스위치 AAA 인증

PART 11

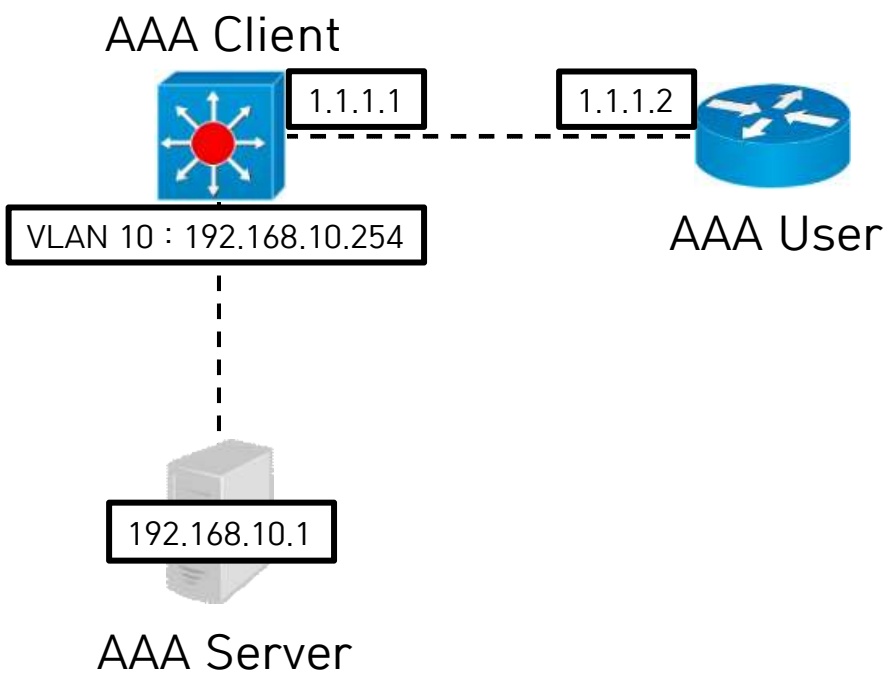
1 - 1. AAA 서버 – 계정 및 인증

. AAA (Authentication, Athorization, Account)

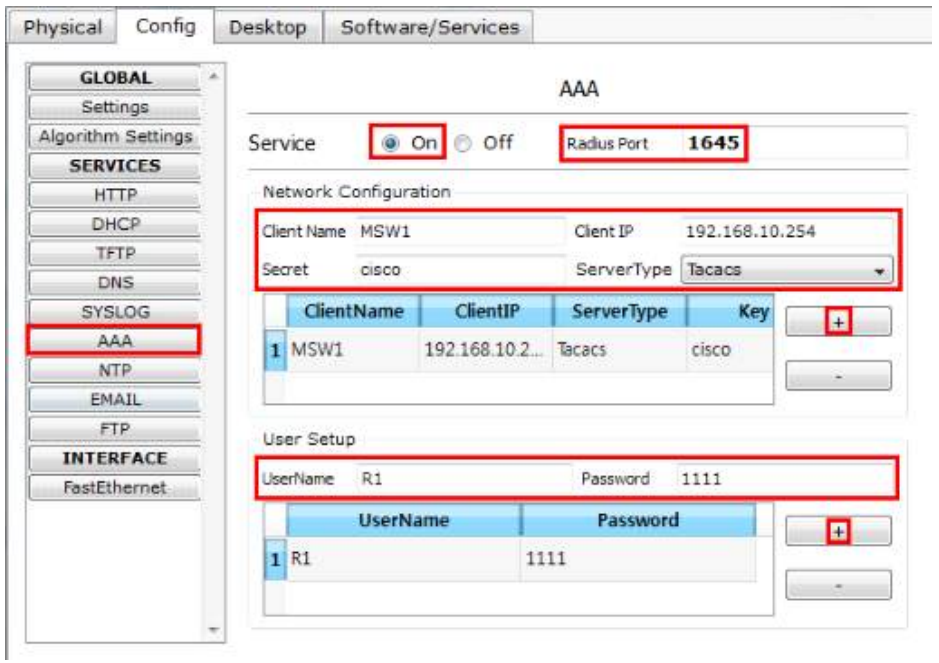
계정(Account)을 만들고 인증(Authentication)하고 권한(Athorization)을 부여하는 기능을 담당하는 서버.

AAA는 Radius와 Tacacs(UDP), Tacacs+(TCP) 프로토콜을 사용.

AAA 서버 : 계정의 생성 및 관리(권한, 인증)
AAA 클라이언트 : 자신에 대한 인증을 AAA 서버를 통해 받을 수 있도록 설정.
AAA 유저 : AAA 클라이언트에 대한 계정, 인증, 권한을 받기 위해 AAA 서버에 대한 설정을 해야함.



