

수업 내용 정리 보고서

작성일: 2026년 6월 24일

챕터 구성

- WAN/LAN 인터페이스 및 L2 데이터 링크 프로토콜
- L2 인증 프로토콜의 동작 원리와 보안성 분석 (PAP vs CHAP)
- ACL(Access Control List)을 이용한 트래픽 제어 및 보안 정책
- 네트워크 실무 운영 및 설정 점검 가이드

WAN/LAN 인터페이스 및 L2 데이터 링크 프로토콜

네트워크 기기 간의 통신을 위해 물리적, 논리적 환경을 어떻게 구분하고 연결할 것인가?

네트워크 환경은 통신 거리와 연결 범위에 따라 크게 근거리 통신망(LAN)과 원거리 통신망(WAN)으로 구분됩니다. 이를 결정짓는 핵심 요소는 인터페이스의 물리적 특성과 데이터를 전송하는 방식(데이터 링크 계층 프로토콜)입니다.

1. Serial Line vs Ethernet Line

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): 전용선으로 직접 연결	Multi-Access (다중 접속): 스위치/허브를 통해 다수 연결
동작 원리	데이터를 1비트씩 순차적으로 전송	프레임(Frame) 단위로 묶어 MAC 주소 기반 스위칭

Serial 회선은 두 지점 사이가 직접 연결된 1:1 구조이므로, Ethernet과 달리 복잡한 MAC 주소 체계 없이도 상대방을 명확히 구분할 수 있는 특성을 가집니다.

2. WAN 구간의 데이터 링크 프로토콜: HDLC와 PPP

Serial 인터페이스(WAN 구간)에서 데이터를 안전하게 전달하기 위해 2계층(Data Link Layer)에서 사용하는 대표적인 캡슐화 프로토콜입니다.

- **HDLC (High-Level Data Link Control)**: 점대점 및 다중 점 링크를 위한 국제 표준입니다. 인증이나 오류 복구 같은 복잡한 기능이 생략되어 있어 처리 속도가 빠르다는 장점이 있습니다. 다만, Cisco 장비는 자체적으로 수정한 *Cisco HDLC*를 기본값으로 사용하는 경우가 많아, 타사 장비와 연결 시 호환성 문제가 발생할 수 있습니다.
- **PPP (Point-to-Point Protocol)**: 서로 다른 제조사의 라우터 간 연결 시 가장 널리 쓰이는 호환성 높은 표준 프로토콜입니다.
 - **LCP (Link Control Protocol)**: 링크의 연결 설정, 유지, 해제 및 품질 모니터링을 담당합니다.
 - **NCP (Network Control Protocol)**: IP, IPX 등 다양한 상위 3계층 프로토콜을 동시에 지원하도록 돕습니다.

3. Frame Relay와 NBMA 환경

Frame Relay는 하나의 물리적 Serial 회선을 논리적으로 여러 개로 분할하여 사용하는 **PVC(Permanent Virtual Circuit, 영구 가상 회선)** 기술을 사용합니다. 이는 물리적으로는 다중 접속(MA)을 지원하지만, LAN처럼 브로드캐스트가 사방으로 퍼지지 않는 **NBMA(Non-Broadcast Multi-Access)** 특성을 가집니다.

- **DLCI (Data-Link Connection Identifier)**: Frame Relay 환경에서 가상 회선(PVC)을 식별하기 위한 2계층 주소입니다. 실무에서는 관리 편의를 위해 통상 3자리 이하의 숫자를 사용합니다.
- **IARP (Inverse ARP)**: 일반 ARP가 IP로 MAC을 찾는 것과 반대로, 이미 알고 있는 2계층 주소(DLCI)를 기반으로 상대방의 3계층 주소(IP)를 자동으로 찾아 매핑하는 프로토콜입니다.

4. [실습] 서브 인터페이스를 이용한 가상 회선 구성

물리 인터페이스 하나를 논리적으로 쪼개어 여러 개의 가상 회선을 효율적으로 관리하기 위해 서브 인터페이스(Sub-Interface)를 활용합니다.

