하기 때문에 통신할 수 없는 상태이지만 스위치를 거친 브로드캐스트 패킷이 PC4까지 도달함을 확인할 수 있다. 즉, IP주소에 의해 필터링이 되고 있으나 스위치 모든 포트가 하나의 브로드캐스트 도메인이기 때문에 스위치에 연결된 모든 호스트에 패킷이 도달하는 상태임을 확인할 수 있다.

퀴즈 - 1

PC1의 IP주소를 192.168.1.10에서 192.168.2.30으로 변경한다면 PC1과 PC3, PC4는 서로 통신이 가능할까? 이유는 무엇인가?

PC1과 PC3, PC4는 서로 통신이 가능해진다. 이유는 스위치는 하나의 브로드캐스트 도메인이기 때문에 IP주소와 서브넷마스크를 이용해 같은 네트워크로 설정하면 서로 통신이 가능한 상태이기 때문이다.

3. VLAN 설정

스위치 SW1의 3번, 4번 포트를 VLAN2로 변경하여 브로드캐스트 도메인을 분리한다. 이를 통해 PC1, PC2의 192.168.1.0 네트워크와 PC3, PC4의 192.168.2.0 네트워크는 IP주소 뿐만 아니라 VLAN을 통해서도 서로 분리되어 보안상으로 더욱 안전한 네트워크로 변경되었다.

① 토폴로지 상의 SW1을 마우스 오른쪽으로 클릭하여 [Configure]를 선택한다.

02_Network_VLAN.gns3* - GNS3

File Edit View Control Device Annotate Tools Help

Topology Summary

- PC1
- PC2
- PC3
- PC4
- SW1

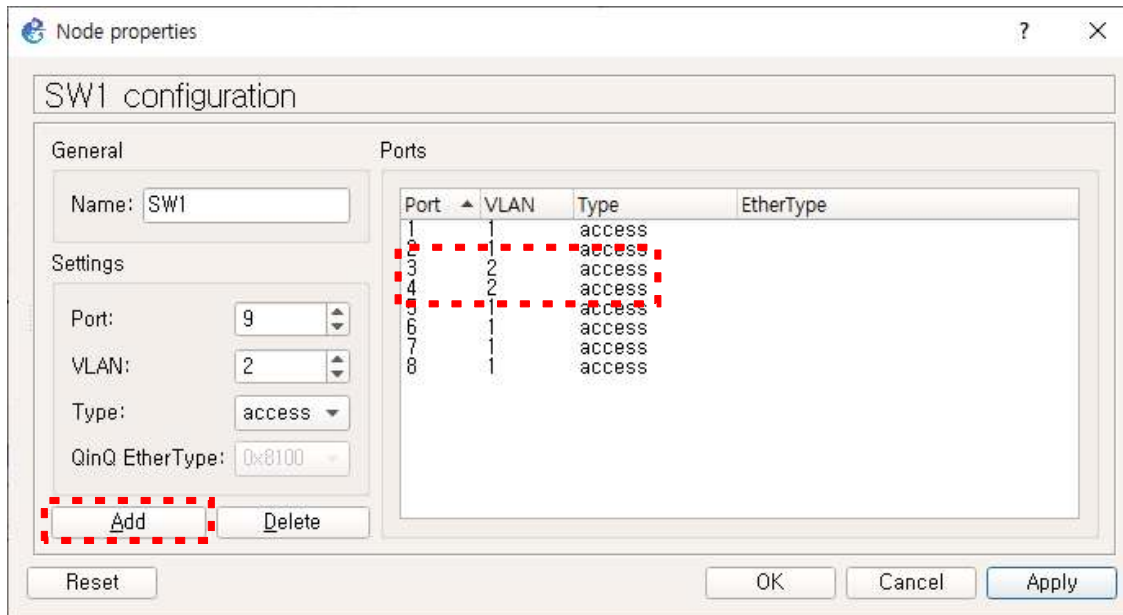
Servers Summary

- Local CPU 7,6...

