

수업 내용 정리 보고서

작성일: 2026년 6월 24일

챕터 구성

- 데이터 링크 계층 프로토콜의 이해와 구성 (PPP, Frame Relay)
- 2계층 인증 메커니즘의 동작 원리와 보안성 분석 (PAP vs. CHAP)
- ACL을 활용한 네트워크 접근 제어 및 보안 정책 수립
- 네트워크 통합 운영 및 실무 점검 가이드

데이터 링크 계층 프로토콜의 이해와 구성 (PPP, Frame Relay)

네트워크 장비를 연결하는 물리적/논리적 환경은 통신 거리와 연결 방식에 따라 크게 **원거리 통신망(WAN)**과 **근거리 통신망(LAN)**으로 구분됩니다. WAN에서는 주로 **Serial Line**이 사용되며, LAN에서는 **Ethernet Line**이 표준으로 쓰입니다.

1. Serial Line과 Ethernet Line의 비교

구분	Serial Line (직렬 회선)	Ethernet Line (이더넷 회선)
주요 용도	WAN 환경, 라우터 간 1:1 연결	LAN 환경, 내부 네트워크 구성
연결 방식	Point-to-Point (점대점) : 두 기기 간 전용선으로 직접 연결	Multi-Access (다중 접속) : 스위치/허브를 통해 다수 기기 연결
동작 원리	데이터를 1비트씩 순차적으로 전송	프레임(Frame) 단위로 묶어 MAC 주소 기반 스위칭

Serial Line은 1:1 연결이므로 상대방의 MAC 주소를 알 필요가 없으며, 대신 2계층에서 데이터를 안전하게 전달하기 위해 **PPP(Point-to-Point Protocol)**나 **HDLC**와 같은 캡슐화 프로토콜을 사용합니다.

2. Frame Relay와 NBMA 기술

Frame Relay는 물리적으로는 다수의 기기가 접속할 수 있는 다중 접속(MA) 환경을 지원하지만, LAN처럼 브로드캐스트 신호가 사방으로 퍼지지 않는 **NBMA(Non-Broadcast Multi-Access)** 기술입니다. 이를 효율적으로 운영하기 위해 다음과 같은 핵심 개념이 사용됩니다.

- **PVC (Permanent Virtual Circuit)**: 하나의 물리적 Serial 회선을 논리적으로 분할하여 만든 영구 가상 회선입니다. 이를 통해 하나의 물리 포트에 여러 목적지 와 독립적인 1:1 연결을 수립할 수 있습니다.
- **DLCI (Data-Link Connection Identifier)**: Frame Relay 환경에서 가상 회선(PVC)을 식별하기 위한 2계층 주소입니다.
- **IARP (Inverse ARP)**: 이미 알고 있는 2계층 주소(DLCI)를 기반으로 상대방의 3계층 주소(IP)를 자동으로 찾아 매핑하는 프로토콜입니다.

실습에서는 하나의 물리 인터페이스를 여러 개의 논리적 인터페이스로 쪼개는 **Sub-Interface**를 활용하여 가상 회선을 구성하였습니다. R1 라우터에서 Serial 1/0 인터페이스를 분할하고 DLCI 102를 할당하는 과정은 다음과 같습니다.

R1의 Serial 인터페이스에서 IP 주소를 할당하고 서브 인터페이스를 생성하여 DLCI 102를 설정하는 과정입니다.

```
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)#
```

R1의 서브 인터페이스 생성 및 DLCI 102 할당 설정 화면

서브 인터페이스를 통해 Multi-Point 구조를 구현하고, 특정 IP와 DLCI를 매핑하는 **frame-relay map ip** 명령어를 사용합니다. 이때 NBMA 환경이므로 **broadcast (b)** 옵션을 추가하여 통신 효율을 높여야 합니다.

```
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)#
```

R1에서 서브 인터페이스에 IP를 부여하고 DLCI 112를 매핑하는 설정

설정된 가상 회선들이 물리적인 Frame Relay 스위치(FRSW)를 통해 어떻게 연결되는지 토폴로지를 통해 확인할 수 있습니다.

```
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#wr
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
```

FRSW를 중심으로 R1, R2, R3, R4가 연결된 Frame Relay 토폴로지

실습 시 주의사항으로는, 하나의 물리 인터페이스에 여러 개의 DLCI를 바인딩하는 **Multi-Point** 방식과, 하나의 서브 인터페이스당 하나의 DLCI만 할당하는 **Point-to-Point** 방식의 차이를 명확히 이해해야 한다는 점입니다.

2계층 인증 메커니즘의 동작 원리와 보안성 분석 (PAP vs. CHAP)

PPP 프로토콜을 사용하는 구간에서는 인접한 라우터 간의 신뢰성을 확보하기 위해 2계층 인증 절차를 거칩니다. 실습에서는 보안성이 낮은 **PAP**와 보안성이 높은 **CHAP**를 모두 구성하여 그 차이를 분석하였습니다.

