수업 내용 정리 보고서

챕터 구성

1. 데이터 링크 계층(L2) 프로토콜의 특징
2. PPP 인증 방식 및 설정 방법
3. ACL(접근 제어 목록)의 기본 원리와 적용 규칙
4. Standard 및 Extended ACL의 비교 및 활용
5. 네트워크 실무 운영 및 트러블슈팅 가이드

데이터 링크 계층(L2) 프로토콜의 특징

1. 데이터 링크 계층(L2)의 핵심 역할

데이터 링크 계층은 물리적 매체(Physical Layer)를 통해 인접한 노드 간에 신뢰성 있는 데이터 전송을 보장하는 역할을 합니다. 상위 계층(L3, 네트워크 계층)에서 내려온 패킷을 **프레임(Frame)**이라는 단위로 캡슐화하며, 물리적 주소(MAC Address 등)를 사용하여 인접 장비 간의 통신을 제어합니다.

2. 주요 L2 프로토콜 분류

네트워크 환경과 연결 방식에 따라 다양한 L2 프로토콜이 사용됩니다. 주요 프로토콜의 특징은 다음과 같습니다.

프로토콜 명칭	주요 특징 및 용도
HDLC (High-Level Data Link Control)	Cisco 환경의 Serial 인터페이스에서 기본적으로 사용되는 프로토콜입니다.
PPP (Point-to-Point Protocol)	두 지점 간의 직접 연결에 사용되며, **인증(PAP, CHAP)** 기능을 지원하여 보안성이 높습니다.
Frame-Relay (FR)	패킷 교환 방식의 WAN 기술로, 다수의 가상 회선을 통해 데이터를 전송합니다.
ARPA (Ethernet)	가장 보편적인 LAN 프로토콜로, MAC 주소를 기반으로 통신합니다.
dot1q (IEEE 802.1Q)	VLAN 태깅(Tagging)을 위해 사용되는 프로토콜로, 하나의 물리적 링크에서 여러 가상 네트워크를 구분합니다.

3. 핵심 운영 원리: 인터페이스별 독립성

라우터와 같은 네트워크 장비의 가장 중요한 특징 중 하나는 **인터페이스마다 서로 다른 회선 프로토콜을 독립적으로 사용**할 수 있다는 점입니다.

- **멀티 프로토콜 지원:** 라우터의 Serial 1/0 인터페이스에는 PPP를 설정하고, FastEthernet 0/0 인터페이스에는 Ethernet(ARPA)을 설정하여 서로 다른 성격의 네트워크를 동시에 연결할 수 있습니다.
- **계층 간의 분리:** L2 프로토콜이 무엇이든 관계없이, 라우터는 L2 프레임을 해제(Decapsulation)하여 내부의 L3 패킷(IP)을 확인한 후 상위 계층으로 전달합니다. 이 덕분에 서로 다른 L2 환경 간의 통신이 가능해집니다.

4. [심화] PPP 인증 메커니즘 (L2 보안의 기초)

PPP 프로토콜은 단순한 데이터 전송을 넘어, 연결 단계에서 상대방을 확인하는 **인증(Authentication)** 과정을 거칠 수 있습니다. 이는 L2 수준에서 보안을 강화하는 중요한 요소입니다.

- **PAP (Password Authentication Protocol):**
  - **방식:** 2-Way Handshake.
  - **취약점:** 패스워드가 **평문(Plain Text)**으로 전송되므로, 중간에서 패킷을 가로챌 경우 보안에 매우 취약합니다.
- **CHAP (Challenge Handshake Authentication Protocol):**
  - **방식:** 3-Way Handshake.
  - **특징:** 해시(Hash) 함수와 메시지 다이제스트를 사용합니다. 실제 비밀번호를 네트워크에 직접 흘려보내지 않으므로 PAP보다 훨씬 안전합니다.
  - **주의사항:** 상호 인증을 위해서는 양단 장비의 **Hostname과 Username 설정이 반드시 일치**해야 연결이 성립됩니다.

