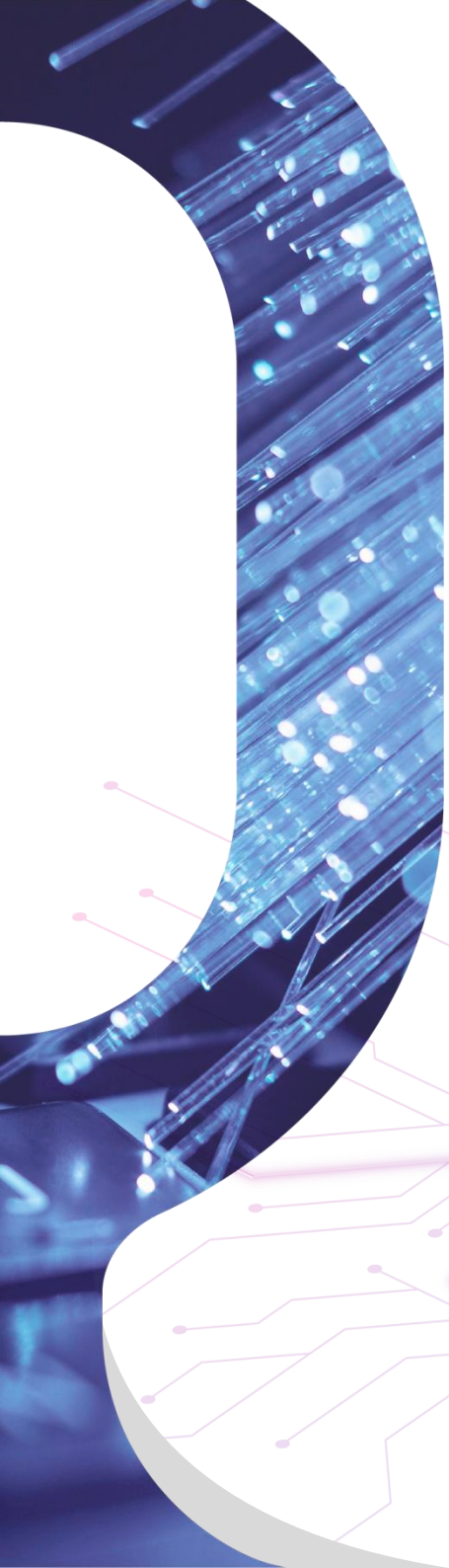


Trouble Shooting Guide

Product. E3010/E4020/E5010

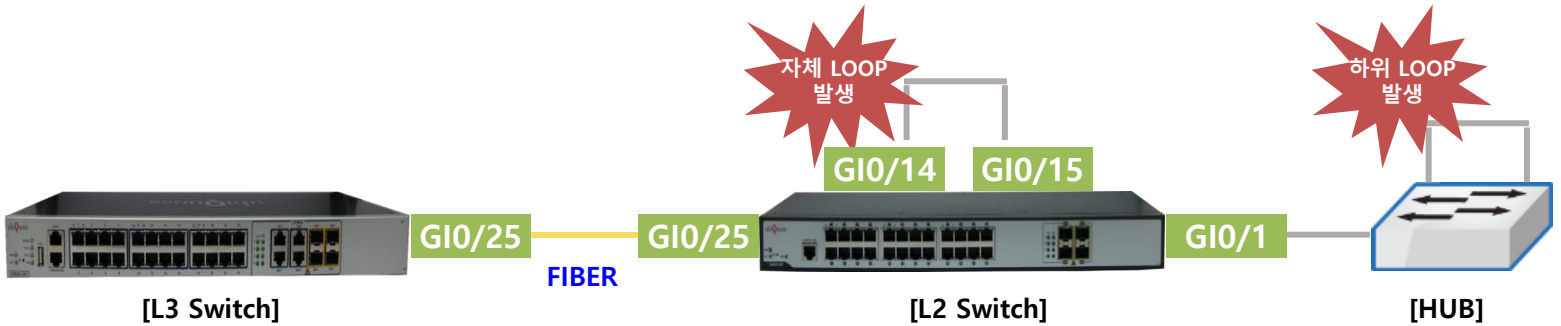
2022.05

ubiQuoss

1. LOOP 발생시 확인 및 조치방법#1

SLD (Self-Loop-Detection) 기능 이용한 LOOP 차단

- SLD 패킷을 초단위 전송하여, LOOP로 인해, SLD 패킷이 재수신되는 경우, LOOP로 간주 및 포트를 차단
- Default 무제한 차단이므로, recovery-time <1-1440min>을 설정하여, 포트 자동 해제되도록 설정필요



