

수업 내용 정리 보고서

챕터 구성

1. L2 프로토콜 및 인증 방식
2. ACL의 유형 및 동작 원리
3. 실무 운영 및 적용 체크리스트

L2 프로토콜 및 인증 방식

데이터 링크 계층(Layer 2)에서는 물리적 매체를 통해 데이터를 전달하기 위해 다양한 **회선 프로토콜(Line Protocol)**을 사용합니다. 주요 프로토콜로는 HDLC, PPP, FR, ARPA(Ethernet), dot1q 등이 있으며, 네트워크 설계 시 **각 인터페이스의 특성에 맞춰 서로 다른 프로토콜을 개별적으로 적용**할 수 있습니다.

인증 방식: PAP vs CHAP

인터페이스 간 연결 시 보안을 위해 인증 과정을 거칩니다. 이때 주의할 점은 **인증(Authentication)은 암호화(Encryption)와는 다른 개념**이라는 것입니다. 인증은 '상대방이 누구인지 확인하는 절차'이며, 암호화는 '데이터 내용을 읽지 못하게 만드는 기술'입니다.

구분	PAP (Password Authentication Protocol)	CHAP (Challenge Handshake Authentication Protocol)
인증 단계	2-Way State (단순 인증)	3-Way 방식 (Challenge-Response 기반)
보안성	낮음 (비교적 단순한 절차)	높음 (해시/메시지 다이제스트 활용)
주요 조건	ID/Password 확인	상대방의 Hostname 과 Username 이 반드시 일치해야 함

* CHAP은 해시(Hash) 기술을 사용하여 비밀번호를 직접 전송하지 않고 메시지 다이제스트를 통해 검증하므로 PAP보다 보안이 강력합니다.

PPP 인증 설정 절차 (Cisco 기준)

PPP 프로토콜을 사용하여 상대방(R2)을 인증하도록 설정하는 예시입니다.

1. **선행 조건:** 장비의 호스트네임 설정 및 인증에 사용할 계정 정보 생성
2. **실행 예시:**

```
! 1. 호스트네임 설정
Router(config)# hostname R1

! 2. 상대방(R2)이 접속할 때 사용할 계정 생성
R1(config)# username R2 password cisco

! 3. 인터페이스 접속 및 인증 방식 지정
R1(config)# interface s1/0
R1(config-if)# ppp authentication pap

! 4. PAP 사용 시 나의 정보(R1)를 상대방에게 전달하도록 설정
R1(config-if)# ppp pap sent-username R1 password cisco
```

3. **확인 방법:** show interface 또는 show ppp authentication 명령어를 통해 프로토콜 상태 확인
4. **주의사항:** CHAP 방식에서는 `sent-username` 설정이 필요하지 않으나, PAP 방식에서는 인증을 위해 자신의 정보를 명시해야 합니다.

ACL의 유형 및 동작 원리

ACL(Access-Control List)은 네트워크 트래픽의 통과 여부(Permit/Deny)를 결정하는 방화벽 역할을 수행합니다. 특정 IP나 프로토콜을 차단하거나 허용하여 네트워크 보안을 강화하고 NAT(Network Address Translation) 구현 시에도 활용됩니다.

ACL의 유형 비교

유형	번호 범위	제어 범위 및 특징
Standard (표준)	1 ~ 99	출발지 IP 주소만을 기준으로 트래픽을 통제 (단순 차단/허용)
Extended (확장)	100 ~ 199	출발지/목적지 IP, 프로토콜(ICMP, TCP 등), 포트 번호까지 정밀하게 제어

ACL 동작의 핵심 원리

- First Match (선착순 적용):** ACL은 리스트의 가장 위에서부터 순차적으로 검사합니다. 조건에 맞는 규칙을 발견하면 즉시 적용하고 검사를 종료합니다. 따라서 세부적인 규칙을 상단에, 포괄적인 규칙을 하단에 배치해야 합니다.
- Implicit Deny (묵시적 거부):** 모든 ACL의 마지막에는 "허용되지 않은 모든 트래픽을 차단한다"는 규칙이 숨겨져 있습니다. 만약 특정 트래픽만 차단하고 나머지를 모두 허용하고 싶다면, 반드시 마지막에 `permit any`를 추가해야 합니다.
- 단일 정책 원칙:** 하나의 인터페이스에는 인바운드(Inbound)와 아웃바운드(Outbound) 각각 하나의 ACL만 적용할 수 있습니다. 만약 A 정책과 B 정책을 모두 적용해야 한다면, 두 정책을 통합한 하나의 새로운 리스트(C)를 개발하여 적용해야 합니다.

효율적인 ACL 설계 방법

검사 효율을 높이기 위해서는 "작은 범위부터 검사"하는 것이 원칙입니다. 단일 호스트나 특정 대역을 먼저 검사하여 불필요한 프로세싱을 줄이는 것이 성능 면에서 유리합니다.

검사 단위: 단일 호스트 → 특정 네트워크 대역(NI) → 전체(ANY)

실무 운영 및 적용 체크리스트

네트워크 실무 환경에서 ACL을 적용하거나 장애를 대응할 때 반드시 숙지해야 할 운영 포인트입니다.

⚠ 운영 주의사항

- **Debug 명령 제한:** 실무 운영 중 debug 명령어를 무분별하게 사용하면 과도한 로그 발생으로 인해 장비의 CPU 부하가 급증하고 서비스 중단이 발생할 수 있습니다. 반드시 필요한 경우에만 제한적으로 사용하십시오.
- **ACL 수정의 어려움:** ACL은 작성 순서가 중요합니다. 중간에 잘못된 규칙을 넣었다면, 단순히 아래에 추가하는 것이 아니라 **기존 리스트를 삭제하고 다시 작성**해야 하는 경우가 많으므로 설정 시 신중해야 합니다.
- **인터페이스 방향(Direction) 확인:** ACL을 적용할 때 **인바운드(In)에 걸 것인지 아웃바운드(Out)에 걸 것인지**에 따라 트래픽 흐름이 완전히 달라집니다. 적용 위치를 잘못 지정하면 의도치 않은 통신 장애가 발생합니다.

문제 해결 및 점검 가이드

상황: 특정 통신이 되지 않고 'Communication administratively prohibited' 메시지가 발생하는 경우

1. **ACL 적용 확인:** 해당 인터페이스에 ip access-group [번호] [in/out]이 제대로 적용되어 있는지 확인합니다.
2. **순서 점검:** show access-list 명령어를 통해 차단(deny) 규칙이 허용(permit) 규칙보다 상단에 위치하여 트래픽을 먼저 잡아먹고 있지는 않은지 확인합니다.
3. **목적적 차단 확인:** 차단하고자 하는 규칙 외에 통과시켜야 할 트래픽에 대해 permit 규칙이 누락되지 않았는지 점검합니다.
4. **Wildcard Mask 검토:** 확장 ACL 사용 시 Wildcard Mask(NI) 값이 대상 네트워크 대역과 일치하는지 재검토합니다.

최종 체크리스트

- [] 인증 방식(PAP/CHAP)에 맞는 사용자 계정 및 호스트네임이 설정되었는가?
- [] ACL 번호가 표준(1-99)인지 확장(100-199)인지 용도에 맞게 선택했는가?
- [] 세부적인 규칙(Host)을 포괄적인 규칙(Any)보다 먼저 작성했는가?
- [] 차단 목적 외의 트래픽을 위해 permit any를 고려했는가?
- [] 인터페이스의 In/Out 방향 설정이 트래픽 흐름과 일치하는가?