AAA

1. AAA란?

○ 기존의 라우터 상에서 구현되는 CLI 기반의 인증보다 더 높은 수준의 확장성을 제공하는 인증과 관련된 서비스
○ AAA: Authentication(인증), Authorization(인가), Accounting(과금)의 약자
- Authentication: 사용자나 관리자가 정말로 맞는지 증명하는 과정으로 일반적으로 사용자 이름과 패스워드가 맞는지를 확인
- Authorization: 인증 이후에 진행되는 과정으로 접근한 사용자 또는 관리자에게 허가된 자원 또는 권한을 제공하는 과정
- Accounting: 감사 기능과 병행이 되는데 사용자나 관리자의 접속 여부, 접속 후 행위, 접속 시간 등에 대해 기록을 남기고 후에 감사하기 위한 용도로 사용

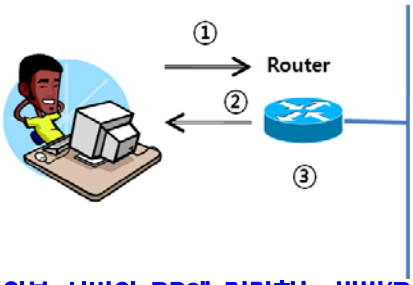
○ 목적: 사용자에 대한 식별, 허용가능한 권한 부여, 접근에 대한 기록과 감사

2. AAA 구현 방법

AAA를 구현하는 방법은 일반적으로 2가지

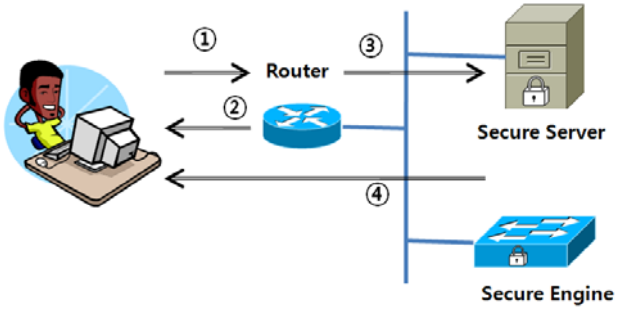
○ **라우터 자신의 로컬 DB에 저장하는 방법**

소규모 네트워크의 경우, 사용자 이름과 패스워드는 시스코 라우터에 저장된다.



○ **외부 서버의 DB에 저장하는 방법(RADIUS, TACACS+)**

대규모 네트워크에서는 인증을 별도로 담당하는 외부의 서버를 두는 것이 유리하다. 이 경우에 RADIUS나 TACAC+와 같은 프로토콜을 사용하는 인증 서버는 단순히 사용자에 대한 인증뿐만 아니라 권한 관리 및 과금도 보다 명확히 관리할 수 있다.



3. AAA 설정

CCIE 시험에는 AAA 중에서도 인증 위주로 출제

3-1. AAA 기능 활성화

RW(config)# **aaa new-model**

AAA 기능을 사용하기 위해서는 'aaa new-model' 명령을 실행시켜야만 관련 명령어가 사용가능

3-2. 텔넷 접속에 대한 AAA 설정 사례

○ 로컬 DB

```
username 사용자이름 password 암호
!
aaa new-model
aaa authentication login default local
!
line vty 0 4
login authentication default
```

○ 외부 서버(RADIUS)

```
username 사용자이름 password 암호
!
aaa new-model
aaa authentication login default group radius
radius-server host w.x.y.z
radius-server key 암호
!
line vty 0 4
login authentication default
```

○ 외부 서버(TACACS+) 실패시 로컬 DB 사용

```
username 사용자이름 password 암호
!
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host w.x.y.z
tacacs-server key 암호
!
line vty 0 4
login authentication default
```

4. RADIUS vs TACACS+

외부 인증서버를 사용하는 대표적인 프로토콜은 RADIUS와 TACACS+, 그리고 Kerberos가 있다.

○ RADIUS(Remote Access Dial-In User Service)

- RFC에서 정의한 표준 프로토콜로 접근 서버 인증과 과금 프로토콜로 개발되었다.
- UDP를 사용하는 클라이언트/서버 프로토콜로 TACACS+에 비해 CPU 부하가 적고 메모리 점유율도 낮다.

○ TACACS+(Terminal Access Controller Access System Plus)

- 시스코에서 개발하였다.
- 인증, 인가, 과금 기능을 분리할 수 있는 타입이 존재
- TACACS는 TACACS의 최초 버전으로 인증만 처리할 수 있다.
- XTACACS(eXtended TACACS)는 인증뿐만 아니라 과금도 수행할 수 있다.
- AAA의 모든 구성요소를 지원하고 TCP를 사용하여 안정성도 높아 가장 보편적으로 사용

RADIUS와 TACACS+ 비교

구분	RADIUS	TACACS+
기능	인증, 인가	인증, 인가, 과금
전송 프로토콜	UDP	TCP
CHAP	단방향	양방향
지원 프로토콜	no ARA, no NETBEUI	멀티 프로토콜 지원
보안	패스워드 암호화	전체 패킷 암호화
과금	확장 가능	제한적