

# 수업 내용 정리 보고서

작성일: 2026년 6월 24일

## 챕터 구성

- WAN 및 LAN 환경의 계층별 통신 프로토콜 이해
- 이종 프로토콜 연동 메커니즘 및 가상 인터페이스 운용
- ACL을 활용한 트래픽 필터링 및 보안 정책 적용
- 네트워크 구축 및 운영을 위한 실무 점검 가이드

## WAN 및 LAN 환경의 계층별 통신 프로토콜 이해

네트워크를 구성하는 기기들은 연결되는 물리적 거리에 따라 서로 다른 통신 환경을 가집니다. 크게 멀리 떨어진 지점을 연결하는 **WAN(Wide Area Network)** 환경과 근거리의 내부 네트워크를 연결하는 **LAN(Local Area Network)** 환경으로 구분할 수 있습니다. 이 두 환경은 데이터를 전달하는 방식과 주소 체계에서 근본적인 차이를 보입니다.

| 구분    | Serial Line (직렬 회선)                      | Ethernet Line (이더넷 회선)                            |
|-------|------------------------------------------|---------------------------------------------------|
| 주요 용도 | WAN (원거리 통신망), 라우터 간 1:1 연결              | LAN (근거리 통신망), 내부 네트워크 구성                         |
| 연결 방식 | Point-to-Point (점대점): 두 기기 간 전용선으로 직접 연결 | Multi-Access (다중 접속): 스위치나 허브를 통해 다수의 기기 연결       |
| 동작 원리 | 데이터를 1비트씩 순차적으로 전송                       | 프레임(Frame) 단위로 데이터를 묶어 전송하며, MAC 주소를 기반으로 목적지 스위칭 |

WAN 구간에서는 데이터를 안전하게 전달하기 위해 2계층(Data Link Layer)에서 프로토콜 캡슐화를 수행합니다. 이때 가장 대표적인 두 프로토콜은 **HDLC**와 **PPP**입니다.

- HDLC (High-Level Data Link Control):** 국제 표준 프로토콜이지만, 많은 경우 제조사별로 변형되어 사용됩니다. 예를 들어 Cisco 장비는 자체적인 Cisco HDLC를 기본값으로 사용하는데, 이는 인증 기능이 없어 처리가 빠르지만 타사 장비와 연결 시 호환성 문제가 발생할 수 있습니다.
- PPP (Point-to-Point Protocol):** 서로 다른 제조사의 라우터 간 연결 시에도 높은 호환성을 보장하는 표준 프로토콜입니다.
  - LCP (Link Control Protocol):** 링크의 연결 설정, 유지, 해제 및 품질을 모니터링합니다.
  - NCP (Network Control Protocol):** IP, IPX 등 다양한 상위 3계층 프로토콜을 동시에 지원할 수 있도록 돕습니다.

## 이중 프로토콜 연동 메커니즘 및 가상 인터페이스 운용

실제 대규모 네트워크에서는 하나의 물리적 회선에 다양한 프로토콜이 혼재되어 나타납니다. 예를 들어, 라우터 간 직접 연결 구간은 PPP를 사용하고, 중간의 프레임 릴레이(Frame Relay) 구간은 또 다른 프로토콜을 사용하는 식입니다. 이때 핵심은 "계층의 독립성"입니다.

### 1. 2계층 프로토콜의 국지성(Locality)과 3계층 데이터의 보존

데이터가 PPP 구간을 지나 Frame Relay 구간을 거쳐 다시 PPP 구간으로 이동할 때, 3계층(IP 패킷)의 원본 데이터는 전혀 훼손되지 않습니다. 라우터는 유입된 패킷의 2계층 헤더를 해제(De-encapsulation)한 뒤, 다음 목적지로 가기 위한 새로운 2계층 헤더로 재포장(Re-encapsulation)하기 때문입니다.