> **실무 및 시험 포인트**
> 1. **"L2 프로토콜은 암호화 프로토콜인가?"**: 아닙니다. PPP의 PAP/CHAP은 '인증(이 사용자가 맞는지 확인)'을 위한 것이지, 데이터 자체를 암호화하여 내용을 숨기는 개념과는 구분해야 합니다.
> 2. **인터페이스 설정 오류:** 라우터 간 연결 시 한쪽은 PPP로, 다른 한쪽은 HDLC로 설정되어 있다면 L2 프로토콜 불일치로 인해 통신이 불가능합니다. 반드시 양단의 프로토콜을 일치시켜야 합니다.

PPP 인증 방식 및 설정 방법

PPP(Point-to-Point Protocol)는 두 노드 간의 직접적인 연결을 지원하는 데이터 링크 계층(L2) 프로토콜입니다. 두 라우터가 연결될 때, 상대방이 신뢰할 수 있는 장비인지 확인하는 과정이 필수적인데 이를 **인증(Authentication)**이라고 합니다. 본 보고서에서는 PPP의 대표적인 인증 방식인 PAP와 CHAP를 비교 분석하고, 실무적인 설정 방법을 정리합니다.

1. 인증 방식의 핵심 비교: PAP vs CHAP

PPP 인증은 단순히 아이디와 비밀번호를 확인하는 것을 넘어, 인증이 이루어지는 단계(Handshake)와 보안 수준에서 큰 차이를 보입니다.

구분	PAP (Password Authentication Protocol)	CHAP (Challenge Handshake Authentication Protocol)
인증 방식	2-Way Handshake	3-Way Handshake
보안성	낮음 (비밀번호가 평문으로 전송됨)	높음 (해시 함수 및 다이제스트 활용)
전송 데이터	비밀번호 자체가 네트워크를 타고 흐름	비밀번호를 해시화한 값만 전송
주요 특징	설정이 간편하지만 스니핑(Sniffing)에 취약	상대방의 호스트네임과 사용자 이름의 일치 필수

> ⚠ **중요 주의사항:** 인증(Authentication)은 "상대방이 누구인지 확인"하는 절차일 뿐, 통신하는 데이터 자체를 암호화(Encryption)하는 개념이 아닙니다. 데이터 보안을 위해서는 별도의 암호화 프로토콜이 필요합니다.

2. Cisco 환경에서의 상세 설정 방법

PPP 인증 설정 시 가장 혼란을 겪는 부분은 **'내가 상대방에게 보낼 정보'**와 **'상대방이 나에게 보낼 정보'**를 구분하는 것입니다.

■ PAP 설정 가이드

PAP는 평문 전송 방식을 사용하므로, 양측 라우터에 상대방의 계정 정보를 미리 등록해야 합니다.

```
! [R1 라우터 설정]
conf t
username R2 password cisco          ! R2가 접속할 때 사용할 계정 생성
interface serial 1/0
 ppp authentication pap              ! 인증 방식으로 PAP 사용 선언
 ppp pap sent-username R1 password cisco ! 내가 R2로 접속할 때 보낼 내 정보
```

■ CHAP 설정 가이드

CHAP은 보안성이 높지만, **호스트네임(Hostname)** 설정이 인증의 핵심 키(Key)로 작용합니다. 호스트네임과 username이 일치하지 않으면 인증에 실패합니다.

```
! [R1 라우터 설정]
conf t
hostname router1                    ! 자신의 호스트네임 설정 (매우 중요)
username router2 password cisco     ! 상대방(router2)의 호스트네임과 비밀번호 등록

interface serial 1/0
 ppp authentication chap             ! 인증 방식으로 CHAP 사용 선언
```

3. 실무 및 시험 대비 핵심 포인트

- **CHAP의 성공 조건:** CHAP 인증이 성공하려면 다음 세 가지 요소가 상대방 설정과 완벽히 매칭되어야 합니다.
  - 나의 *Hostname* = 상대방의 *Username*
  - 상대방의 *Hostname* = 나의 *Username*
  - 설정된 *Password*의 일치
- **트러블슈팅(Troubleshooting) 시 유의사항:**

    - PPP 인증 실패 시 가장 먼저 확인해야 할 것은 **Hostname**과 **Username**의 매칭 여부입니다.
    - 실무 환경에서는 debug 명령어를 사용하여 인증 과정을 확인할 수 있으나, 과도한 로그 발생으로 인해 라우터의 **CPU 부하가 100%**에 도달하여 장비가 다운될 수 있으므로 극도로 주의하여 사용해야 합니다.
- **설계 시 고려사항:** 보안이 중요한 기업 망에서는 반드시 CHAP 사용을 권장하며, PAP는 보안 요구사항이 낮은 폐쇄적인 환경에서만 제한적으로 사용합니다.

