

수업 내용 정리 보고서

작성일: 2026년 6월 24일

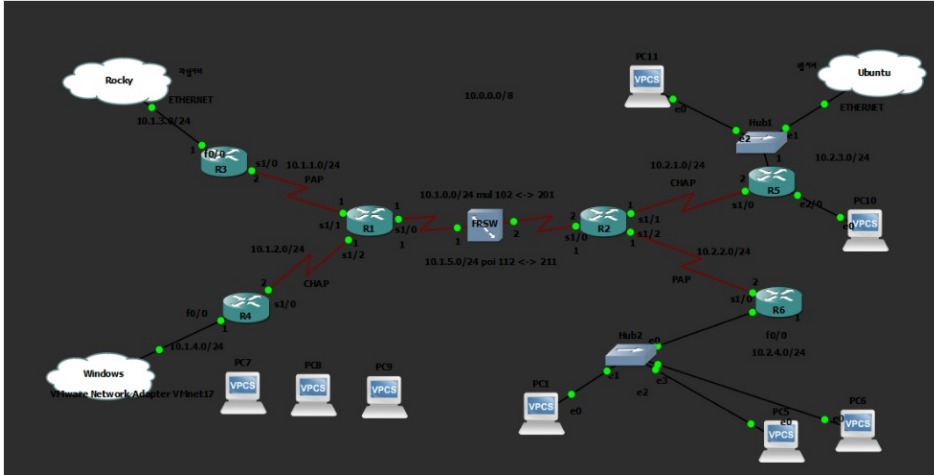
챕터 구성

1. WAN/LAN 인터페이스 및 L2 프로토콜 동작 원리
2. L2 인증 프로토콜의 보안성 비교 분석(PAP vs CHAP)
3. ACL을 이용한 네트워크 트래픽 제어 및 보안 정책 적용
4. 네트워크 연결성 검증 및 운영 트러블슈팅 체크리스트

WAN/LAN 인터페이스 및 L2 프로토콜 동작 원리

네트워크를 구성하는 물리적/논리적 환경은 통신 범위와 연결 방식에 따라 크게 **WAN(Wide Area Network)**과 **LAN(Local Area Network)**으로 구분됩니다. WAN 환경에서는 주로 **Serial Line**이 사용되어 라우터 간 1:1 연결(Point-to-Point)을 수행하며, 데이터를 1비트씩 순차적으로 전송하는 특징을 가집니다. 반면, LAN 환경에서는 **Ethernet Line**이 사용되어 스위치나 허브를 통해 다수의 기기가 연결되는 다중 접속(Multi-Access) 환경을 구축하며, MAC 주소를 기반으로 데이터를 프레임(Frame) 단위로 스위칭합니다.

본 실습에서는 이러한 다양한 환경을 결합한 혼합 네트워크 토폴로지를 구성하여 각 계층의 동작을 분석합니다. 전체적인 구조는 라우터(R1~R6)와 Frame Relay 스위치(FRSW1)를 중심으로 구성되어 있습니다.



연결 방식 중 하나인 **Frame Relay**는 물리적으로는 다중 접속(Multi-Access)을 지원하지만, 브로드캐스트 신호가 사방으로 퍼지지 않는 **NBMA(Non-Broadcast Multi-Access)** 기술입니다. 이를 효율적으로 운영하기 위해 하나의 물리적 Serial 회선을 논리적으로 여러 개로 분할한 **PVC(Permanent Virtual Circuit)**를 사용하며, 각 가상 회선은 **DLCI(Data-Link Connection Identifier)**라는 2계층 주소로 식별됩니다.

실습에서는 물리 인터페이스(Serial 1/0)를 **Sub-Interface**로 쪼개어 관리합니다. 예를 들어, R1의 Serial 1/0 인터페이스를 논리적으로 분할하여 각각 다른 DLCI를 할당하는 설정 과정을 확인합니다. R1에서 서브 인터페이스 생성 후 IP 주소를 할당하고, Frame Relay 명령어를 통해 특정 DLCI를 매핑하는 절차를 수행합니다.

