

# 수업 내용 정리 보고서

## 챕터 구성

1. 네트워크 인터페이스 기본 및 동작 원리
2. WAN L2 프로토콜 및 캡슐화 메커니즘
3. 접근 제어 리스트(ACL) 설정 및 운영
4. 네트워크 통신 및 보안 실무 점검



# 네트워크 인터페이스 기본 및 동작 원리

네트워크 장비가 데이터를 주고받기 위해서는 물리적인 연결뿐만 아니라, 해당 연결이 논리적으로 활성화되어 있어야 합니다. 인터페이스의 상태를 이해하는 것은 네트워크 트러블슈팅의 첫걸음입니다.

## 1. 물리적/논리적 연결의 구분

네트워크 기기를 연결하는 환경은 통신 범위와 방식에 따라 크게 **Serial**과 **Ethernet**으로 구분됩니다.

| 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 | <b>Point-to-Point (점대점)</b> : 두 기기 간 전용선으로 직접 연결 | <b>Multi-Access (다중 접속)</b> : 스위치/허브를 통해 다수 기기 연결 |
| 식별 방식 | 상대방이 명확하여 복잡한 주소 체계 불필요                          | <b>MAC 주소</b> 를 기반으로 목적지 스위칭 수행                   |

\* 해석: Serial은 주로 멀리 떨어진 라우터끼리 직접 연결할 때 사용하며, Ethernet은 근거리에서 여러 대의 PC나 서버를 묶을 때 사용합니다.

## 2. 인터페이스 상태 확인 및 활성화

라우터의 Layer 3(L3) 포트는 보안과 자원 관리를 위해 기본적으로 **shutdown**(비활성) 상태로 설정되어 있습니다. 따라서 포트를 사용하려면 반드시 **no shutdown** 명령어를 통해 명시적으로 활성화해야 합니다.

인터페이스의 동작 상태는 **show ip int bri**(show ip interface brief) 명령어를 통해 확인할 수 있으며, 다음 두 가지 지표를 반드시 구분해야 합니다.

- Status (1계층 상태)**: 물리적 연결(Physical Layer)이 정상인지 나타냅니다.
- Protocol (2계층 상태)**: 데이터 링크 계층(Data Link Layer)의 논리적 프로토콜 매칭이 정상인지 나타냅니다.

**실무 포인트**: 만약 Status는 *up*인데 Protocol이 *down*이라면, 물리적 케이블은 연결되었으나 양 끝단의 2계층 프로토콜(예: HDLC vs PPP) 설정이 서로 맞지 않음을 의미합니다.

# WAN L2 프로토콜 및 캡슐화 메커니즘

WAN 구간(Serial Line)에서 데이터를 안전하게 전달하기 위해서는 2계층(Data Link Layer)에서 데이터를 특정 규격으로 감싸는 **캡슐화(Encapsulation)** 프로토콜이 필요합니다.

## 1. 대표적인 WAN 프로토콜 비교

| 프로토콜 | 특징                     | 장단점 및 주의사항                                                           |
|------|------------------------|----------------------------------------------------------------------|
| HDLC | 빠르고 단순한 국제 표준 프로토콜     | 인증/오류 복구 기능이 없어 속도는 빠르나, Cisco 전용 HDLC 사용 시 타사 장비와 호환성 문제가 발생할 수 있음. |
| PPP  | 높은 호환성을 가진 표준 WAN 프로토콜 | LCP(링크 제어)와 NCP(네트워크 제어)를 통해 연결 설정, 품질 모니터링, 다양한 상위 프로토콜 지원 가능.      |

## 2. Frame Relay와 NBMA 환경

Frame Relay는 하나의 물리적 회선을 논리적으로 나누어 사용하는 **NBMA(Non-Broadcast Multi-Access)** 기술입니다. 물리적으로는 여러 기기가 접속할 수 있지만, LAN처럼 브로드캐스트 신호가 전 구간으로 퍼지지 않는 특성을 가집니다.

- **PVC (Permanent Virtual Circuit)**: 물리적 Serial 회선을 논리적으로 분할하여 만든 영구 가상 회선입니다.
- **DLCI (Data-Link Connection Identifier)**: Frame Relay 환경에서 가상 회선을 식별하기 위한 2계층 주소입니다. 실무에서는 관리 편의를 위해 3자리 이하의 숫자를 권장합니다.
- **IARP (Inverse ARP)**: 이미 알고 있는 DLCI(2계층)를 기반으로 상대방의 IP(3계층)를 자동으로 찾아 매핑하는 프로토콜입니다.

## 3. 캡슐화의 독립성과 데이터 흐름

데이터가 여러 구간을 통과할 때, 3계층(IP) 패킷의 원본은 유지되면서 2계층 헤더만 교체됩니다. 이를 **재포장(Re-encapsulation)**이라고 합니다.