ACL(접근 제어 목록)의 기본 원리와 적용 규칙

1. ACL의 정의 및 역할

ACL(Access-Control List)은 네트워크 트래픽의 흐름을 제어하는 일종의 '논리적인 방화벽' 역할을 수행합니다. 라우터나 스위치를 통과하는 패킷을 검사하여, 설정된 조건에 따라 통과(Permit)시킬지 혹은 차단(Deny)할지를 결정합니다.

- **주요 기능:** 특정 호스트 또는 네트워크 대역의 접근 권한 제어, 트래픽 필터링.
- **확장 활용:** NAT(Network Address Translation) 구현 시 어떤 트래픽을 변환할지 결정하는 기준점으로도 연동됩니다.

2. ACL의 핵심 작동 원리

ACL을 설계하고 적용할 때 반드시 이해해야 하는 두 가지 핵심 메커니즘이 있습니다.

① 순차적 적용 (Top-Down 방식)

ACL은 리스트의 **가장 윗줄부터 아래로 순차적으로** 조건을 검사합니다. 패킷이 리스트의 특정 조건과 일치(Matching)하는 즉시 해당 동작(Permit/Deny)을 수행하고 검사를 종료합니다. 따라서 **조건의 순서**가 매우 중요합니다.

> **실무/시험 포인트:** 범위가 좁은 조건(예: 특정 단일 호스트)을 상단에 배치하고, 범위가 넓은 조건(예: 전체 대역)을 하단에 배치해야 합니다. 만약 넓은 범위의 조건을 상단에 두면, 그 아래에 있는 정교한 조건들은 절대 실행될 기회를 얻지 못합니다.

② 묵시적 거부 (Implicit Deny)

모든 ACL의 맨 마지막에는 사용자가 눈으로 볼 수 없지만 **"모든 트래픽을 차단한다(deny any)"**라는 규칙이 숨겨져 있습니다. 이는 보안을 위한 기본 설계입니다.

- **주의사항:** 특정 트래픽만 차단(Deny)하려는 목적으로 ACL을 작성했다면, 반드시 마지막 줄에 permit any를 추가해야 합니다. 그렇지 않으면 차단 대상이 아닌 나머지 모든 정상 트래픽이 묵시적 거부 규칙에 걸려 함께 차단됩니다.

3. ACL의 종류 및 비교

제어할 수 있는 정보의 상세 수준에 따라 **Standard**와 **Extended**로 구분됩니다.

구분	Standard ACL (표준)	Extended ACL (확장)
번호 범위	1 ~ 99	100 ~ 199
제어 기준	출발지 IP 주소(Source IP)	출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP 등), 포트 번호
정밀도	낮음 (단순 차단/허용)	매우 높음 (상세 서비스 제어 가능)
설계 전략	목적지 근처에 배치	출발지(Source) 근처에 배치하여 자원 낭비 방지

4. 적용 규칙 및 인터페이스 제약 사항

ACL은 작성하는 것만으로 작동하지 않으며, 반드시 네트워크 인터페이스에 적용(Apply)해야 합니다.

- **방향성 및 개수 제한:** 하나의 인터페이스에는 **인바운드(Inbound) 1개, 아웃바운드(Outbound) 1개**의 ACL만 적용할 수 있습니다.
    - *만약 여러 정책을 적용해야 한다면?* 여러 개의 ACL을 하나로 통합하여 하나의 리스트로 만든 뒤 적용해야 합니다.
- **설계 효율성:** 트래픽이 발생한 지점(Source 측)과 가까운 곳에서 차단할수록 네트워크 대역폭과 라우터의 자원 소모를 줄일 수 있어 효율적입니다.
- **차단 시 메시지:** ACL에 의해 트래픽이 거부될 경우, 통신 측에서는 Communication administratively prohibited라는 메시지를 받게 됩니다.