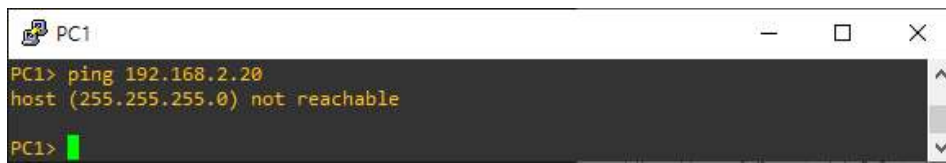
Console

Running GNS3 version 1.5.4 on Windows (64-bit) with Python 3.6.0 Qt 5.7.1.
Copyright (c) 2006-2020 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

- ② SW1의 설정에서 3번 포트를 선택하고, VLAN을 2로 변경 후, [Add]를 클릭한다. 4번 포트도 같은 방법으로 변경한다.

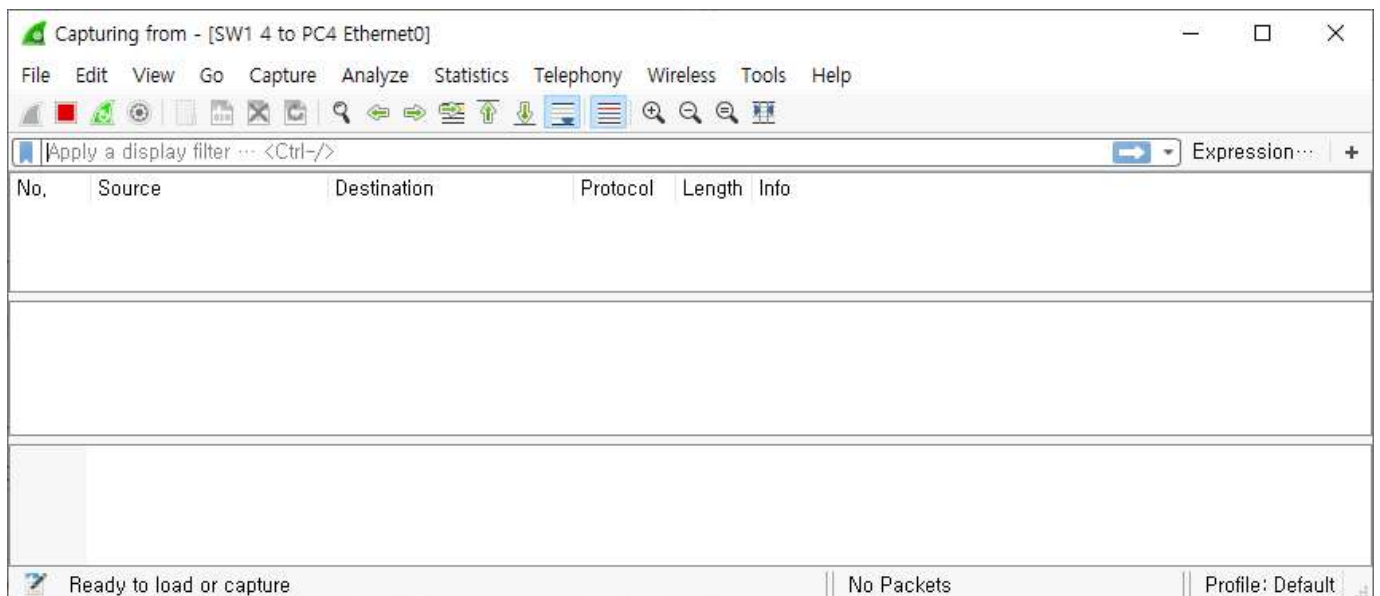


- ③ PC1에서 192.168.2.20으로 ping을 보낸다.



※ PC1은 192.168.1.0 네트워크, PC4는 192.168.2.0 네트워크로 서로 다른 네트워크에 속하기 때문에 통신할 수 없는 상태이다.

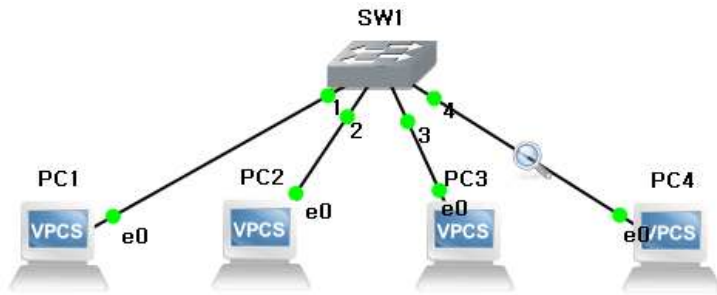
- ④ 실행중인 와이어샤크의 패킷을 확인한다.