SLD 설정 및 확인

[설정방법]

```
Switch(config)# sld enable                                  (Global 모드 SLD 기능 활성화)
Switch(config)# interface range gi 0/14-0/15                (다운링크 포트 진입)
Switch(config-if-range)# sld enable                         (포트 SLD 기능 활성화)
Switch(config-if-range)# sld recovery-time 5                (포트 차단 후 해제시간 지정 = 5분)
Switch# show sld                                            (LOOP 발생시 포트 상태 확인)
Interface  Enable  Flag  Sts   Link  Recovery  Count  Last change   (Sts loop = loop,  Sts ok =normal)
Gi0/14       yes     .L   loop  down       295      1  00:00:05
Gi0/15       yes     .L   loop  down       295      1  00:00:05
Gi0/11       yes     .N     ok  up           0      0  01w01d02h
```

[차단로그]

```
May 26 14:30:05.007 [4] %SLD-4-PORT_SELF_LOOPED: Giga0/14 disabled: received SLD PDU
May 26 14:30:05.078 [4] %PM-SP-4-ERR_DISABLE: sld error detected on Gi0/14, putting Gi0/14 in err-disable state
May 26 14:30:04.977 [4] %SLD-4-PORT_SELF_LOOPED: Giga0/15 disabled: received SLD PDU
May 26 14:30:05.007 [4] %PM-SP-4-ERR_DISABLE: sld error detected on Gi0/15, putting Gi0/15 in err-disable state
```

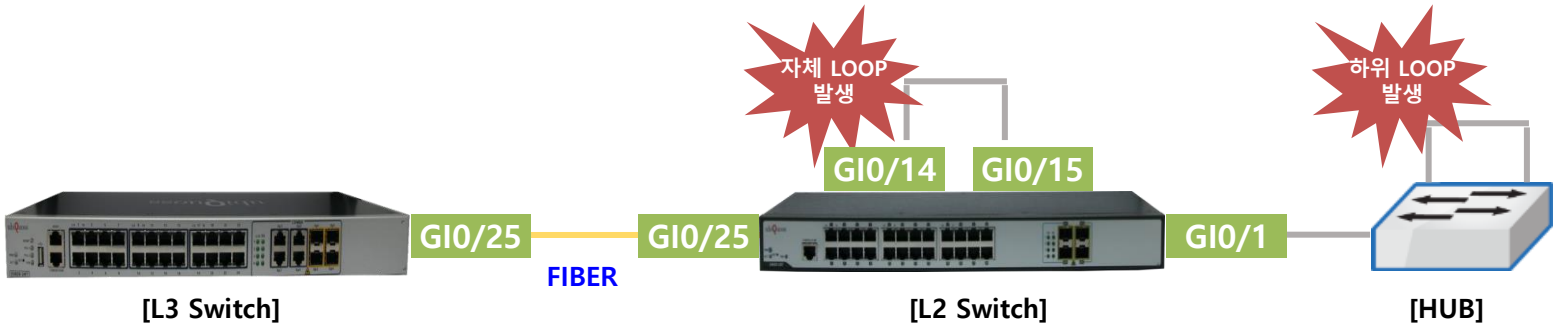
[해제로그]

```
May 26 14:35:04.982 [5] %SLD-5-PORT_ENABLE: Giga0/15 enabled by auto recovery timer
May 26 14:35:05.012 [5] %SLD-5-PORT_ENABLE: Giga0/14 enabled by auto recovery timer
```

1. LOOP 발생시 확인 및 조치방법#2

STP (Spanning-Tree Protocol) 기능 이용한 LOOP 차단

- BPDU 패킷을 초단위 전송하여, LOOP로 인해, BPDU 패킷이 재수신되는 경우, LOOP로 간주 및 포트를 차단
- 1) 자체 LOOP (포트간 연결) 차단시 : Role (Backp), Sts (BLK)처리, 2) 하단 LOOP로 차단시 : loopback guard err-disabled 처리