5. 관리 및 운영 가이드 (Troubleshooting)

① 수정 및 삭제 전략

전통적인 방식의 ACL은 중간에 특정 라인만 삽입하거나 삭제하는 것이 매우 까다롭습니다.
실무 팁: 설정 실수로 인해 네트워크 장애가 우려될 경우, 기존 ACL을 삭제하고 처음부터 다시 작성하는 것이 가장 안전하고 확실한 방법입니다. (단, Named ACL을 사용하면 부분 수정이 어느 정도 가능합니다.)

② 명령어 활용

```
# ACL 설정 예시 (Standard)
access-list 1 deny host 1.1.1.2
access-list 1 permit any

# ACL 설정 예시 (Extended)
access-list 100 deny icmp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255

# 인터페이스 적용
interface fastethernet 0/0
ip access-group 1 in

# 확인 명령어
show access-lists
```

③ 운영 중 주의사항

- **Debug 명령어 주의:** 실무 운영 장비에서 debug 명령어를 무분별하게 사용하면 로그 과다 발생으로 인해 **CPU 부하가 100%**에 도달하여 장비가 다운될 수 있습니다.
- **방향성 확인:** ACL 적용 시 *Inbound*(들어오는 패킷 검사)와 *Outbound*(나가는 패킷 검사) 방향을 혼동하면 의도치 않은 차단이 발생할 수 있으므로 반드시 확인이 필요합니다.

Standard 및 Extended ACL의 비교 및 활용

네트워크 보안의 핵심 요소인 **ACL(Access-Control List, 접근 제어 목록)**은 라우터나 스위치에서 특정 트래픽을 허용(Permit)하거나 차단(Deny)하는 일종의 방화벽 역할을 수행합니다. ACL을 올바르게 설계하고 적용하기 위해서는 Standard와 Extended의 근본적인 차이점을 이해하고, 트래픽 흐름에 따른 최적의 배치 전략을 세우는 것이 중요합니다.

1. Standard vs Extended ACL 핵심 비교

ACL은 필터링할 수 있는 정보의 범위에 따라 두 가지 유형으로 나뉩니다. 어떤 정보를 기준으로 트래픽을 판단하느냐에 따라 적용 위치와 설계 방식이 완전히 달라집니다.

구분	Standard ACL (표준)	Extended ACL (확장)
번호 범위	1 ~ 99	100 ~ 199
필터링 기준	**출발지(Source) IP 주소**만 확인	**출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP 등), 포트 번호**까지 확인
제어 정밀도	낮음 (특정 호스트 전체 차단에 유리)	높음 (특정 서비스/프로토콜만 선별 차단 가능)
최적의 적용 위치	**목적지(Destination)와 가까운 곳**	**출발지(Source)와 가까운 곳**

2. ACL 설계 및 운영의 4대 핵심 원칙

ACL을 설정할 때 실수를 방지하고 네트워크 효율성을 극대화하기 위해 반드시 숙지해야 할 규칙들입니다.

① Top-Down 방식과 순차 적용

ACL은 리스트의 **맨 위 라인부터 순차적으로** 조건을 검사합니다. 조건이 일치하는 항목을 발견하면 즉시 해당 동작(Permit/Deny)을 수행하고 검사를 종료합니다. 따라서 *범위가 좁고 구체적인 조건(특정 호스트)을 상단에, 범위가 넓은 조건(특정 대역 또는 Any)을 하단에 배치*해야 합니다.

② 묵시적 거부 (Implicit Deny Any)의 함정

모든 ACL의 마지막에는 눈에 보이지 않는 **'deny any'** 규칙이 숨겨져 있습니다.

- **주의사항:** 특정 트래픽만 차단(Deny)하고 나머지는 모두 허용하고 싶다면, 반드시 ACL 맨 마지막 줄에 permit any를 명시적으로 추가해야 합니다.
- 이를 누락할 경우, 차단하고자 했던 트래픽 외의 모든 정상적인 통신이 차단되는 장애가 발생합니다.

③ 인터페이스 적용 규칙 (Inbound vs Outbound)

하나의 인터페이스에는 방향별로 **인바운드(In) 1개, 아웃바운드(Out) 1개**의 ACL만 적용할 수 있습니다.