1) AAA 서버 설정



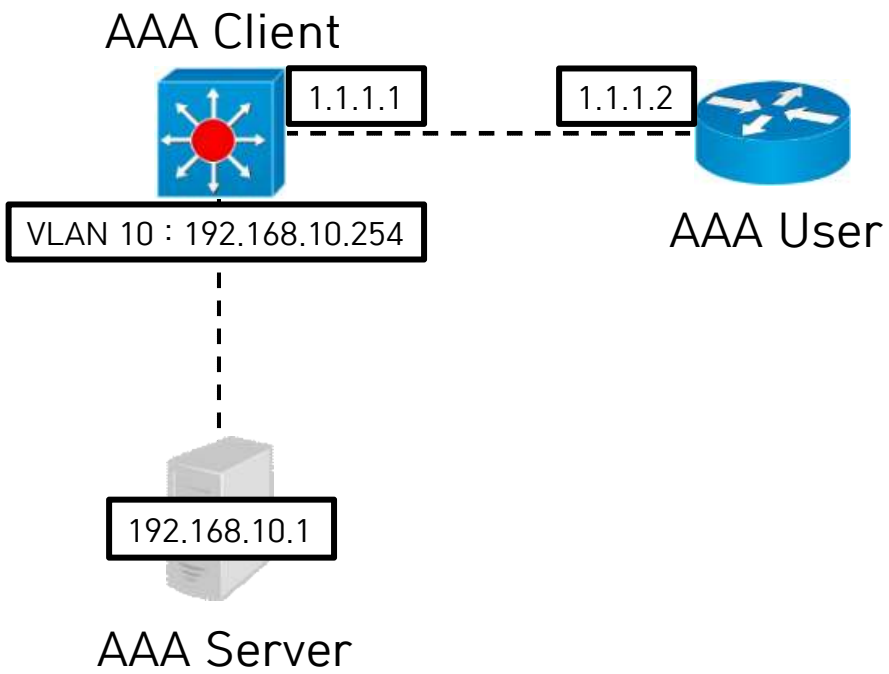
1 - 2. AAA 서버 - 계정 및 인증

. AAA (Authentication, Athorization, Account)

계정(Account)을 만들고 인증(Authentication)하고 권한(Athorization)을 부여하는 기능을 담당하는 서버.

AAA는 Radius와 Tacacs(UDP), Tacacs+(TCP) 프로토콜을 사용.

AAA 서버 : 계정의 생성 및 관리(권한, 인증)
AAA 클라이언트 : 자신에 대한 인증을 AAA 서버를 통해 받을 수 있도록 설정.
AAA 유저 : AAA 클라이언트에 대한 계정, 인증, 권한을 받기 위해 AAA 서버에 대한 설정을 해야함.



2) AAA 클라이언트 설정

MSW1(config)# aaa new-model
aaa 서버 시작
MSW1(config)# aaa authentication login default group tacacs+ local
Tacacs+ 서버 인증을 거치되 접속 실패 시 위에 설정한 유저 이름과 암호로 접속
MSW1(config)# tacacs-server host 192.168.10.1
Tacacs+ 서버 주소
MSW1(config)# tacacs-server key cisco
tacacs+ 서버 Secret key 값

MSW1(config)# line console 0
MSW1(config-line)# login authentication default
console로 접속 시 기본으로 위의 인증 방식을 거친다.
MSW1(config-line)# exit

MSW1(config)# line vty 0 4
MSW1(config-line)# login authentication default
텔넷으로 접속 시 기본으로 위의 인증 방식을 거친다.

MSW1(config)# username msw password 2222
Tacacs+ 서버에 장애 발생 시 이 유저 이름으로 접속하게 됨.

MSW1(config)# enable password cisco
Privilege 모드로 진입 가능하게 함. (사용 권한 레벨 15)

3) AAA 유저에서 접속

telnet 192.168.10.254

1 - 3. AAA 서버 - 권한

. Athorization

1) 사용자 별 권한 수준 (Privilege Level)을 지정
2) 권한 수준 별 사용 가능한 명령어를 지정
3) 콘솔 및 텔넷 접속 시 인증 방식을 로컬(login local)로 지정

라우터나 스위치의 명령어 사용 권한은 0 ~ 15까지 16단계로 구분
(미리 정의된 권한 수준은 0, 1, 15가 있음)

사용 권한 0 : disable, enable, exit, help, logout
사용 권한 1 : 설정 및 중요한 내용을 제외하고, 기본적인 장비의 동작을 확인하고 장애를 처리할 수 있는 명령어들을 사용할 수 있음 (확장 ping을 제외)
사용 권한 15 : 모든 명령어를 사용할 수 있는 최상위 권한

```
Router>show privilege
Current privilege level is 1
Router>enable
Password:
Router#show privilege
Current privilege level is 15
```

AAA 클라이언트에서 설정 - AAA 서버 없이 로컬에서 권한 부여

MSW1(config)# username user1 privilege 5 password 1111
user1으로 접속하는 사용자는 사용 권한 레벨이 5가 됨. (기본은 레벨 1)

레벨 5에서 사용할 수 있는 주요 명령어 : show ip int brief

패킷 트레이서에서는 권한 부여를 못함.
Cisco ACS 같은 프로그램을 통해서 권한 부여 가능