실습 목표: 하나의 Serial 인터페이스를 서브 인터페이스로 분할하고, Frame Relay를 통해 1:1 및 다중 접속(Multi-point) 구조를 구현한다.

1. **선행 조건**: 물리 인터페이스의 IP를 제거하고 활성화 상태를 확인한다.
2. **수행 단계**:
 - 서브 인터페이스 생성 (예: interface s1/0.12)
 - IP 주소 할당 및 Frame Relay 설정
 - **Static 매핑**: frame-relay map ip [상대IP] [DLCI] 명령어를 사용한다. 이때 NBMA 환경이므로 broadcast 옵션을 추가하여 통신 범위를 확장한다.
 - **Multi-point 매핑**: 하나의 서브 인터페이스에 여러 개의 DLCI를 바인딩하여 1:N 구조를 구현한다.

결과 확인: show frame-relay map 명령어를 통해 설정된 DLCI와 IP의 매핑 상태가 active인지 확인한다.

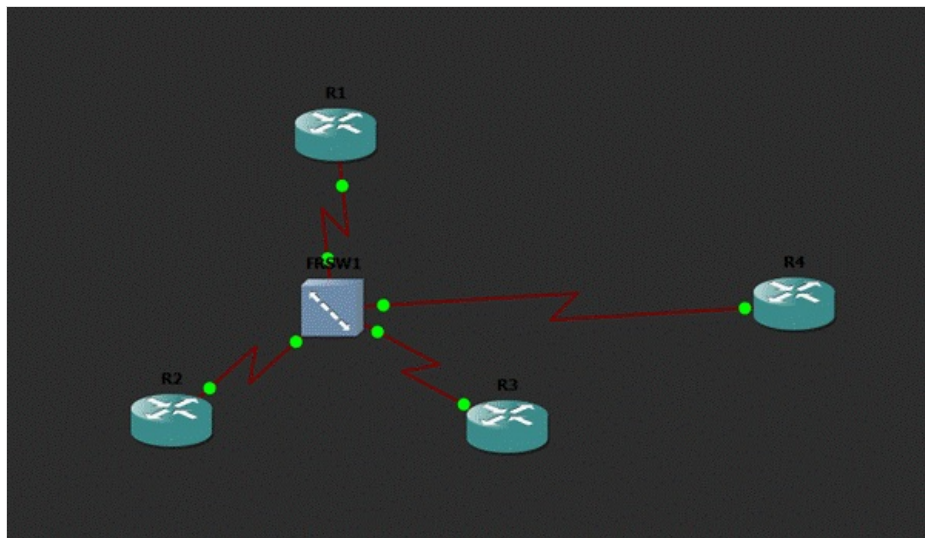
```
R1(config)#int s1/0
R1(config-if)#no ip add
R1(config-if)#int s1/0.12
R1(config-subif)#ip add 1.1.1.1 255.255.255.0
R1(config-subif)#fra
R1(config-subif)#frame
R1(config-subif)#frame-relay inte
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#
```

서브 인터페이스를 생성하고 DLCI 102를 할당하는 설정 과정이다.

```
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)#
```

하나의 서브 인터페이스에 여러 DLCI를 매핑하는 Multi-point 설정과 broadcast 옵션 적용 사례이다.



Frame Relay 스위치(FRSW1)를 중심으로 R1, R2, R3, R4가 연결된 물리적 토폴로지이다.

```
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
```

R1의 인터페이스 상태(Status: up, Protocol: up)와 Frame Relay 매핑 정보를 확인하는 결과이다.

```

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
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

```

R2의 인터페이스 상태와 DLCI 201, 203을 통한 매핑 현황이다.

```

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(0x130,0x4C00), 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

```

R3의 인터페이스 상태 및 라우팅 테이블을 통해 직접 연결된 네트워크 대역을 확인하는 과정이다.

L2 인증 프로토콜의 동작 원리와 보안성 분석 (PAP vs CHAP)

두 장비 간의 연결을 활성화하기 위해 사용하는 2계층 인증은 얼마나 안전한가?