데이터 흐름 예시:

[PPP 헤더 + ICMP 패킷]  $\rightarrow$  (R1)  $\rightarrow$  [Frame Relay 헤더 + ICMP 패킷]  $\rightarrow$  (R2)  $\rightarrow$  [새로운 PPP 헤더 + ICMP 패킷]

따라서 구간별로 사용하는 2계층 프로토콜이나 인증 방식이 다르더라도, 올바른 3계층 라우팅만 확보된다면 종단 간(End-to-End) 통신은 정상적으로 이루어집니다.

```
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)#
```

### 2. Frame Relay와 NBMA 구조

Frame Relay는 물리적으로는 다수의 기기가 접속할 수 있는 다중 접속(Multi-Access) 환경을 지원하지만, LAN처럼 브로드캐스트 신호가 모든 방향으로 퍼지지 않는 NBMA(Non-Broadcast Multi-Access) 특성을 가집니다. 이를 효율적으로 관리하기 위해 다음과 같은 기술을 사용합니다.

- PVC (Permanent Virtual Circuit): 하나의 물리적 회선을 논리적으로 분할하여 만든 영구 가상 회선입니다.
- DLCI (Data-Link Connection Identifier): Frame Relay 환경에서 특정 PVC를 식별하기 위한 2계층 주소입니다.
- IARP (Inverse ARP): 이미 알고 있는 2계층 주소(DLCI)를 기반으로 상대방의 3계층 주소(IP)를 자동으로 찾아내는 프로토콜입니다.
- Sub-Interface: 하나의 물리적 인터페이스를 논리적으로 쪼개어(예: s1/0.12) 여러 개의 가상 회선을 생성하는 방식입니다.

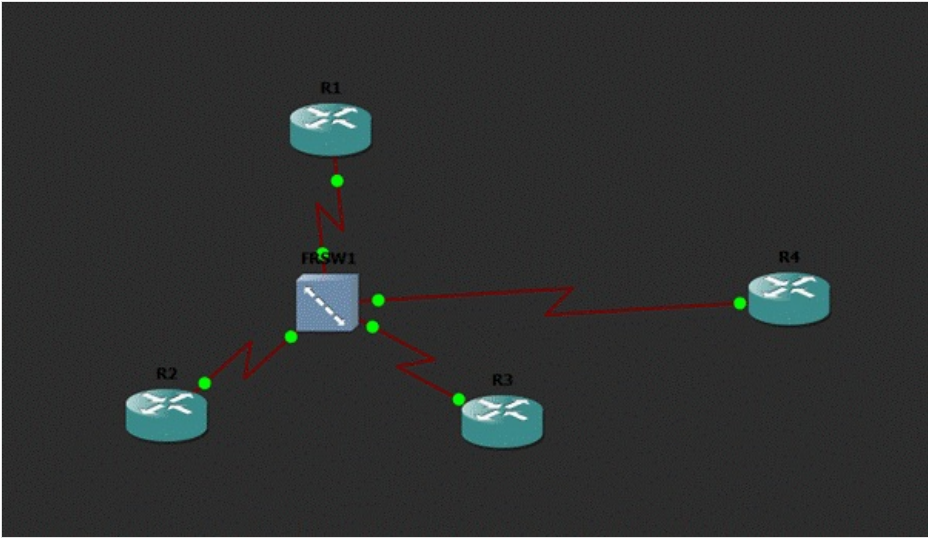
```
R1
R1(config)#no ip add
% Incomplete command.

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)#
```

### 3. 인증 메커니즘: PAP vs CHAP

PPP 연결 시 보안을 위해 인증 절차를 거칩니다. 인증 방식에 따라 보안 수준이 극명하게 갈립니다.

- PAP (Password Authentication Protocol): ID와 패스워드를 평문(Plain text)으로 전송합니다. 스니핑 공격 시 계정 정보가 그대로 노출되므로 매우 취약합니다.
- CHAP (Challenge Handshake Authentication Protocol): 패스워드를 직접 보내지 않고, 단방향 해시(Hash) 처리된 값을 교환합니다. 라우터는 해싱된 결과값을 비교하여 인증하므로, 패킷이 탈취되어도 원본 비밀번호를 복원할 수 없어 안전합니다.