- 만약 두 개 이상의 서로 다른 정책을 하나의 인터페이스에 적용해야 한다면, 각각의 ACL을 하나로 통합한 **새로운 통합 ACL(Combined ACL)**을 만들어 적용해야 합니다.

④ 효율적인 배치 전략 (Placement Strategy)

네트워크 자원 소모를 줄이기 위한 배치 전략은 ACL 유형에 따라 반대로 움직입니다.

- **Extended ACL:** 트래픽이 발생하자마자(Source 근처) 차단하는 것이 효율적입니다. 불필요한 트래픽이 네트워크 망을 타고 이동하며 대역폭을 점유하는 것을 방지할 수 있습니다.
- **Standard ACL:** 출발지 IP만 보고 판단하므로, 출발지 근처에 배치하면 해당 호스트가 가고자 하는 *모든* 목적지로의 통신이 막힐 수 있습니다. 따라서 의도치 않은 차단을 막기 위해 목적지(Destination) 근처에 배치하는 것이 안전합니다.

3. 실무 설정 예시 및 명령어

■ Standard ACL 설정 (특정 호스트 차단 후 나머지 허용)

```
conf t
access-list 1 deny host 1.1.1.2     ! 특정 호스트 1.1.1.2 차단
```

```
access-list 1 permit any           ! 나머지 모든 트래픽 허용 (필수!)
interface fastethernet 0/0
ip access-group 1 in               ! 인터페이스에 인바운드 적용
```

■ **Extended ACL 설정 (특정 대역의 ICMP 트래픽만 차단)**

```
conf t
! [Source_NID] [Source_Wildmask] [Destination_Address] [Destination_Wildmask]
access-list 100 deny icmp 192.168.10.0 0.0.0.255 10.1.1.5 0.0.0.0
access-list 100 permit ip any any   ! ICMP 외의 다른 트래픽은 허용
interface fastethernet 0/0
ip access-group 100 in
```

4. Troubleshooting 및 운영 주의사항

> ⚠ **실무 운영 Tip:**
>
> - **Debug 명령어 주의:** 운영 중인 장비에서 debug 명령어를 과도하게 사용하면 CPU 부하가 100%로 치솟아 장비가 다운될 수 있습니다. 가급적 show 명령어를 통해 상태를 먼저 확인하십시오.
> - **차단 확인:** ACL에 의해 트래픽이 거부될 경우, 송신 측에서는 '*Communication administratively prohibited*'라는 메시지를 받게 됩니다.
> - **수정의 어려움:** 기존 ACL 중간에 새로운 규칙을 삽입하는 것은 매우 까다롭습니다. 실수 방지를 위해 기존 리스트를 삭제하고 새로 작성하거나, 부분 수정이 가능한 **Named ACL** 방식을 사용하는 것이 권장됩니다.
> - **확인 명령어:** show access-lists를 통해 현재 적용된 리스트와 각 규칙별 매칭된 패킷 수를 확인할 수 있습니다.

네트워크 실무 운영 및 트러블슈팅 가이드

1. 데이터 링크 계층(L2) 및 보안 인증 프로토콜

네트워크의 물리적 연결 직후 단계인 데이터 링크 계층에서는 라우터 인터페이스 간의 통신을 정의하는 회선 프로토콜을 사용합니다. 각 인터페이스는 독립적으로 서로 다른 프로토콜을 설정할 수 있는 유연성을 가집니다.

PPP(Point-to-Point Protocol) 인증 방식 비교

PPP 연결 시 보안을 강화하기 위해 인증 과정을 거치게 됩니다. 여기서 주의할 점은 **인증(Authentication)은 '누구인지 확인'하는 절차이지, 데이터 자체를 암호화하는 과정이 아니라는 점**입니다.