PPP 프로토콜을 사용할 때, 인접한 장비 간의 신뢰성을 확인하기 위해 인증 과정을 거칩니다. 이는 물리적으로 연결된 링크를 활성화하기 위한 **국지적(Local)** 검증 절차입니다.

1. PAP vs CHAP 비교

특징	PAP (Password Authentication Protocol)	CHAP (Challenge Handshake Authentication Protocol)
인증 방식	2-way handshake (단순 인증)	3-way handshake (챌린지-응답 방식)
전송 데이터	ID와 Password를 평문(Plain text) 으로 전송	해시(Hash) 처리된 값을 전송
보안성	매우 낮음 (스니핑에 취약)	높음 (비밀번호 원본 노출 안 됨)

2. [실습] 인증 메커니즘 분석 및 보안 취약점 확인

실습 목표: PAP와 CHAP의 패킷 캡처 결과를 비교하여 암호화 여부를 확인하고, `debug` 명령어로 인증 과정을 분석한다.

- PAP 인증 테스트:** ID와 Password를 설정한 후 패킷을 캡처한다.
- CHAP 인증 테스트:** Hostname과 Password를 설정하고 `ppp debug authentication` 명령어를 통해 로그를 확인한다.

분석 결과:

- PAP의 취약점:** 와이어샤크(Wireshark)와 같은 스니핑 도구로 패킷을 분석하면 사용자의 ID와 Password가 글자 그대로 노출된다.
- CHAP의 보안성:** 패킷에는 비밀번호 자체가 아닌, 해싱된 결과값만 포함된다. 라우터는 수신된 해시값을 자신이 가진 비밀번호로 직접 만든 해시값과 비교하므로, 중간에 패킷이 탈취되더라도 원본 비밀번호를 복원할 수 없다.

PAP와 CHAP의 인증 패킷 흐름을 비교한 분석이다. CHAP의 경우 Challenge와 Response 과정이 나타난다.

CHAP 인증 시 비밀번호가 해싱되어 전송되는 과정을 보여주는 캡처 결과이다.

PAP 인증 시 ID와 Password가 평문으로 그대로 노출되는 치명적인 보안 취약점 사례이다.

중요 원리: 인증의 국지성(Locality)

PPP 인증은 인접한 장비 간의 링크를 열기 위한 절차일 뿐이다. 따라서 R3와 R6가 통신할 때, 중간에 있는 R1이나 R2가 R3와 R6 사이의 인증 정보를 대행하거나 요구하지 않는다. 즉, 통신 양 끝단의 라우터끼리 서로의 계정을 알 필요는 없다.

ACL(Access Control List)을 이용한 트래픽 제어 및 보안 정책

네트워크 트래픽을 특정 조건에 따라 허용하거나 차단하려면 어떻게 해야 하는가?

ACL(Access Control List)은 라우터에서 트래픽을 필터링하는 방화벽 역할을 수행합니다. 특정 호스트, 네트워크 대역, 혹은 특정 프로토콜과 포트 번호를 기준으로 통신을 제어할 수 있습니다.

1. 표준 ACL vs 확장 ACL

구분	표준 ACL (Standard ACL)	확장 ACL (Extended ACL)
번호 범위	1 ~ 99	100 ~ 199
제어 대상	출발지 IP 주소만 기반으로 제어	출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP 등), 포트 번호 기반 제어
주요 용도	단순한 호스트 차단	특정 서비스(SSH, FTP 등)만 선택적 차단/허용

2. ACL 적용 시 반드시 지켜야 할 핵심 규칙

- 순차 적용 원칙:** ACL은 위에서부터 순서대로 검사하며, 조건에 맞는 항목을 찾으면 즉시 적용하고 검사를 종료한다. 따라서 "작은 범위(특정 호스트)를 먼저 작성하고, 큰 범위(전체 대역)를 나중에 작성"해야 한다.
- 묵시적 거부(Implicit Deny):** 모든 ACL의 마지막에는 deny any가 숨겨져 있다. 즉, 명시적으로 permit을 해주지 않은 모든 트래픽은 자동으로 차단된다. 따라서 허용할 트래픽이 있다면 반드시 permit 명령어를 추가해야 한다.
- 적용 방향(Direction):** 인터페이스의 inbound(유입) 또는 outbound(유출) 방향을 정확히 지정해야 한다.