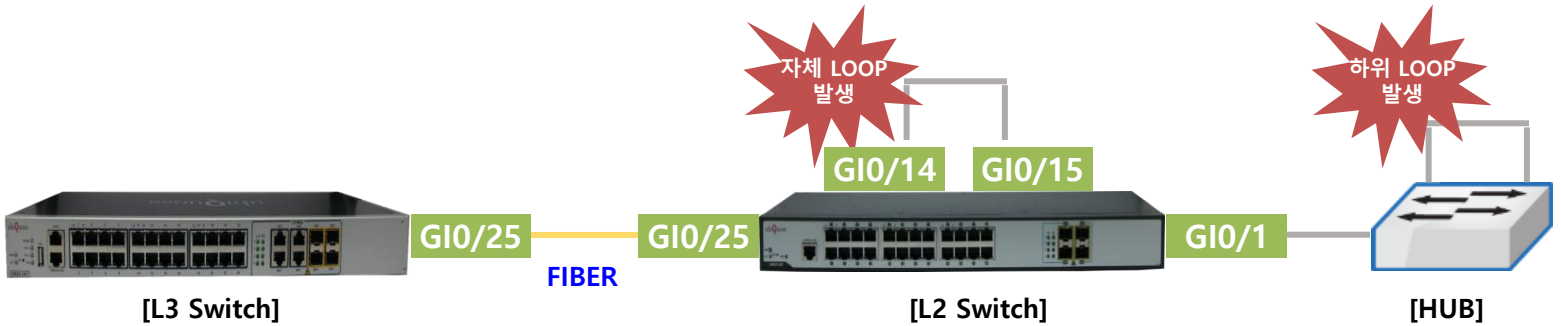
STP 설정 및 확인

```
[설정방법]
Switch(config)# spanning-tree mode rpvst+                          (STP mode rpvst+ 지정)
Switch(config)# spanning-tree pathcost method short                (STP pathcost short 지정)
Switch(config)# spanning-tree errdisable-timeout enable            (loopback guard 차단시, 해제기능 활성화)
Switch(config)# spanning-tree errdisable-timeout interval 60       (loopback guard 차단시, 60sec 후 차단해제)
Switch(config)# spanning-tree rpvst+ configuration                 (STP 적용할 VLAN 설정 모드 진입)
Switch(config-rpvst+)# vlan 1                                      (VLAN1 적용)
Switch(config-rpvst+)# vlan 10                                     (VLAN10 적용)
Switch(config-rpvst+)# exit
Switch(config)# spanning-tree enable                               (STP 활성화)

[자체 LOOP시 차단]
Switch# show spanning-tree rpvst+
---------------- ---------- --- --------- -------- --------------------------------
Giga0/15         Backp      BLK 4         128.115  P2p      portfast          (자체 LOOP시 포트 BLOCK : Role (Backp), Sts (BLK) 처리, LOOP 해제시, 자동 BLK 해제)

[하단 LOOP시 차단]
Switch# show interface status |include 0/15
Port      Name               Status       Vlan       Duplex  Speed   Type
--------- ------------------ ------------ ---------- ------- ------- ----------------
Gi0/1                        err-disabled 1006       full    a-1000  10/100/1000BaseT (하단 LOOP시 포트 err-disabled = shutdown 처리, errdisable-timeout에 의해 해제)

Aug 10 17:32:27.554 [4] %PM-SP-4-ERR_DISABLE: stp-loopback-guard error detected on Gi0/1, putting Gi0/1 in err-disable state
Aug 10 17:33:27.468 [4] %PM-SP-4-ERR_RECOVER: Attempting to recover from stp-loopback-guard err-disable state on Gi0/1
```

1. LOOP 발생시 확인 및 조치방법#3

TC (Traffic-Control)기능 이용한 LOOP 차단

- Traffic이 설정한 임계치를 초과하여, 유입시, 포트 차단, 임계치 이하로 유입시, 포트 차단 해제 (LOOP or 이상트래픽 차단 가능)
- SLD/STP의 경우, 송신 패킷을 재수신하는 경우, LOOP로 감지하나, 하단 HUB에서 패킷 Drop시, 감지불가 → TC 기능으로 차단/해제



TC 설정 및 확인

[설정방법]
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# traffic-control broadcast inbound 1200 500 block-mode (broadcast 1200pps 초과시 포트 차단, 500pps 이하시 포트 차단해제)
Switch(config-if-Giga0/1)# traffic-control multicast inbound 1200 500 block-mode (multicast 1200pps 초과시 포트 차단, 500pps 이하시 포트 차단해제

Switch# show port traffic-control

Port	traffic	high-pps	low-pps	status	avg-pps	
Gi0/1	broadcast	1200	500	blocked	288,797	(broadcast 1200pps 초과시 : blocked, 해제시 : normal)
	multicast	1200	500	blocked	72,680	(multicast 1200pps 초과시 : blocked, 해제시 : normal)

[차단로그]
May 26 15:47:34.924 [5] %PORT-TC-5-BLOCK: Inteface Giga0/1, block the traffic
May 26 15:47:34.924 [6] %PORT-TC-6-HIGH_THR: Interface Giga0/1 multicast-inbound (72,680) reached threshold (1200)
May 26 15:47:34.907 [6] %PORT-TC-6-HIGH_THR: Interface Giga0/1 broadcast-inbound (288,797) reached threshold (1200)