[데이터 흐름 예시]

[ PPP 헤더 + ICMP 패킷 ] → (R1) → [ Frame Relay 헤더 + ICMP 패킷 ] → (R2)  
→ [ 새로운 PPP 헤더 + ICMP 패킷 ]

따라서 구간마다 사용하는 2계층 프로토콜이나 인증 방식이 다르더라도, 3계층 기반의 종단 간(End-to-End) 통신에는 영향을 주지 않습니다.

# 접근 제어 리스트(ACL) 설정 및 운영

ACL(Access Control List)은 특정 트래픽을 허용(Permit)하거나 차단(Deny)하여 네트워크 보안을 강화하는 도구입니다. 번호 대역에 따라 동작 방식이 완전히 다릅니다.

## 1. ACL 종류 및 차이점

| 종류           | 번호 대역     | 제어 기준                                           |
|--------------|-----------|-------------------------------------------------|
| Standard ACL | 1 ~ 99    | 출발지(Source) IP 주소만 확인하여 차단/허용                   |
| Extended ACL | 100 ~ 199 | 출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP 등), 포트 번호까지 정밀 제어 |

## 2. ACL 설정 절차 (Extended ACL 기준)

정교한 제어를 위해 다음과 같은 순서로 설정을 진행합니다.

- 선행 조건: 차단하고자 하는 서비스의 포트 번호(예: SSH=22, FTP=21)와 트래픽 방향(Inbound/Outbound)을 파악합니다.
- 실행 예시 (외부 SSH 차단 설정):

```
conf t
access-list 100 deny tcp any any eq 22  (모든 곳에서 오는 22번 포트 차단)
access-list 100 permit ip any any      (나머지 모든 IP 통신은 허용)
interface s1/0
ip access-group 100 in                  (인터페이스로 들어오는 트래픽에 적용)
```

- 확인 방법: show access-lists 명령어로 매칭된 패킷 수를 확인합니다.
- 주의사항: Implicit Deny 원칙에 따라, ACL의 마지막에는 "모든 것을 차단"하는 규칙이 숨겨져 있습니다. 따라서 허용할 트래픽은 반드시 명시적으로 permit 해주어야 합니다.

## 3. 주요 보안 시나리오 적용

- 특정 서비스 제한: FTP/SMB(포트 20, 21, 139, 445) 접속을 특정 네트워크 대역에서만 허용하고 나머지는 차단합니다.
- 인바운드/아웃바운드 구분:
  - Inbound: 인터페이스로 들어오는 패킷을 검사 (라우터 내부로 들어오기 전 차단).
  - Outbound: 인터페이스를 통해 나가는 패킷을 검사 (라우터에서 외부로 나가기 전 차단).

## 네트워크 통신 및 보안 실무 점검

---

실습과 이론을 바탕으로 네트워크 운영 시 반드시 점검해야 할 핵심 보안 및 운영 포인트를 정리합니다.

### 1. PPP 인증 방식의 보안성 점검

PPP 연결 시 사용하는 인증 방식에 따라 스니핑(Sniffing, 패킷 도청)에 대한 취약점이 달라집니다.

- **PAP (Password Authentication Protocol):**
  - **방식:** ID와 비밀번호를 **평문(Plain text)**으로 전송합니다.
  - **위험성:** 와이어샤크와 같은 도구로 패킷을 캡처하면 계정 정보가 그대로 노출되므로 매우 위험합니다.
- **CHAP (Challenge Handshake Authentication Protocol):**
  - **방식:** 비밀번호를 직접 보내지 않고, **단방향 해시(Hash)** 처리된 값을 비교합니다.
  - **안전성:** 패킷이 탈취되더라도 원본 비밀번호를 복원할 수 없어 보안성이 높습니다.

### 2. 운영 및 트러블슈팅 체크리스트

현장에서 발생할 수 있는 오해와 문제 해결을 위한 가이드입니다.

- **[ ] 인증의 국지성(Locality) 이해:** PPP 인증(CHAP/PAP)은 인접한 장비 간의 링크를 열기 위한 **구간별 인증**입니다. R3에서 R6까지 통신한다고 해서 R3와 R6가 서로의 비밀번호를 알 필요는 없습니다. 각 구간(R3-R1, R2-R6)의 인증만 성공하면 됩니다.
- **[ ] 인터페이스 활성화 확인:** 통신이 안 될 경우 가장 먼저 **no shutdown**이 되어 있는지, 그리고 **show ip int bri**에서 Status와 Protocol이 모두 **up**인지 확인하십시오.
- **[ ] Frame Relay 매핑 확인:**
  - 정적(Static) 매핑 시에는 **broadcast** 옵션이 필요할 수 있습니다(NBMA 특성).
  - 동적(Dynamic) 매핑은 IARP를 통해 자동으로 이루어지므로 설정 속도가 빠릅니다.
- **[ ] ACL 적용 방향 오류:** 트래픽이 막힌다면 ACL이 **in**에 적용되어야 하는지 **out**에 적용되어야 하는지, 그리고 서비스 포트가 정확한지 재검토하십시오.