구분	PAP (Password Authentication Protocol)	CHAP (Challenge Handshake Authentication Protocol)
핸드셰이크	2-Way Handshake	3-Way Handshake
전송 방식	패스워드를 **평문(Plain Text)**으로 전송	**해시(Hash)** 및 메시지 다이제스트 활용
보안성	낮음 (스니핑에 취약)	높음 (데이터 변조 및 재전송 공격 방어)
필수 설정	ID/PW 일치	상대방의 **Hostname과 Username**이 반드시 일치해야 함

[실무 설정 예시 - CHAP]
CHAP는 보안을 위해 호스트네임 매칭이 필수적이므로, 양단 장비의 이름 설정에 유의해야 합니다.

```
! Router 1 설정
hostname router1
username router2 password cisco  ! 상대방(router2)의 호스트네임을 ID로 지정

interface serial 1/0
 ppp authentication chap
```

---

2. ACL(Access-Control List) 설계 및 운용 전략

ACL은 네트워크 트래픽의 흐름을 제어하는 핵심적인 방화벽 역할을 수행합니다. 단순한 차단을 넘어 네트워크 자원을 효율적으로 관리하기 위한 설계 능력이 요구됩니다.

ACL의 핵심 동작 원리

- **Top-Down 방식:** ACL은 리스트의 맨 위 라인부터 순차적으로 검사합니다. 조건이 일치하는 항목을 발견하면 즉시 실행하고 하위 항목은 검사하지 않습니다. 따라서 **범위가 좁고 구체적인 조건(예: 특정 호스트)을 상단에 배치**해야 합니다.
- **묵시적 거부(Implicit Deny):** 모든 ACL의 마지막에는 눈에 보이지 않는 deny any 규칙이 존재합니다. 특정 트래픽만 차단하고 나머지는 허용하고 싶다면, 반드시 리스트 끝에 permit any를 명시해야 전체 통신이 끊기는 사고를 막을 수 있습니다.
- **인터페이스 적용 제한:** 하나의 인터페이스에는 인바운드(Inbound) 1개, 아웃바운드(Outbound) 1개의 ACL만 적용할 수 있습니다. 여러 정책을 적용해야 한다면, 정책들을 하나의 리스트로 통합하여 설계해야 합니다.

Standard vs Extended ACL 비교

특징	Standard ACL (표준)	Extended ACL (확장)
번호 범위	1 ~ 99	100 ~ 199
제어 기준	**출발지(Source) IP** 주소만 확인	출발지/목적지 IP, 프로토콜(TCP/UDP/ICMP), 포트 번호
정밀도	낮음 (단순 차단/허용)	매우 높음 (상세한 서비스 제어 가능)
적용 위치 권장	목적지(Destination)와 가까운 곳	출발지(Source)와 가까운 곳

---

3. 실무 운영 및 트러블슈팅 가이드

현업에서 네트워크 장애를 해결하거나 장비를 운영할 때 반드시 숙지해야 할 주의사항입니다.

> ⚠ **실무자 경고: Debug 명령어 사용 주의**
> 운영 중인 장비에서 debug 명령어를 무분별하게 실행할 경우, 과도한 로그 생성으로 인해 **CPU 점유율이 100%로 급증하며 장비가 다운(Hang)**될 수 있습니다. 반드시 트래픽 양을 확인하고 필요한 경우에만 제한적으로 사용하십시오.

Troubleshooting 체크리스트

1. **ACL 차단 메시지 확인:** 특정 통신이 불가능할 때 'Communication administratively prohibited' 메시지가 발생한다면, 이는 물리적 장애가 아닌 **ACL 정책에 의한 의도적인 차단**임을 의미합니다.
2. **방향성(Direction) 재검토:** ACL이 적용된 인터페이스의 방향(Inbound vs Outbound)이 의도한 대로 설정되었는지 확인하십시오.
3. **설계 효율성 검토:** 네트워크 자원 소모를 줄이려면 트래픽이 발생하는 **소스(Source) 측 말단에서 최대한 빨리 차단**하는 것이 가장 효율적입니다.
4. **수정 및 삭제:** ACL 중간에 규칙을 삽입하거나 삭제하는 것은 논리적 오류를 범하기 쉽습니다. 실수를 방지하기 위해 기존 리스트를 삭제하고 새로 작성하거나, *Named ACL*을 활용하여 관리하는 것이 안전합니다.

[확인 명령어]
`show access-lists` : 현재 적용된 ACL의 내용과 매칭된 패킷 수를 확인하여 정책이 의도대로 작동하는지 점검합니다.