[해제로그]
May 26 15:47:44.945 [6] %PORT-TC-6-LOW_THR: Interface Giga0/1 broadcast-inbound (7) reached threshold (500)
May 26 15:47:44.945 [6] %PORT-TC-6-LOW_THR: Interface Giga0/1 broadcast-inbound (7) reached threshold (500)
May 26 15:47:44.964 [7] %PORT-TC-7-UNBLOCK: Inteface Giga0/1, keep block state by multicast traffic
May 26 15:47:44.964 [7] %PORT-TC-7-UNBLOCK: Inteface Giga0/1, keep block state by broadcast traffic

2. SFP 연동 포트 link up 불가시 조치방법#1

광레벨 RX 저하에 의한 link up 불가

- 대국장비에 연결된 광모듈과 동일 Type(거리)의 모듈인지 확인
- 광케이블 연결된 포트의 광레벨을 측정하여, 정상 범위내 RX값이 측정되는 지 확인

광레벨 확인 및 조치방법

[광레벨 확인]

```
Switch# show interface status
Port      Name               Status       Vlan       Duplex  Speed   Type
--------- ------------------ ------------ ---------- ------- ------- ----------------
Gi0/25    == UPLINK#1 ==     notconnect   trunk        full    auto 1000BaseSX
```

(notconnect : LINK DOWN, connected : LINK UP)

```
Switch# show interface transceiver
 Optical   Optical
         Temperature  Voltage  Current   Tx Power  Rx Power
Port     (Celsius)    (Volts)  (mA)      (dBm)     (dBm)
-------  -----------  -------  --------  --------  --------
Gi0/25      36.8        3.33     7.0       -5.1     -27.4 –
```

(RX : -17 ~ 0dBm 초과상태로, 대국장비 포함 회선 및 광모듈 점검필요)

[광레벨 범위]

Transceiver	Veondor	Vendor PN	RX 범위	TX 범위
10G LR(10km)	FOTTU	P31-64D10-RLP	-14 ~ 0dBm	-7.3 ~ 0.5dBm
10G ER(40km)	FOTTU	P55-64D40-RLP	-14 ~ 0dBm	-0.3 ~ 4dBm
10G ZR(80km)	FOTTU	P55-64D80-RLP	-24 ~ -7dBm	0 ~ 4dBm
10G ZR(80km)	LTI	LTI-SFP+ZR	-24 ~ -7dBm	0 ~ 5dBm
1G(10km)	Hi-Optel	HSFP-24-3311S-22	-22 ~ -3dBm	-9.5 ~ -3dBm
1G(40km)	Hi-Optel	HSFP-24-2521S-22	-22 ~ -3dBm	-5 ~ 0dBm
1G(500m)	HG	MXP-248S	-17 ~ 0dBm	-9 ~ -3dBm
100M(2km)	Hi-Optel	HSFP-03-3311M-12	-32 ~ -3dBm	-20 ~ -14dBm

2. SFP 연동 포트 link up 불가시 조치방법#2

SPEED AUTO-NEGO 불일치에 의한 link up 불가

- 대국장비와의 광모듈 Type 일치 및 광레벨 정상이나, link up 불가한 경우, SPEED AUTO-NEGO 불일치 여부 확인필요
- SPEED AUTO-NEGO 불일치시, SPEED MANUAL 스위치 = link up, SPEED AUTO 스위치 = link down으로 출력