※ 스위치 SW1의 3번, 4번 포트는 VLAN2로 지정되고, 다른 포트와는 통신할 수 없는 상태가 되었다. 현재 SW1의 VLAN 설정에 의해 2개의 브로드캐스트 도메인으로 변경되었다.

| VLAN | 해당 포트 번호 | 비고 |
|------|------------------|----------|
| 1 | 1, 2, 5, 6, 7, 8 | PC1, PC2 |
| 2 | 3, 4 | PC3, PC4 |

과제 - 3 브로드캐스트 도메인 확인하기



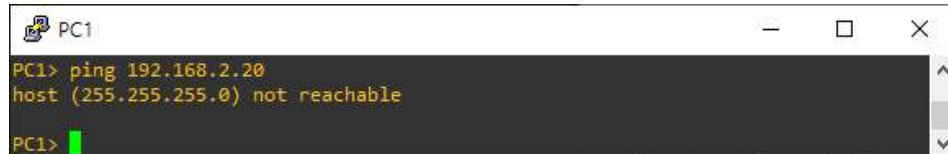
다음의 2구간을 와이어샤크로 모니터링 하여 2개의 와이어샤크 창을 열어둔다.

구간 1 : SW1 ↔ PC2

구간 2 : SW1 ↔ PC4

PC1에서 192.168.2.20으로 ping을 수행하고, 그 결과를 와이어샤크를 통해 확인하고 해석을 작성하시오.

PC1의 콘솔 화면 캡처

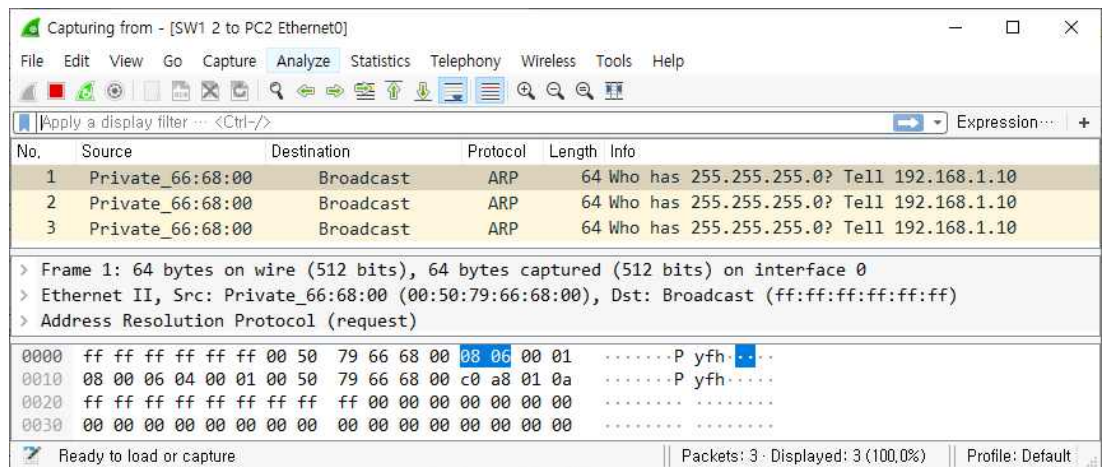


PC3의 콘솔 화면 설명

192.168.2.20이 서로 다른 네트워크이므로 도달할 수 없음을 표시한다.

구간 1의 와이어샤크 화면 캡처

- 와이어샤크 창의 패킷 중 이번 과정의 패킷만 보이게 캡처하세요.



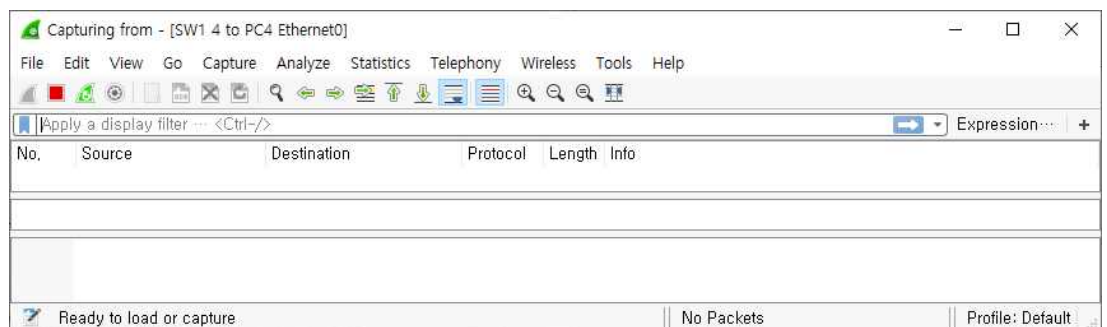
구간 1의 패킷에 대한 설명

- 캡처된 패킷의 번호(No.)를 포함하여 설명하시오.