실습 화면 해석: R1 서브 인터페이스 및 FR 설정

- 명령어 수행: interface s1/0.12를 통해 서브 인터페이스를 생성하고 ip add 1.1.1.1 255.255.255.0로 주소를 부여함.
- FR 매핑: frame-relay interface-dlci 102 명령을 사용하여 해당 서브 인터페이스를 DLCI 102번과 연결함.

```
R1(config)#int s1/0
R1(config-if)#no ip add
R1(config-if)#int s1/0.12
R1(config-subif)#ip add 1.1.1.1 255.255.255.0
R1(config-subif)#fra
R1(config-subif)#frame
R1(config-subif)#frame-relay inte
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#
```

Frame Relay는 NBMA 특성을 가지므로, 정적(Static) 매핑 시 브로드캐스트가 가능하도록 map ip [IP] [DLCI] b와 같이 'b(broadcast)' 옵션을 반드시 추가해야 합니다. R1에서 멀티포인트(Multi-point) 구조를 구현하기 위해 서브 인터페이스에 여러 DLCI를 바인딩하는 과정을 살펴보면 다음과 같습니다.

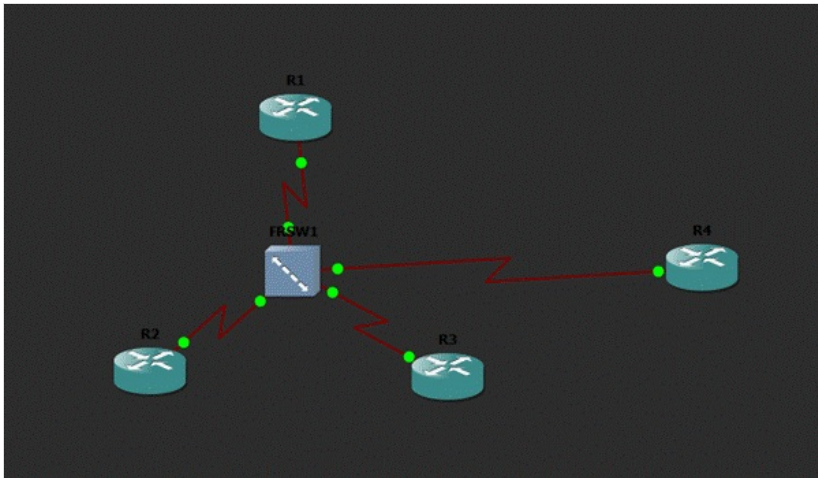
실습 화면 해석: R1 멀티포인트 및 정적 매핑

- 멀티포인트 설정: interface s1/0.21 mul 명령으로 멀티포인트 서브 인터페이스를 생성함.
- 브로드캐스트 옵션 적용: frame-relay map ip 1.1.2.2 112 b 명령에서 끝에 'b'를 붙여 NBMA 환경에서의 통신 효율을 높임.

```
R1(config)#no ip add
% Incomplete command.

R1(config)#int s1/0
R1(config-if)#no ip add
R1(config-if)#int s1/0.12
R1(config-subif)#ip add 1.1.1.1 255.255.255.0
R1(config-subif)#fra
R1(config-subif)#frame
R1(config-subif)#frame-relay inte
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#exit
R1(config-subif)#int s1/0.21 mul
R1(config-subif)#ip add 1.1.2.1 255.255.255.0
R1(config-subif)#frame
R1(config-subif)#frame-relay map ip 1.1.2.2 112 b
R1(config-subif)#
```

설정이 완료된 후에는 실제 매핑 상태를 확인해야 합니다. show frame-relay map 명령을 통해 설정한 IP 주소와 DLCI 번호가 올바르게 매칭되어 'active' 상태인지 점검합니다.