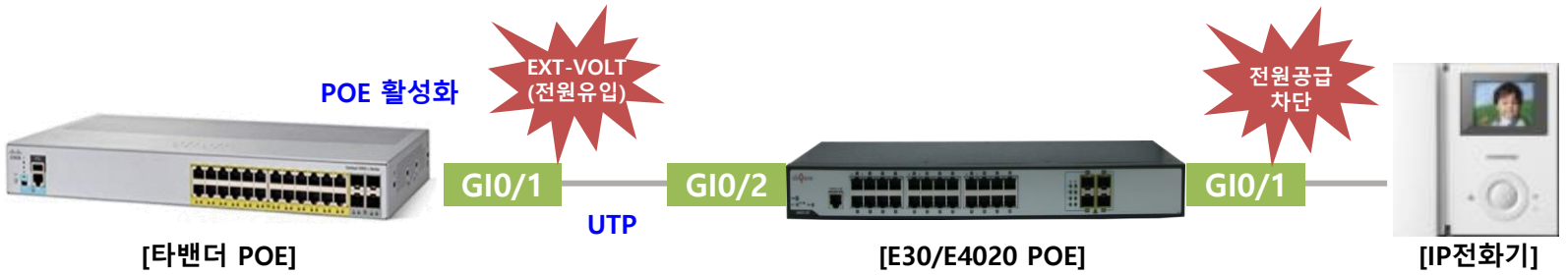
SPEED AUTO-NEGO 확인 및 조치방법

```
[L3 SPEED AUTO-NEGO 확인]
Switch# show interface status
Port     Name               Status       Vlan       Duplex  Speed   Type
-------- ------------------ ------------ ---------- ------- ------- ----------------
Gi0/25   == L2#1 ==     connected    trunk        full    1000 1000BaseSX          (1000 = SPEED MANUAL, a-1000 = SPEED AUTO)

[L2 SPEED AUTO-NEGO 확인]
Switch# show interface status
Port     Name               Status       Vlan       Duplex  Speed   Type
-------- ------------------ ------------ ---------- ------- ------- ----------------
Gi0/25   == UPLINK#1 ==     notconnect   trunk        full    auto 1000BaseSX        (1000 = SPEED MANUAL, a-1000 = SPEED AUTO)

[L2 SPEED MANUAL 변경 후 확인]
Switch(config)# interface gi0/25
Switch(config-if-Giga0/25)# speed nonegotiate                                    (SPEED MANUAL = speed nonegotiate,  SPEED AUTO = no speed nonegotiate)
Switch# show interface status
Port     Name               Status       Vlan       Duplex  Speed   Type
-------- ------------------ ------------ ---------- ------- ------- ----------------
Gi0/25   == UPLINK#1 ==     connected    trunk        full    1000 1000BaseSX
```

3. POE 하위 단말 전원 공급 불가

EXT-VOLT (외부전원) 유입에 의한 하위 단말 POE 전원 공급 불가

- 타밴더 POE와 당사 POE간 다단 구성시, POE 기능 활성화 및 당사 장비를 PD로 인지하여, EXT-VOLT (외부전원) 유입되는 CASE 발생
- 당사 POE 구OS (r261미만) EXT-VOLT (외부전원) 유입시, 칩 보호차원 ALL 포트 전원 공급을 차단하도록 설계됨
- 최신OS(r264)에서는 EXT-VOLT (외부전원) 유입시, 타포트의 전원 공급을 정상적으로 유지하도록 보완 (최신OS 업그레이드 필요)



EXT-VOLT 확인 및 조치방법

[EXT-VOLT 유입 포트 확인]

```
Switch# show logging |include PoE Voltage
 May 28 08:52:20.958 [5] %POE-5-EVENT: PoE Voltage Injection into the port in Giga0/2

Switch# show power inline port-status
 Port       Enable       Status                 Force-power  Class        AF/AT                 (EXT_VOLT = 외부 전원 유입 포트)
 Giga0/1    En (reg only)  off (DISCHARGED_LOAD_CAP) Disable    Class4(30.0W)  802.3AT   (DISCHARGED_LOAD_CAP = 외부 전원 유입으로 전원 공급 차단)
 Giga0/2    En (reg only)  off (EXT_VOLT)         Disable      Class0(15.4W)  802.3AT
```

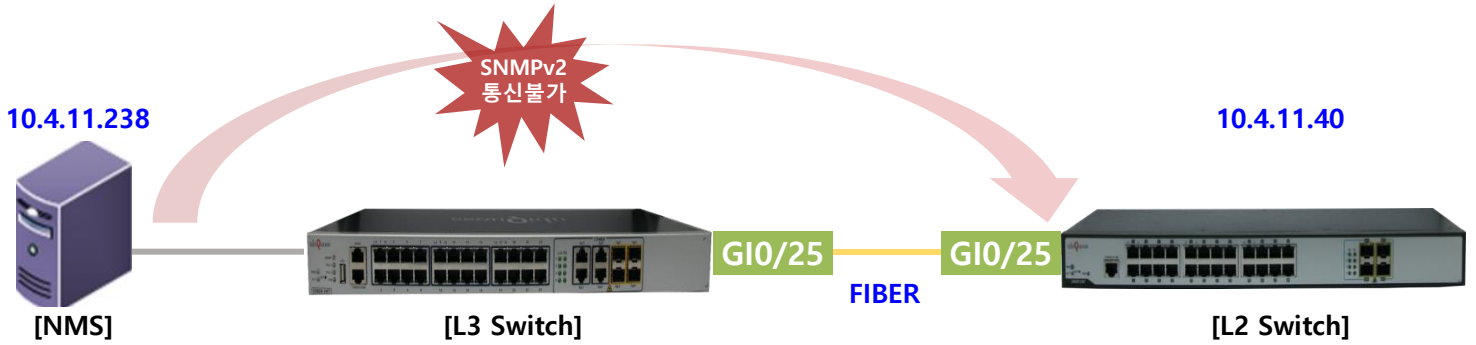
[최신OS 업그레이드 후 확인]

```
Switch# show power inline port-status
 Port       Enable       Status                 Force-power  Class        AF/AT
 Giga0/1    En (reg only)  on  (802-3AF/AT-DET)    Disable      Class4(30.0W)  802.3AT   (802-3AF/AT-DET) = 타포트 전원 공급 정상
 Giga0/2    En (reg only)  off (EXT_VOLT)         Disable      Class0(15.4W)  802.3AT   (EXT_VOLT = 외부 전원 유입 포트)

 Switch# show power inline all-port-power
 All port Power.
 ================================
 ifname         power
 ================================
 gi0/1          8.4 (W)                                                    전원 공급 8.4 (W) 정상
 gi0/2          0.0 (W)
```