1번 ~3번 패킷은 PC1이 192.168.2.20으로 보내 ping이 브로드캐스트 되었기 때문에 PC2에게도 패킷이 도달함을 확인할 수 있다.

구간 2의 와이어샤크 화면 캡처

- 와이어샤크 창의 패킷 중 이번 과정의 패킷만 보이게 캡처하세요.



구간 2의 패킷에 대한 설명

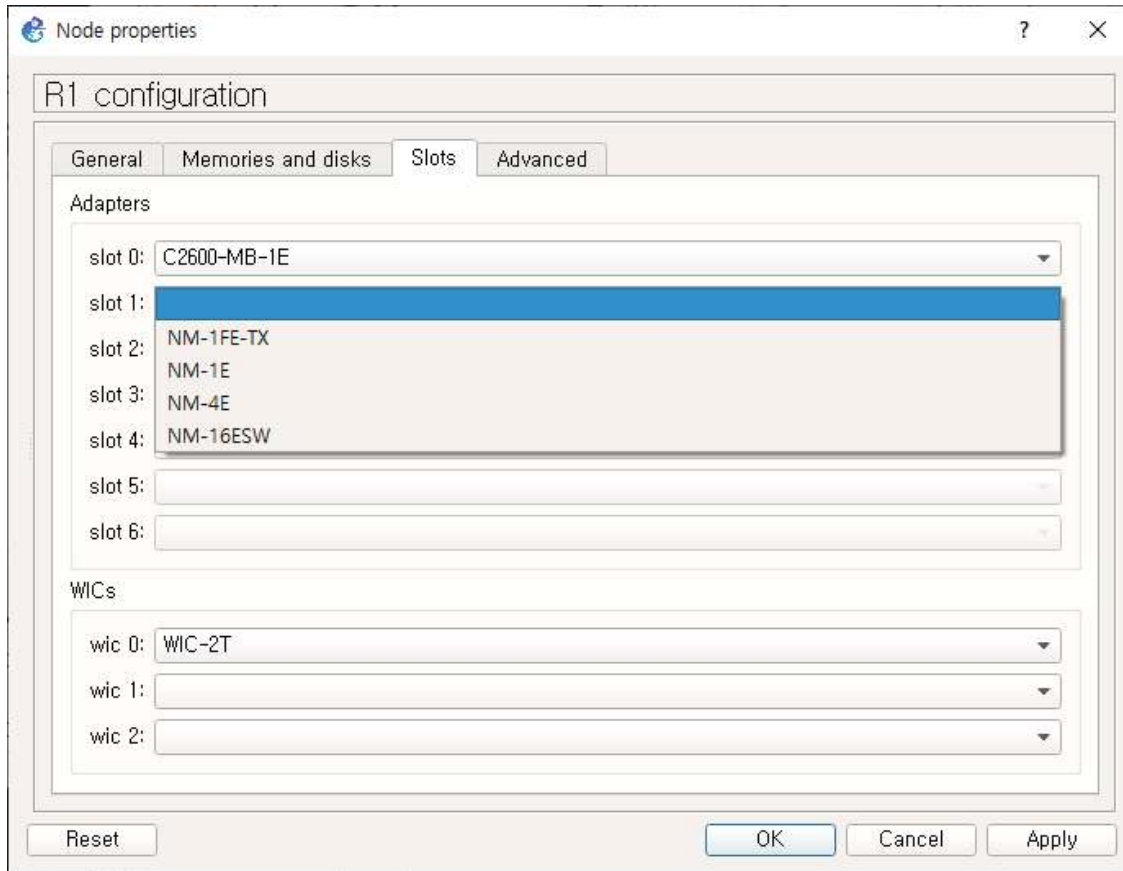
- 캡처된 패킷의 번호(No.)를 포함하여 설명하시오.