인터페이스 활성화 시 주의할 점은 물리 인터페이스의 상태 변화입니다. no shutdown 명령을 통해 인터페이스를 활성화하면, 시스템 로그를 통해 'Interface Serial1/0, changed state to up'과 같은 메시지가 출력되며 물리 계층(L1)이 정상적으로 올라왔음을 알려줍니다. 참고로 Loopback과 같은 가상 인터페이스는 별도의 no shut 명령 없이도 생성 즉시 활성화됩니다.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#enc ppp
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#end
R1#wr
Building configuration...
[OK]
R1#
*Jun 23 10:17:51.459: %SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#no shut
R1(config-if)#
*Jun 23 10:18:33.407: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config-if)#end
R1#
*Jun 23 10:18:33.407: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administrative State Down
R1#
*Jun 23 10:18:34.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
*Jun 23 10:18:34.847: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#ping 1.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/36 ms
R1#
```

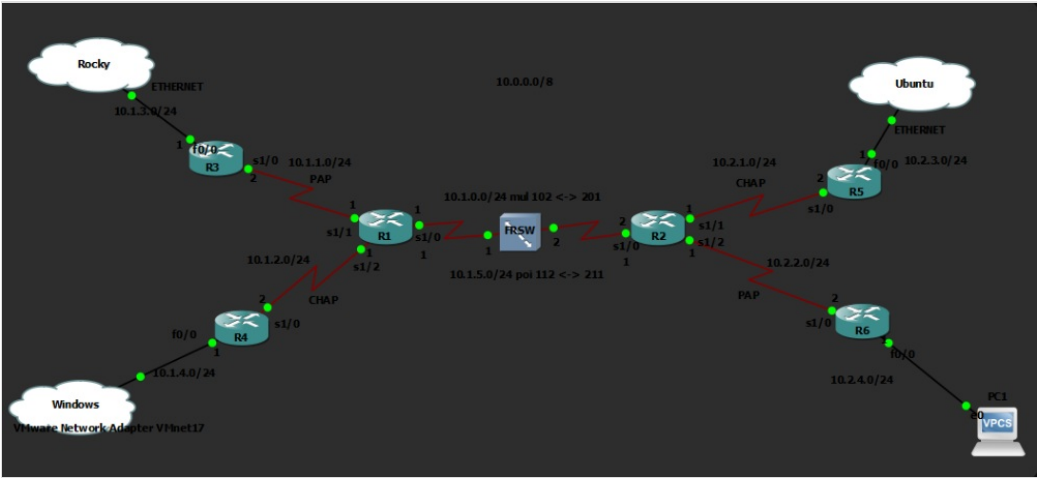
L2 인증 프로토콜의 보안성 비교 분석(PAP vs CHAP)

PPP(Point-to-Point Protocol) 환경에서는 인접한 라우터 간의 연결을 허용하기 위해 2계층 인증 절차를 거칩니다. 이 인증은 종단 간(End-to-End) 전체 경로에 대해 수행되는 것이 아니라, 물리적으로 직접 연결된 인접 장비 간의 국지적(Local) 검증 절차입니다. 따라서 R3과 R6가 통신한다고 해서 두 장비 사이에 직접적인 사용자 계정 정보를 공유할 필요는 없습니다.

인증 방식은 크게 PAP(Password Authentication Protocol)와 CHAP(Challenge Handshake Authentication Protocol)로 나뉩니다.

구분	PAP (Password Authentication Protocol)	CHAP (Challenge Handshake Authentication Protocol)
인증 방식	2-way handshake (ID/PW 전송)	3-way handshake (Challenge-Response)
보안성	낮음 (평문 전송)	높음 (해시/다이제스트 활용)
취약점	스니핑 시 ID와 Password가 그대로 노출됨.	원본 비밀번호가 네트워크에 흐르지 않음.

실습 토폴로지에서는 PPP와 Frame Relay가 혼합된 환경을 구성하여 각 구간별 인증 동작을 분석합니다.



먼저 보안이 취약한 **PAP** 방식의 설정과 패킷을 확인합니다. R2에서 상대방(R1)의 계정을 생성하고, 자신의 ID와 Password를 평문으로 보내도록 설정합니다.

실습 화면 해석: PAP 설정 및 스니핑 취약점 확인

- **설정 단계:** `ppp authentication pap`로 인증 방식을 지정하고, `ppp pap sent-username R2 password cisco`를 통해 전송할 정보를 입력함.
- **취약점 발견:** 패킷 캡처 결과, 'Authenticate-Request' 메시지 안에 Password='cisco'와 같이 비밀번호가 **평문(Plain text)**으로 적나라하게 노출되는 것을 확인할 수 있습니다.