1. PAP와 CHAP의 비교 분석

특징	PAP (Password Authentication Protocol)	CHAP (Challenge Handshake Authentication Protocol)
인증 방식	2-Way Handshake	3-Way Handshake (Challenge-Response)
데이터 형태	평문(Plain Text) 전송	해시(Hash/Message Digest) 값 전송
보안성	낮음 (스니핑 시 비밀번호 노출 위험)	높음 (비밀번호 원본이 네트워크에 흐르지 않음)
주요 특징	단순하고 설정이 쉬움	상대방의 Hostname/Username 일치 필요

2. 실습을 통한 보안 취약점 검증

먼저 R2 라우터에서 PAP 인증을 설정하였습니다. `ppp authentication pap` 명령을 통해 인증을 요구하고, 자신의 ID와 패스워드를 상대방에게 전송하도록 설정합니다.

```
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)#
```

R2에서 PAP 인증을 활성화하고 사용자 정보를 설정하는 과정

패킷 캡처 도구를 통해 확인한 결과, PAP 방식은 인증 과정에서 ID와 Password가 암호화되지 않은 **평문 상태**로 네트워크에 노출되는 치명적인 취약점이 확인되었습니다.

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

패킷 캡처를 통해 PAP 인증 시 비밀번호가 평문으로 노출된 결과

반면, CHAP 인증은 보안을 강화하기 위해 3-Way Handshake 방식을 사용합니다. R3와 R4 간의 연결에서 `ppp authentication chap`을 설정하여 동작을 확인하였습니다.

```

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)#

```

R3에서 CHAP 인증을 적용하고 사용자 계정을 생성하는 설정

패킷 캡처를 통해 확인한 CHAP은 비밀번호 자체를 보내는 대신, **Challenge 값에 대한 Response(해시값)**만을 주고받습니다. 따라서 공격자가 패킷을 가로채더라도 원본 비밀번호를 알 수 없습니다.

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=0x90092addf6da1f288717ce4daeab8bcb)
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

CHAP 인증 과정에서 비밀번호 대신 해시값이 교환되는 패킷 캡처 화면

라우터의 debug ppp authentication 명령어를 사용하면 상세한 인증 로그를 볼 수 있습니다. 로그를 분석해보면 라우터가 비밀번호 원본을 비교하는 것이 아니라, 전달받은 해시값을 계산하여 일치 여부를 판단함을 알 수 있습니다.

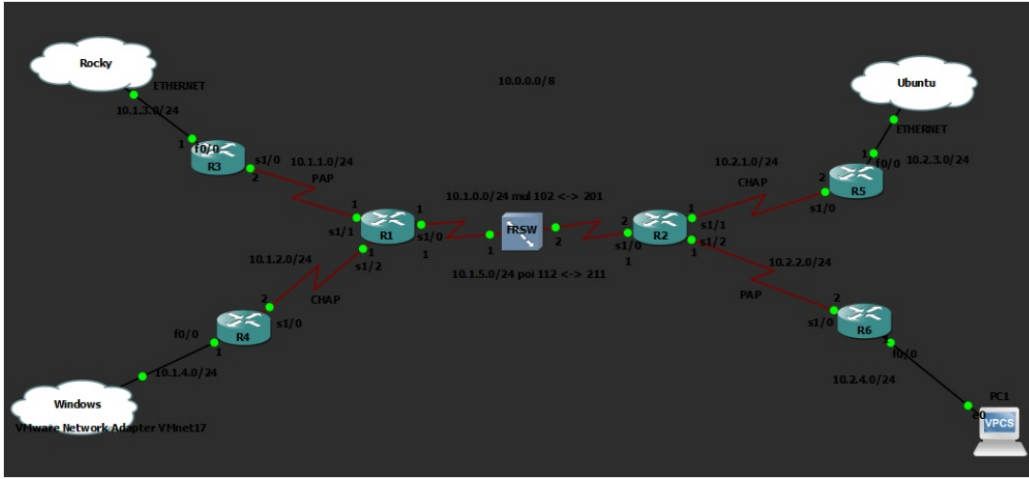
```

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

```

CHAP 인증 동작 시 해시값을 비교하여 성공하는 과정을 보여주는 디버그 로그

이러한 인증 메커니즘은 오직 "해당 구간의 물리적 길을 여는 역할"만을 수행합니다. 즉, 인증은 인접한 장비 간의 국지적(Local) 검증이며, 멀리 떨어진 원격지 라우터의 인증 정보를 대항하지 않습니다.