4. SNMPv2 통신 불가

SNMPv2 설정오류 및 상위망 ACL 차단에 의한 통신 불가

- NMS와 스위치간, SNMPv2 Community 설정값 불일치에 의한 통신불가 여부 확인필요
- 상위망 SNMPv2 접근 대역 ACL 차단에 의한 통신불가 여부 확인필요



SNMPv2 통신 확인 및 조치방법

[SNMPv2 설정 확인]
Switch(config)# access-list extended PERMIT_SNMP permit ip host 40.1.1.100 any
Switch(config)# access-list extended PERMIT_SNMP permit ip host 10.4.11.238 any (SNMP ACL에 NMS 대역 허용여부 확인)
Switch(config)# access-list extended PERMIT_SNMP deny ip any any
Switch(config)# ip option snmp-acl access-group PERMIT_SNMP
!
Switch(config)# snmp-server community ro (SNMP Community 설정값 일치 여부 확인 및 재설정)

New password: public123#
Retype new password: public123#

[SNMPv2 통신 확인]
Switch# tcpdump interface any udp port 161
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
17:24:43.113070 In 00:e0:91:56:1f:a6 ethertype IPv4 (0x0800), length 91: 10.4.11.238.58932 > 10.4.11.40.161: C=public123# GetNextRequest(24) .1.3.6.1.2.1.1.3
17:24:43.115915 Out 70:30:5d:1c:43:91 ethertype IPv4 (0x0800), length 91: 10.4.11.40.161 > 10.4.11.238.58932: C=public123# GetResponse(28) .1.3.6.1.2.1.1.3.0=2818700

(TCPDUMP로 UDP 161 패킷 정상 송/수신 여부 확인 및 Community값 일치 여부 확인 → Request 패킷이 없는 경우, 상위망에서 ACL 차단여부 확인필요)

5. 비정상 IP 할당에 따른 서비스 불가

스위치 하단 공유기 연결 오류에 의한 사설IP 할당 및 서비스 불가

- 스위치 하단 공유기 연결시, WAN 포트에 연결하여야 하나, LAN 포트에 잘못 연결하여, 공유기의 사설IP 할당 → 서비스 불가 발생
- 공유기의 포트를 LAN → WAN으로 변경 필요하며, 타포트로의 사설IP 할당을 예방하기 위해서는 DHCP-FILTER 사전 설정필요

IP할당 내역 확인 및 조치방법

```
[IP할당 내역 확인]
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# ip dhcp snooping
Switch# show ip dhcp snooping binding
State Codes: (E) - Lease Time Expired

Mac Address    IP Address      State                Lease(sec) Vlan Interface
-------------- --------------- -------------------- ---------- ---- ---------
0000.6a0d.0102 192.168.1.11    Ack                  3600       1 Giga0/11
0000.6a0d.0103 192.168.1.12    Ack                  3600       1 Giga0/12

[DHCP FILTER 설정 후 IP재할당 확인]
Switch(config)# interface range gi 0/1-0/24
Switch(config-if-range)# filter dhcp
Switch# show ip dhcp snooping binding
State Codes: (E) - Lease Time Expired

Mac Address    IP Address      State                Lease(sec) Vlan Interface
-------------- --------------- -------------------- ---------- ---- ---------
0000.6a0d.0102 182.223.75.11   Ack                  3600       1 Giga0/11
0000.6a0d.0103 182.223.75.12   Ack                  3600       1 Giga0/12
```

(dhcp snooping 설정하여, ip할당 내역 확인)

(공유기 연결 오류에 의한 타포트 사설ip 할당 내역 확인)

(다운링크에서 유입되는 dhcp offer/ack 차단 / 업링크 설정 금지)

(다운링크에서 유입되는 dhcp offer/ack 차단 후 ip 정상 할당 확인)