```

R2(config)#username R1 password cisco
R2(config)#int s1/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password cisco
R2(config-if)#
*Jun 23 10:29:37.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2(config-if)#

```

7	10.633329	N/A	N/A	PPP LCP	16 Echo Request
8	14.804944	N/A	N/A	PPP LCP	18 Configuration Request
9	14.820254	N/A	N/A	PPP LCP	18 Configuration Request
10	14.820254	N/A	N/A	PPP LCP	18 Configuration Ack
11	14.835006	N/A	N/A	PPP LCP	18 Configuration Ack
12	14.835006	N/A	N/A	PPP PAP	17 Authenticate-Request (Peer-ID='R2', Password='cisco')
13	14.850235	N/A	N/A	PPP PAP	17 Authenticate-Request (Peer-ID='R1', Password='cisco')
14	14.850235	N/A	N/A	PPP PAP	9 Authenticate-Ack (Message='')
15	14.865410	N/A	N/A	PPP PAP	9 Authenticate-Ack (Message='')
16	14.865410	N/A	N/A	PPP IP...	14 Configuration Request
17	14.880530	N/A	N/A	PPP IP...	14 Configuration Request
18	14.880530	N/A	N/A	PPP IP...	14 Configuration Ack
19	14.880530	N/A	N/A	PPP CD...	8 Configuration Request

반면, **CHAP** 방식은 훨씬 안전합니다. R3에서 CHAP를 설정하면, 상대방(R4)이 던지는 챌린지(Challenge) 값에 대해 자신의 비밀번호를 해싱(Hashing)하여 응답(Response)합니다. 라우터는 원본 비밀번호를 직접 비교하는 것이 아니라, 계산된 해시 값을 비교하므로 네트워크상에서 비밀번호가 노출되지 않습니다.

실습 화면 해석: CHAP 동작 및 보안성 검증

- **설정 단계:** `ppp authentication chap` 명령을 사용하며, 상대방의 호스트 이름과 사용자 이름이 일치해야 인증이 성공합니다.
- **패킷 분석:** 캡처된 로그를 보면 Challenge와 Response 단계에서 매우 긴 해시 값(예: 0x8988...)이 오가는 것을 볼 수 있으며, 비밀번호 자체는 보이지 않습니다.
- **디버그 확인:** `debug ppp authentication`을 통해 확인한 결과, SUCCESS 메시지와 함께 해시 값 비교를 통한 인증 완료 과정을 실시간으로 모니터링할 수 있습니다.

```

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int s1/0
R3(config-if)#enc ppp
R3(config-if)#ip add 1.1.1.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
*Jun 23 10:42:35.887: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R3(config-if)#
*Jun 23 10:42:35.887: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administra
tive State Down
R3(config-if)#
*Jun 23 10:43:03.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, chan
ged state to up
R3(config-if)#exit
R3(config)#username R4 password cisco
R3(config)#int s1/0
R3(config-if)#ppp authentication chap
R3(config-if)#
*Jun 23 10:47:14.571: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, chan
ged state to down
R3(config-if)#
*Jun 23 10:47:27.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, chan
ged state to up
R3(config-if)#

```

1	0.000000	N/A	N/A	PPP LCP	16 Echo Request
2	3.814666	N/A	N/A	PPP LCP	19 Configuration Request
3	3.830124	N/A	N/A	PPP LCP	19 Configuration Request
4	3.830124	N/A	N/A	PPP LCP	19 Configuration Ack
5	3.845134	N/A	N/A	PPP LCP	19 Configuration Ack
6	3.845134	N/A	N/A	PPP CH...	27 Challenge (NAME='R4', VALUE=0x90092addf6da1f28871ce4daeab8bcb)
7	3.862016	N/A	N/A	PPP CH...	27 Challenge (NAME='R3', VALUE=0xd8ae239a32882e835c108ce0f959f18a)
8	3.862016	N/A	N/A	PPP CH...	27 Response (NAME='R3', VALUE=0x8988b1c999341acc8062ab4f09817ad1)
9	3.877734	N/A	N/A	PPP CH...	27 Response (NAME='R4', VALUE=0x8975f3bb42d81ca453bca4b72281f084)
10	3.877734	N/A	N/A	PPP CH...	8 Success (MESSAGE='')
11	3.892743	N/A	N/A	PPP CH...	8 Success (MESSAGE='')
12	3.892743	N/A	N/A	PPP IP...	14 Configuration Request
13	3.907754	N/A	N/A	PPP CD...	8 Configuration Request
14	3.907754	N/A	N/A	PPP IP...	14 Configuration Request
15	3.907754	N/A	N/A	PPP IP...	14 Configuration Ack
16	3.922681	N/A	N/A	PPP IP...	14 Configuration Ack
17	3.922681	N/A	N/A	PPP CD...	8 Configuration Request
18	3.922681	N/A	N/A	PPP CD...	8 Configuration Ack