PPP와 Frame Relay가 혼합된 복합 네트워크 토폴로지 구성도

ACL을 활용한 네트워크 접근 제어 및 보안 정책 수립

ACL(Access Control List)은 라우터를 통과하는 트래픽을 허용(permit)하거나 거부(deny)하는 일종의 방화벽 역할을 수행합니다. 실습에서는 목적과 범위에 따라 표준 ACL과 확장 ACL을 나누어 적용하였습니다.

1. ACL의 종류 및 적용 규칙

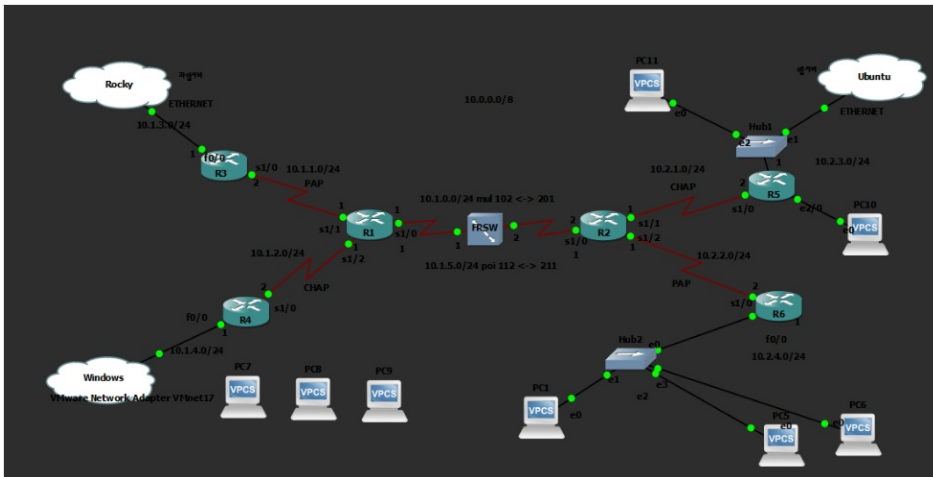
- **Standard ACL (1~99):** 출발지 IP 주소만을 기반으로 트래픽을 제어합니다. 범위가 넓어 정밀한 제어가 어렵습니다.
- **Extended ACL (100~199):** 출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP), 포트 번호(eq 22, 80 등)를 모두 사용하여 정밀하게 제어합니다.

2. 실습 시나리오 및 보안 정책 적용

실습에서는 다음과 같은 구체적인 보안 요구사항을 구현하였습니다.

1. **Windows NI 기반 접근 제어:** 특정 Windows 클라이언트만 Rocky 파일 서버에 접근할 수 있도록 R3의 인터페이스에 Inbound ACL을 적용하였습니다.
2. **서비스별 차단 (SSH, FTP, SMB):** 외부에서 R5 라우터로의 SSH 접속(Port 22)을 차단하거나, 특정 대역에서만 FTP(20, 21) 및 SMB(139, 445) 통신이 가능하도록 확장 ACL을 구성하였습니다.
3. **ICMP(Ping) 차단:** 특정 구간에서 네트워크 탐색을 막기 위해 ICMP 트래픽을 거부하는 정책을 수립하였습니다.

ACL을 적용할 때 가장 주의해야 할 점은 "**묵시적 Deny(Implicit Deny)**"입니다. ACL의 맨 마지막에는 허용되지 않은 모든 것을 차단하는 규칙이 숨겨져 있으므로, 특정 트래픽만 차단하고 나머지는 허용하고 싶다면 반드시 마지막에 `permit ip any any`를 추가해야 합니다.



다양한 호스트와 서버가 연결된 ACL 적용 대상 네트워크 토폴로지

네트워크 통합 운영 및 실무 점검 가이드

네트워크 구축 후에는 구성이 의도한 대로 동작하는지 단계별로 점검해야 합니다. 실습에서 확인된 점검 순서와 주요 명령어는 다음과 같습니다.

1. 인터페이스 및 계층별 상태 점검

가장 먼저 물리적(L1) 연결과 논리적(L2) 프로토콜 연결 상태를 확인합니다. `show ip int bri` 명령어를 사용합니다.

- **Status:** 1계층(물리적) 상태를 의미합니다. `administratively down`이라면 `no shutdown` 명령이 필요합니다.

- **Protocol:** 2계층(논리적) 상태를 의미합니다. L2 프로토콜(PPP, Frame Relay 등)이 서로 매칭되지 않으면 down 상태가 됩니다.