현재 스위치 SW1의 4번 포트는 VLAN2에 속하여 서로 다른 브로드캐스트 도메인이기 때문에 PC1이 보낸 브로드캐스트 패킷은 PC4에 도달할 수 없는 상태이다.

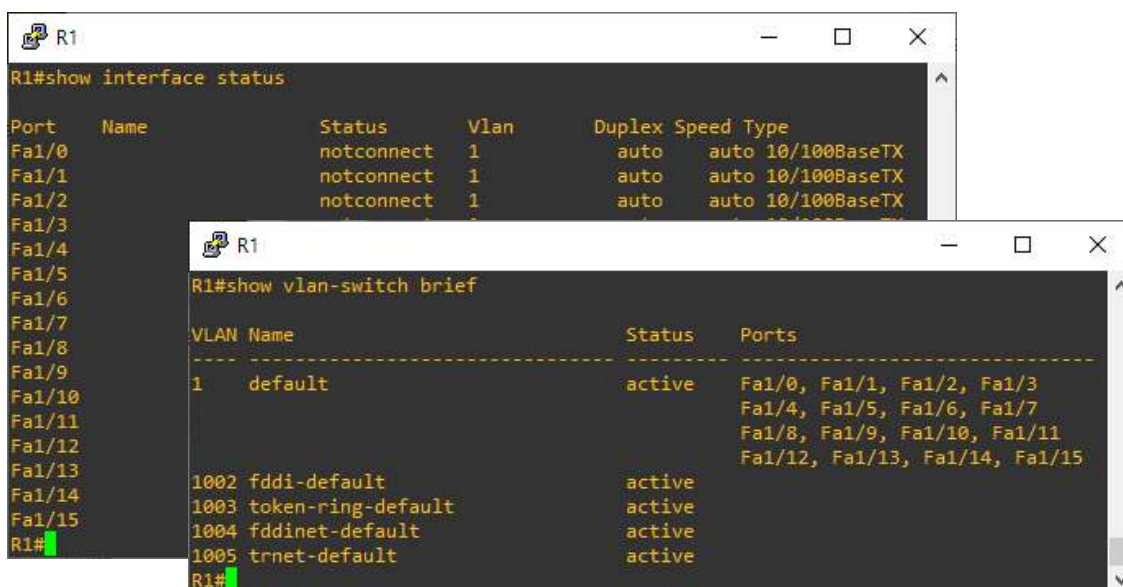
■ 스위치 실습을 위한 스위치 모듈 추가

GNS에서 기본적으로 제공하는 스위치는 기능이 제한되어 있고 명령어를 이용한 제어를 할 수 없다. 스위치 실습을 위해서는 라우터에 스위치 모듈(NM-16ESW)을 추가하여 16개 이더넷 포트를 이용해 스위치 실습을 할 수 있다.

- ① 라우터의 Configure 창에서 [Slots] 탭을 클릭한다. slot 중 하나를 선택하여 스위치 모듈(NM-16ESW)을 추가한다.



- ② 라우터에 콘솔(console)로 접속 후, show interface status 명령을 통해 이더넷 포트의 상태를 확인할 수 있다. 이제 라우터를 통해 스위치 실습을 할 수 있는 준비가 되었다.



③ 다음과 같이 VLAN을 설정할 수 있다.

```

SW1
SW1#vlan database
SW1(vlan)#vlan 2 name vlan2
VLAN 2 added:
  Name: vlan2
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface range FastEthernet 1/8 - 15
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 2
SW1(config-if-range)#exit
SW1(config)#exit
SW1#
*Mar  1 00:01:57.789: %SYS-5-CONFIG_I: Configured from console by console
SW1#show vlan-switch brief

```

| VLAN | Name | Status | Ports |
|------|--------------------|--------|--|
| 1 | default | active | Fa1/0, Fa1/1, Fa1/2, Fa1/3 Fa1/4, Fa1/5, Fa1/6, Fa1/7 |
| 2 | vlan2 | active | Fa1/8, Fa1/9, Fa1/10, Fa1/11 Fa1/12, Fa1/13, Fa1/14, Fa1/15 |
| 1002 | fddi-default | active | |
| 1003 | token-ring-default | active | |
| 1004 | fddinet-default | active | |
| 1005 | trnet-default | active | |

④ 필요에 따라 R1의 Symbol과 이름을 스위치와 같게 변경할 수 있다.