```

R4#debug ppp authentication
PPP authentication debugging is on
R4#
*Jun 23 10:51:49.831: Se1/0 PPP: Authorization required
*Jun 23 10:51:49.847: Se1/0 CHAP: 0 CHALLENGE id 3 len 23 from "R4"
*Jun 23 10:51:49.847: Se1/0 CHAP: I CHALLENGE id 9 len 23 from "R3"
*Jun 23 10:51:49.859: Se1/0 CHAP: Using hostname from unknown source
*Jun 23 10:51:49.859: Se1/0 CHAP: Using password from AAA
*Jun 23 10:51:49.859: Se1/0 CHAP: 0 RESPONSE id 9 len 23 from "R4"
*Jun 23 10:51:49.879: Se1/0 CHAP: I RESPONSE id 3 len 23 from "R3"
*Jun 23 10:51:49.879: Se1/0 CHAP: I SUCCESS id 9 len 4
*Jun 23 10:51:49.887: Se1/0 PPP: Sent CHAP LOGIN Request
*Jun 23 10:51:49.891: Se1/0 PPP: Received LOGIN Response PASS
R4#
*Jun 23 10:51:49.891: Se1/0 PPP: Sent LCP AUTHOR Request
*Jun 23 10:51:49.891: Se1/0 PPP: Sent IPCP AUTHOR Request
*Jun 23 10:51:49.891: Se1/0 LCP: Received AAA AUTHOR Response PASS
*Jun 23 10:51:49.891: Se1/0 IPCP: Received AAA AUTHOR Response PASS
*Jun 23 10:51:49.891: Se1/0 CHAP: 0 SUCCESS id 3 len 4
*Jun 23 10:51:49.891: Se1/0 PPP: Sent CDPCP AUTHOR Request
*Jun 23 10:51:49.891: Se1/0 CDPCP: Received AAA AUTHOR Response PASS
*Jun 23 10:51:49.911: Se1/0 PPP: Sent IPCP AUTHOR Request

```

ACL을 이용한 네트워크 트래픽 제어 및 보안 정책 적용

ACL(Access Control List)은 네트워크 인터페이스를 통과하는 트래픽을 허용(Permit)하거나 거부(Deny)하는 방화벽 역할을 수행합니다. ACL은 크게 두 가지 유형으로 나뉩니다.

- **표준 ACL (Standard ACL, 1-99):** 출발지 IP 주소만을 기준으로 트래픽을 제어합니다. 설정이 간단하지만 정밀한 제어가 어렵습니다.
- **확장 ACL (Extended ACL, 100-199):** 출발지/목적지 IP 주소뿐만 아니라 프로토콜(TCP, UDP, ICMP 등)과 포트 번호(Port Number)를 기준으로 정밀하게 제어합니다.

ACL 적용 시 반드시 기억해야 할 핵심 원칙은 다음과 같습니다.

1. **순차적 적용:** ACL은 작성된 순서대로 검사합니다. 상단에서 조건이 일치하면 하단의 규칙은 검사하지 않고 즉시 적용됩니다. 따라서 **좁은 범위(Specific)를 먼저 작성하고, 넓은 범위(General)를 나중에 작성해야** 합니다.
2. **묵시적 거부 (Implicit Deny):** ACL의 맨 마지막에는 눈에 보이지 않는 deny any 규칙이 존재합니다. 즉, 명시적으로 허용(Permit)하지 않은 모든 트래픽은 자동으로 차단됩니다. 실수로 특정 서비스를 막았다면, permit ip any any를 추가하여 나머지 트래픽을 허용해 주어야 합니다.