# ACL을 활용한 트래픽 필터링 및 보안 정책 적용

네트워크 보안의 핵심은 특정 트래픽만을 허용하거나 차단하는 **ACL(Access Control List)** 설정입니다. ACL은 크게 두 가지 유형으로 나뉩니다.

| 구분     | Standard ACL (1-99) | Extended ACL (100-199)                     |
|--------|---------------------|--------------------------------------------|
| 필터링 기준 | 출발지 IP 주소 기반        | 출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP 등), 포트 번호 기반 |
| 정밀도    | 낮음 (단순 차단/허용)       | 높음 (서비스별 세밀한 제어 가능)                        |

## 실무 적용 시나리오 및 명령어 구조

ACL을 적용할 때는 `access-list` 명령어로 규칙을 먼저 정의한 후, `ip access-group` 명령어를 통해 특정 인터페이스의 **inbound(유입)** 또는 **outbound(유출)** 방향에 바인딩해야 합니다.

### 시나리오 1: 특정 서비스 접근 제어 (Extended ACL)

특정 서버로의 SSH(22번 포트) 접속을 외부에서 차단하고, 내부의 특정 네트워크(10.1.4.0/24)에서만 FTP(20, 21번 포트) 및 SMB(139, 445번 포트) 서비스가 가능하도록 설정하는 예시입니다.

```
! 외부의 SSH 접속 차단
access-list 100 deny tcp any any eq 22
access-list 100 permit ip any any

! 특정 대역에서만 FTP/SMB 허용 및 나머지 차단
access-list 100 permit tcp 10.1.4.0 0.0.0.255 10.1.3.0 0.0.0.255 eq 21
access-list 100 deny tcp any any eq 21
access-list 100 permit ip any any

! 인터페이스에 적용
interface s1/0
 ip access-group 100 in
```

### 시나리오 2: 방향성 제어 (Outbound ACL)

내부 사용자가 외부의 특정 사이트(HTTP, DNS)에 접속하지 못하도록 인터페이스의 나가는 방향(outbound)에 정책을 적용할 수 있습니다.

```
! HTTP(80) 및 DNS(53) 차단
access-list 100 deny tcp any any eq 80
access-list 100 deny udp any any eq 53
access-list 100 permit ip any any

interface e2/1
 ip access-group 100 out
```

```
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
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
```

# 네트워크 구축 및 운영을 위한 실무 점검 가이드

---

네트워크 구축 후 통신이 되지 않는다면, 다음의 단계별 체크리스트를 통해 문제의 원인을 파악해야 합니다.

## 1. 인터페이스 상태 및 계층별 점검 (show ip int bri)

가장 먼저 수행해야 할 명령어입니다. 출력 결과에서 **Status**와 **Protocol**을 구분하여 판단합니다.

- **Status (1계층 - 물리적 연결):** administratively down으로 표시된다면, 해당 인터페이스가 shutdown 상태인 것입니다. no shutdown 명령어로 활성화해야 합니다.
- **Protocol (2계층 - 논리적 연결):** Status는 up인데 Protocol이 down이라면, L2 프로토콜 매칭 오류(예: 한쪽은 HDLC, 한쪽은 PPP)이거나 인증(PAP/CHAP) 실패를 의미합니다.

## 2. 라우팅 및 가상 회선 점검

- **Routing Table:** show ip route를 통해 목적지 네트워크로 가는 경로가 존재하는지, Next-hop IP가 올바른지 확인합니다.
- **Frame Relay Map:** show frame-relay map을 통해 DLCI 번호와 매핑된 IP 주소가 실제 물리적 연결 구조와 일치하는지 점검합니다.

## 3. 실무자 오답/오해 포인트

- **"Loopback 인터페이스는 항상 켜져 있다?"**  $\rightarrow$  가상 인터페이스인 Loopback은 생성 시 자동으로 활성화되므로 별도의 no shut 명령어가 필요하지 않습니다.
- **"Frame Relay 스위치는 STP 영향을 받는다?"**  $\rightarrow$  Frame Relay 전용 스위치는 일반 Ethernet 스위치와 동작 방식이 다르므로, STP(Spanning Tree Protocol)가 동작하지 않습니다.
- **"인증 실패 시 상대방의 비밀번호를 알 수 있다?"**  $\rightarrow$  CHAP 방식은 해시값을 사용하므로 로그(debug)를 확인하더라도 원본 비밀번호는 노출되지 않습니다. 반면, PAP는 평문이므로 보안에 주의해야 합니다.