6. CRC 발생시 확인 및 조치방법

CRC (Cyclic Redundancy Check)

- CRC 에러는 이더넷프레임의 "CRC Checksum" 에 문제가 있을 때 발생한다
- 물리적인 포트/회선/모듈등의 점검 필요

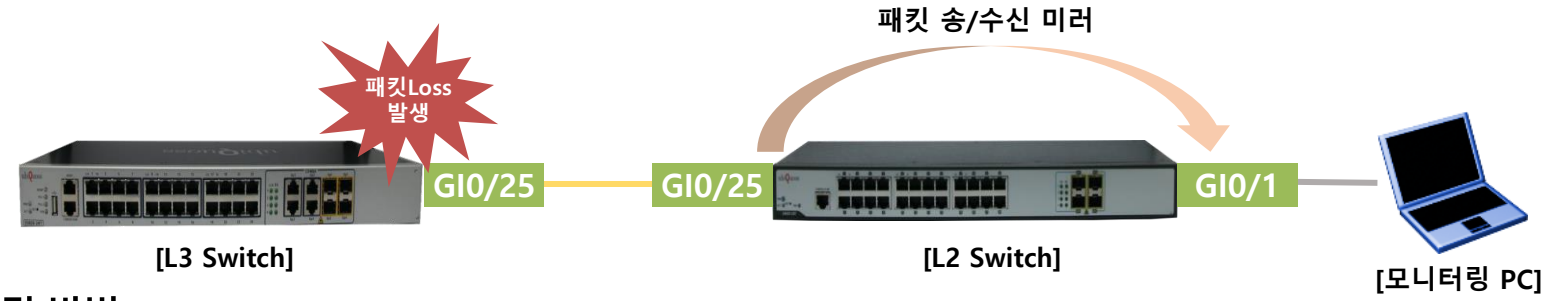
CRC발생 확인

```
[확인방법#1]
Switch# show interface gi0/25                    (특정 포트 CRC발생 확인)
Giga0/1 is up, line protocol is up (connected)
--- 중략 ---
    324 CRC, 0 oversized, 0 dropped              (CRC Count 증가여부 확인)

[확인방법#2]
Switch# show interface | include CRC             (전체 포트 CRC발생 확인)
    0 CRC, 0 oversized, 0 dropped
    --- 중략 ---
    324 CRC, 0 oversized, 0 dropped              (CRC Count 증가여부 확인)
    0 CRC, 0 oversized, 0 dropped

[확인방법#3]
Switch# clear counters                 (CRC Count 초기화 후 재 조회시 지속 증가여부 확인)
Switch# show interface | include CRC

[조치방법]
1) CRC발생 포트 Connector 탈/실장
2) 대국장비 모듈 교체, CRC발생 장비 모듈 교체
3) CRC발생 포트 연결 케이블 교체
```

7. 패킷 Loss 발생시 확인 및 조치방법

패킷 Loss 발생

- 장비 운용중 패킷 Loss 발생시 Mirror 통한 점검 가능
- 포트 기준 TX/RX 패킷을 모니터링 PC로 미러하여 패킷 Loss 여부 등 특이사항 확인



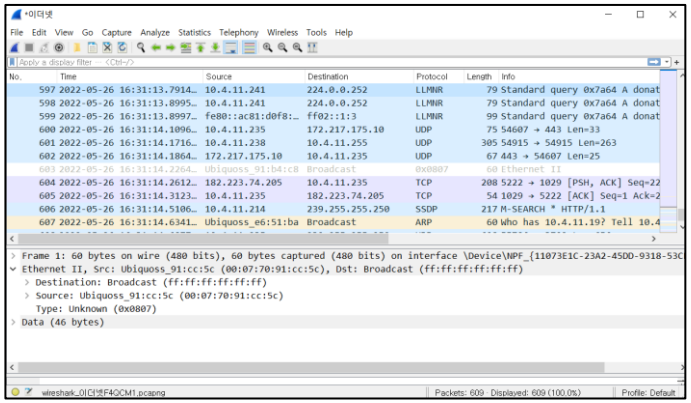
미러링 방법

[설정방법]

```
Switch(config)# interface gi 0/1                                    (모니터링 PC 연결 interface 진입)
Switch(config-if-Giga0/1)# mirror interface gi0/25 direction both   (Gi0/25 포트 송/수신 패킷 미러링 설정)
Switch(config-if-Giga0/1)# mirror interface gi0/25 direction receive  (Gi0/25 포트 수신 패킷 미러링 설정)
Switch(config-if-Giga0/1)# mirror interface gi0/25 direction transmit (Gi0/25 포트 송신 패킷 미러링 설정)
```