3. **방향성 (Direction):** 인터페이스의 inbound(들어오는 트래픽) 또는 outbound(나가는 트래픽)를 정확히 지정해야 합니다.

실습에서는 다음과 같은 보안 시나리오를 구현하였습니다.

- **시나리오 1:** Windows PC에서만 특정 파일 저장소(Rocky)에 접근 가능하도록 R3의 인터페이스에 표준 ACL 적용.
- **시나리오 2:** 외부로부터의 SSH(TCP 22) 접속을 차단하기 위해 R5 인터페이스에 확장 ACL 적용.

- 시나리오 3: 특정 서비스(FTP, SMB 등)만 허용하고 나머지 서비스는 차단하도록 R3에 확장 ACL 적용.
- 시나리오 4: 내부망 보호를 위해 R6 인터페이스로 들어오는 모든 트래픽을 차단(Deny Any).

네트워크 연결성 검증 및 운영 트러블슈팅 체크리스트

네트워크 설정 후에는 반드시 물리적/논리적 연결 상태를 단계별로 검증해야 합니다. 단순히 '통신이 된다/안 된다'를 넘어, 어느 계층에서 문제가 발생했는지 파악하는 것이 트러블슈팅의 핵심입니다.

1단계: 인터페이스 및 L2 상태 점검

show ip interface brief 명령을 통해 인터페이스의 상태를 확인합니다.

- Status (L1): up이면 물리적 케이블 연결이 정상이며, administratively down이면 no shutdown 명령이 누락된 것입니다.
- Protocol (L2): up이면 L2 프로토콜(PPP, Frame Relay 등) 매칭이 성공한 것이며, down이면 캡슐화 방식 불일치나 인증 오류를 의심해야 합니다.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 1.23.0.0 255.255.0.0 1.123.0.2
R1(config)#ip route 1.23.0.0 255.255.0.0 1.123.0.3
R1(config)#ip route 1.34.0.0 255.255.0.0 1.123.0.3
R1(config)#ip route 1.43.0.0 255.255.0.0 1.123.0.3
R1(config)#end
R1#sh ip int bri
Building configuration...
[OK]
R1#
*Jun 22 15:07:46.263: %SYS-5-CONFIG_I: Configured from console by console
R1#sh ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
Serial1/0 unassigned YES unset up up
Serial1/0.1234 1.123.0.1 YES manual up up
Serial1/1 unassigned YES unset administratively down down
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
Ethernet2/0 unassigned YES unset administratively down down
Ethernet2/1 unassigned YES unset administratively down down
Ethernet2/2 unassigned YES unset administratively down down
Ethernet2/3 unassigned YES unset administratively down down
SSLVPN-VIF0 unassigned NO unset up up
R1#sh fram
R1#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.2 dlci 102(0x66,0x1860), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.3 dlci 103(0x67,0x1870), static,
broadcast,
CISCO, status defined, active
```