3. [실습] 시나리오별 보안 정책 적용

실습 목표: 다양한 서비스(SSH, FTP, SMB, ICMP)에 대해 차별적인 접근 제어 정책을 수립한다.

- 시나리오 1 (표준 ACL):** 특정 윈도우 PC에서만 파일 스토리지에 접근할 수 있도록 R3 인터페이스에 인바운드 정책을 적용한다.
- 시나리오 2 (확장 ACL - 서비스 차단):** 외부에서의 SSH(TCP 22) 접근을 차단하되, 나머지 일반 IP 트래픽은 허용한다.

```
access-list 100 deny tcp any any eq 22
access-list 100 permit ip any any
```

- 시나리오 3 (확장 ACL - 특정 서비스 허용/차단):** 특정 대역에서만 FTP(20, 21)와 SMB(139, 445)를 사용하게 하고, 나머지는 차단한다.

ACL 정책을 적용하기 위한 네트워크 구성 토폴로지이다.

네트워크 실무 운영 및 설정 점검 가이드

네트워크 장애 발생 시 무엇을 먼저 점검해야 하는가?

실무 운영 중 발생하는 대부분의 문제는 인터페이스 상태, L2 프로토콜 매칭, 인증 오류, 또는 ACL 설정 실수에서 기인합니다. 아래 체크리스트를 통해 체계적으로 점검하십시오.

1. 인터페이스 및 연결 상태 점검

- **L3 포트 활성화 확인:** 라우터 포트는 기본적으로 shutdown 상태입니다. 반드시 `no shutdown` 명령어로 활성화했는지 확인하십시오.
- **계층별 상태 확인 (`show ip int bri`):**
 - **Status (L1):** 물리적 연결 상태입니다. `administratively down`이라면 명령어로 포트를 끄거나 켜 상태를 의미합니다.
 - **Protocol (L2):** 논리적 연결 상태입니다. `down`이라면 캡슐화 방식(HDLC/PPP)이 다르거나, 인증(PAP/CHAP)이 실패한 경우입니다.
- **가상 인터페이스:** Loopback 인터페이스와 같이 생성된 가상 인터페이스는 별도의 `no shut` 없이도 기본적으로 활성화됩니다.

2. ACL 및 라우팅 점검

- **ACL 적용 방향 및 인터페이스:** `ip access-group [번호] [in/out]` 명령어가 의도한 인터페이스와 방향에 정확히 적용되었는지 확인하십시오.
- **ACL 우선순위:** 차단 규칙을 허용 규칙보다 먼저 작성했는지 확인하십시오. 거꾸로 작성할 경우 의도치 않은 트래픽이 차단될 수 있습니다.
- **라우팅 테이블:** `show ip route`를 통해 목적지 네트워크로 가는 경로가 올바른 Next-hop(또는 인터페이스)을 가리키고 있는지 확인하십시오.

3. 문제 해결(Troubleshooting) 순서

1. **물리 계층 확인:** 케이블 연결 및 인터페이스 Status 확인.
2. **데이터 링크 계층 확인:** Protocol 상태 확인 및 `show frame-relay map` 등을 통한 L2 매핑 확인.
3. **인증 확인:** PPP 사용 시 `debug ppp authentication`을 통해 인증 로그 분석.
4. **네트워크 계층 확인:** ping 테스트를 통한 종단 간(End-to-End) 통신 확인 및 라우팅 경로 점검.
5. **보안 정책 확인:** `show access-list`로 ACL 적용 규칙과 hitcount를 확인하여 트래픽이 차단되고 있는지 점검.