[확인방법]

Wireshark 프로그램 실행하여 미러 결과 확인



8. 부트모드 진입시 확인 및 조치방법

부트모드 진입

- OS 손상 등으로 정상 부팅상태가 아닌 부트모드 진입상태
- TFTP를 이용한 임시 부팅으로 복구 후 손상된 OS 삭제 후 재업로드 진행

부트모드 복구

```
[복구방법]
1. 콘솔 연결 및 UTP MNG 포트 연결 (MNG 포트가 없는 제품은 GI0/1 연결)
BOOTLOADER 2.1.6 version
== 중략 ==
Hit Ctrl+C key to stop autoboot:  2
Bootloader >>                                   (정상 부팅이 아닌 부트모드 진입 상태 확인)

2. 부트모드 프롬프트에서  IP/NETMASK/OS IMAGE를 지정
Bootloader >> setenv ipaddr 10.4.11.100         (SWITCH IP)
Bootloader >> setenv netmask 255.255.255.0
Bootloader >> setenv serverip 10.4.11.200       (TFTP 서버 PC IP)
Bootloader >> setenv bootfile UbiEnt.r264.bin   (TFTP 서버 디렉토리 저장된 OS IMAGE NAME)
Bootloader >> saveenv

3. 휘발성 메모리에 OS를 다운로드 및 부팅 실행
Bootloader >> run boot_from_tftp
Using egiga0 device
TFTP from server 10.4.11.200; our IP address is 10.4.11.100
Filename 'UbiEnt.r264.bin'.
Load address: 0x2000000
Loading: ###################################################################

4. 장비가 정상적으로 부팅 되는지 확인한다. 정상부팅 후 OS를 삭제하고 재 Upgrade를 한다
Switch login:
```

9. 원격 접속 불가

ACL및 방화벽 등 원격접속 차단에 의한 접속 불가

- 스위치 원격접속 ACL 설정에 의한 통신불가 여부 확인필요
- 방화벽 원격접속 정책 차단 or 접근 대역 ACL 차단에 의한 통신불가 여부 확인필요

원격 접속 통신 확인 및 조치방법

[원격 접속 설정 확인]

```
Switch(config)# service ssh                                  (원격 접속 활성화)
Switch(config)# ip ssh port 2222                             (SSH Port 변경)
Switch(config)# access-list 22 permit host 10.4.11.235       (SSH ACL에 접속 IP대역 허용여부 확인)
Switch(config)# access-list 22 deny any
Switch(config)# ip option ssh-acl access-group 22            (SSH ACL 활성화)
```

[SSH 통신 확인]

```
Switch#tcpdump interface any port 2222
16:21:54.692034  In 98:83:89:98:fd:97 ethertype IPv4 (0x0800), length 72: 10.4.11.235.2304 > 10.4.11.44.2222: Flags [S], seq 2579343963, win 65520, options [mss
1260,nop,wscale 8,nop,nop,sackOK], length 0
16:21:54.692768 Out 70:30:5d:35:fd:24 ethertype IPv4 (0x0800), length 68: 10.4.11.44.2222 > 10.4.11.235.2304: Flags [S.], seq 3650586713, ack 2579343964, win 14600, options
[mss 1460,nop,nop,sackOK,nop,wscale 6], length 0
```

(TCPDUMP로 port 2222 패킷 정상 송/수신 여부 확인 → 수신 패킷이 없는 경우, 상위망에서 ACL 차단 or 방화벽 차단 여부 확인필요)

```
Switch#tcpdump interface any port 2222
16:29:50.405211  In 98:83:89:98:fd:97 ethertype IPv4 (0x0800), length 72: 10.4.11.235.2384 > 10.4.11.44.2222: Flags [S], seq 3489403285, win 65520, options [mss
1260,nop,wscale 8,nop,nop,sackOK], length 0
16:29:51.418786  In 98:83:89:98:fd:97 ethertype IPv4 (0x0800), length 72: 10.4.11.235.2384 > 10.4.11.44.2222: Flags [S], seq 3489403285, win 65520, options [mss
1260,nop,wscale 8,nop,nop,sackOK], length 0
```

(TCPDUMP로 port 2222 패킷 정상 송/수신 여부 확인 → 송신 패킷이 없는 경우, 장비 ACL 차단여부 확인 필요)

끊임없이 혁신하는 글로벌 네트워크 전문기업 **UBIQUOSS**

ubiQuoss

www.ubiquoss.com

☎ Call Center(24 Hour) : TEL. 1577-9550 I FAX.031-8017-1183

경기도 성남시 분당구 판교로 255번길 68(삼평동 616)