라우터의 인터페이스 상태를 확인하여 물리적/논리적 연결 상태를 점검하는 과정입니다.

```
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 1.23.0.2
R2(config)#ip route 1.43.0.0 255.255.0.0 1.23.0.2
R2(config)#end
R2#wr
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-Vi0 unassigned NO unset up up
R2#sh fram
R2#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.3 dlc1 201(0xC9,0x3090), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.1 dlc1 201(0xC9,0x3090), static,
broadcast,
CISCO, status defined, active
Serial1/0.123 (up): point-to-point dlc1, dlc1 203(0xCB,0x30B0), broadcast
status defined, active
```

show ip int bri 명령을 통한 인터페이스의 Status와 Protocol 상태 확인

Serial 인터페이스의 경우, 물리적 포트 활성화뿐만 아니라 L2 프로토콜이 up 상태인지 반드시 확인해야 합니다.

```
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-Vi0 unassigned NO unset up up
R3#sh fram
R3#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.2 dlc1 301(0x12D,0x48D0), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.1 dlc1 301(0x12D,0x48D0), static,
broadcast,
CISCO, status defined, active
Serial1/0.123 (up): point-to-point dlc1, dlc1 302(0x12E,0x48E0), broadcast
status defined, active
Serial1/0.134 (up): ip 1.34.0.2 dlc1 304(0x130,0x4C00), static,
broadcast,
CISCO, status defined, active
Serial1/0.143 (up): point-to-point dlc1, dlc1 314(0x13A,0x4CAB), 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
```

Serial 인터페이스의 IP 할당 및 L2 프로토콜의 Up 상태 확인

또한, 인터페이스가 shutdown 상태인 경우 no shutdown 명령을 통해 활성화해야 하며, Loopback과 같은 가상 인터페이스는 별도의 활성화 명령이 필요하지 않은 경우가 많습니다.

```
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 Administra
tive State Down
R1#
*Jun 23 10:18:34.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, chan
ged 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#
```

Serial 인터페이스 활성화를 위해 no shutdown 명령을 수행하는 과정

2. 라우팅 및 연결성 검증

L2 연결이 완료되면 show ip route로 라우팅 테이블을 확인하고, ping을 통해 종단 간(End-to-End) 통신을 검증합니다.

라우팅 테이블을 통해 각 네트워크 대역이 어떤 인터페이스를 통해 연결되어 있는지 확인합니다.

```

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 1.43.0.1
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 15:02:41.779: %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 dlc1 403(0x193,0x6430), static,
broadcast
CISCO, status defined, active
Serial1/0.143 (up): point-to-point dlc1, dlc1 413(0x190,0x6400), 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 = 72/80/92 ms

```

show ip route 명령을 통한 라우팅 테이블과 직접 연결된 네트워크 확인

최종적으로 서로 다른 네트워크 대역 간에 ICMP Echo를 전송하여 성공적으로 데이터가 전달되는지 확인합니다.

```

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

```

R4에서 특정 목적지 IP로 Ping을 수행하여 100% 성공하는 결과

```

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

```

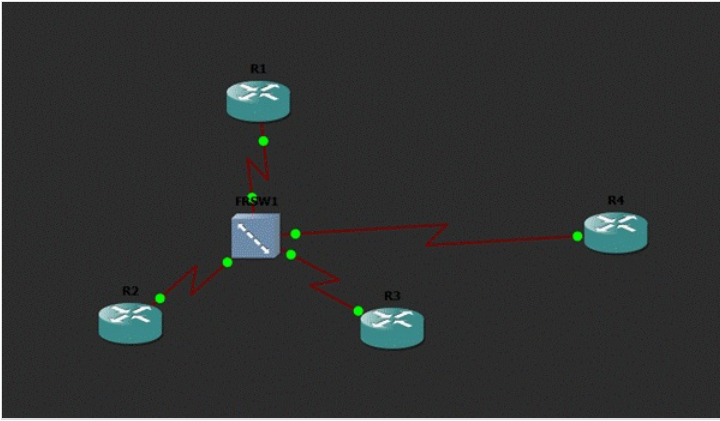
다양한 네트워크 대역으로의 Ping 테스트를 통해 통신 성공을 검증하는 화면

3. 실무 트러블슈팅 체크리스트

통신 장애 발생 시 다음 순서로 점검하십시오.

- Step 1. 물리 계층 점검: show ip int bri에서 Status가 up인지 확인. administratively down이면 no shut 실행.
- Step 2. 데이터 링크 계층 점검: Protocol 상태가 up인지 확인. PPP의 경우 인증(CHAP/PAP) 설정 불일치, Frame Relay의 경우 DLCI/IARP 매핑 오류 확인.
- Step 3. 네트워크 계층 점검: show ip route로 경로 존재 여부 확인. ping 테스트 시 ACL에 의한 차단 여부 검토.
- Step 4. 상세 분석: debug ppp authentication과 같은 명령어를 사용하여 인증 과정의 구체적인 에러 메시지(Challenge/Response 실패 등) 확인.

추가 실습 화면



본문 내용을 보충하는 실습 화면으로, 설정·상태·검증 결과를 함께 확인할 수 있습니다