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 1.34.0.0 255.255.0.0 1.123.0.2
R2(config)#ip route 1.43.0.0 255.255.0.0 1.123.0.2
R2(config)#end
R2#sh ip int bri
Building configuration...
[OK]
R2#
*Jun 22 15:06:28.895: %SYS-5-CONFIG_I: Configured from console by console
R2#sh ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
Serial1/0 unassigned YES unset up up
Serial1/0.123 1.23.0.1 YES manual up up
Serial1/0.1234 1.123.0.2 YES manual up up
Serial1/1 unassigned YES unset administratively down down
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
Ethernet2/0 unassigned YES unset administratively down down
Ethernet2/1 unassigned YES unset administratively down down
Ethernet2/2 unassigned YES unset administratively down down
Ethernet2/3 unassigned YES unset administratively down down
SSLVPN-VIF0 unassigned NO unset up up
R2#sh fram
R2#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.3 dlci 201(0xC9,0x3090), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.1 dlci 201(0xC9,0x3090), static,
broadcast,
CISCO, status defined, active
Serial1/0.123 (up): point-to-point dlci, dlci 203(0xCB,0x30B0), broadcast
status defined, active
```

```
R3#sh ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
Serial1/0 unassigned YES unset up up
Serial1/0.123 1.23.0.2 YES manual up up
Serial1/0.134 1.34.0.1 YES manual up up
Serial1/0.143 1.43.0.1 YES manual up up
Serial1/0.1234 1.123.0.3 YES manual up up
Serial1/1 unassigned YES unset administratively down down
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
Ethernet2/0 unassigned YES unset administratively down down
Ethernet2/1 unassigned YES unset administratively down down
Ethernet2/2 unassigned YES unset administratively down down
Ethernet2/3 unassigned YES unset administratively down down
SSLVPN-VIF0 unassigned NO unset up up
R3#sh fram
R3#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.2 dlci 301(0x12D,0x48D0), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.1 dlci 301(0x12D,0x48D0), static,
broadcast,
CISCO, status defined, active
Serial1/0.123 (up): point-to-point dlci, dlci 302(0x12E,0x48E0), broadcast
status defined, active
Serial1/0.134 (up): ip 1.34.0.2 dlci 304(0x13D,0x4C00), static,
broadcast,
CISCO, status defined, active
Serial1/0.143 (up): point-to-point dlci, dlci 314(0x13A,0x4CA0), broadcast
status defined, active
R3#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/16 is subnetted, 4 subnets
C 1.23.0.0 is directly connected, Serial1/0.123
C 1.34.0.0 is directly connected, Serial1/0.134
C 1.43.0.0 is directly connected, Serial1/0.143
C 1.123.0.0 is directly connected, Serial1/0.1234
```

2단계: L2 매핑 및 라우팅 테이블 점검

Frame Relay 환경에서는 show frame-relay map을 통해 DLCI 매핑이 'active' 상태인지 확인하고, 라우터의 show ip route를 통해 목적지 네트워크로 가는 경로가 생성되었는지 확인합니다.

3단계: 종단 간 연결성(End-to-End) 테스트

ping 명령을 통해 실제 데이터 전송이 가능한지 확인합니다. R4에서 다양한 네트워크 대역으로 핑을 보낸 결과, 성공적인 통신과 응답 시간(RTT)을 확인할 수 있습니다.

```
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip route 1.123.0.0 255.255.0.0 1.34.0.1
R4(config)#ip route 1.123.0.0 255.255.0.0 1.42.0.1
R4(config)#ip route 1.23.0.0 255.255.0.0 1.34.0.1
R4(config)#ip route 1.23.0.0 255.255.0.0 1.43.0.1
R4(config)#end
R4#wr
Building configuration...
[OK]
R4#
*Jun 22 15:03:41.779: %SYS-5-CONFIG-I: Configured from console by console
R4#sh ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
Serial1/0 unassigned YES unset up up
Serial1/0.134 1.34.0.2 YES manual up up
Serial1/0.143 1.43.0.2 YES manual up up
Serial1/1 unassigned YES unset administratively down down
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
Ethernet2/0 unassigned YES unset administratively down down
Ethernet2/1 unassigned YES unset administratively down down
Ethernet2/2 unassigned YES unset administratively down down
Ethernet2/3 unassigned YES unset administratively down down
SSLVPN-VIF0 unassigned NO unset up up
R4#sh frame-relay map
Serial1/0.134 (up): ip 1.34.0.1 dcli 403(0x193,0x6430), static, broadcast, CISCO, status defined, active
Serial1/0.143 (up): point-to-point dcli, dcli 413(0x19D,0x64D0), broadcast status defined, active
R4#ping 1.23.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.23.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/55/72 ms
R4#ping 1.23.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.23.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/89/92 ms
```

```
R4#ping 1.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/57/92 ms
R4#ping 1.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.10.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/59/76 ms
R4#ping 1.32.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.32.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/56/64 ms
R4#ping 1.48.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.48.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/66/92 ms
R4#ping 1.64.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.64.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms
R4#ping 1.96.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.96.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
R4#ping 1.112.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.112.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 2.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/77/96 ms
```

```
R4#ping 3.112.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.112.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/157/176 ms
R4#ping 3.96.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.96.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/128/160 ms
R4#ping 3.80.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.80.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/124/144 ms
R4#ping 3.64.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.64.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/107/128 ms
R4#ping 2.64.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.64.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/116/152 ms
R4#ping 2.80.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.80.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/137/156 ms
R4#ping 2.96.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.96.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/76/80 ms
R4#ping 2.112.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.112.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/111/132 ms
```

☑ 운영 트러블슈팅 체크리스트

- 인터페이스 상태: Status가 up인가? (L1 확인)
- 프로토콜 일치: Protocol이 up인가? (L2 캡슐화/인증 확인)
- 인증 오류: PPP 구간에서 CHAP/PAP 설정과 계정 정보가 일치하는가?
- 매핑 오류: Frame Relay의 DLCI와 IP 매핑이 정확하며 broadcast(b) 옵션이 필요한 곳에 적용되었는가?
- ACL 정책: 트래픽이 차단된다면 Implicit Deny에 걸린 것은 아닌가? 규칙의 순서가 올바른가?

- 라우팅: 라우팅 테이블에 목적지 대역이 존재하며, Next-hop IP가 유효한가?