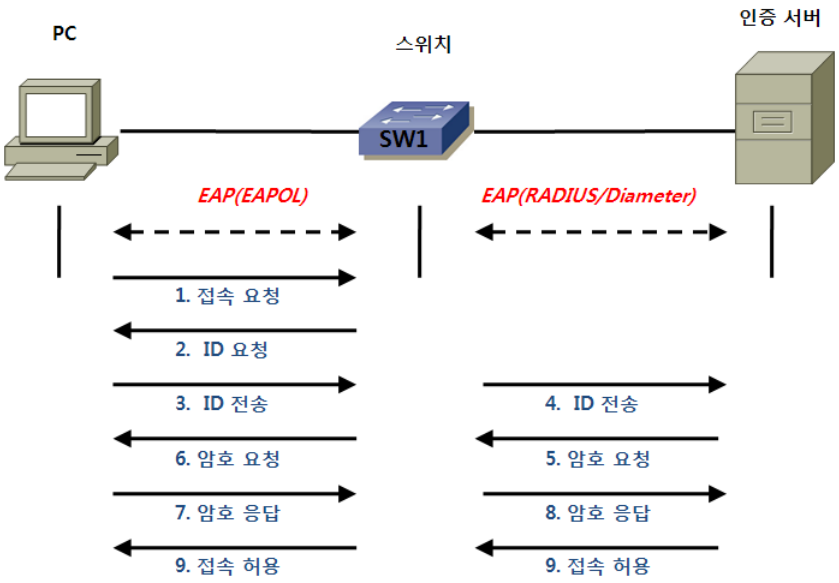
802.1X 인증

1. 802.1X 인증?

○ 인증서버를 이용하여 특정 장비의 접속을 제어하는 방법
- 802.1X를 사용하려면 PC와 스위치 및 인증서버 모두가 이 기능을 지원해야 한다.
- 공공장소에서 접속이 가능한 스위치나 무선랜 Access Point에서 많이 사용하는 인증방식

2. 802.1X 동작 방식

[그림 802.1X 인증 절차]



802.1X 인증을 위해 EAP(Extensible Authentication Protocol)라는 프로토콜이 사용된다. PC와 스위치간에는 EAP가 EAPOL (EAP over LAN) 프레임으로 인캡슐레이션되어 송수신된다. 스위치와 AAA 서버 사이에는 EAP가 RADIUS 패킷으로 인캡슐레이션되어 송수신된다.

3. 스위치에서의 802.1X 설정

- 특정 스위치 포트에 802.1X 인증을 설정하면 인증을 통과하기 전에는 EAPOL, STP 및 CDP 프레임만 허용된다. 인증 후에는 정상적 통신이 이루어진다.
- 802.1X는 정적인 액세스 포트, 보이스 VLAN 포트 및 L3 Routed 포트에서만 지원된다.
- 트렁크 포트, 동적인 포트, EtherChannel, SPAN의 목적지 포트에서는 지원되지 않는다.

○ AAA 활성화 및 RADIUS 서버 지정

```
SW(config)# aaa new-model
SW(config)# radius-server host 1.1.1.100 key cisco
```

○ 테스트

```
SW# test aaa group radius dot1x cisco legacy
```

- 이용자명(dot1x)과 암호(cisco)는 AAA 서버에서 설정한 것과 동일한 것을 사용해야 한다.

○ 콘솔 포트를 위한 설정

```
SW(config)# aaa authentication login CON-AUTH line none
SW(config)# line console 0
SW(config-line)# login authentication CON-AUTH
```

- 스위치의 콘솔포트 접속시에는 AAA 인증을 하지 말고 콘솔포트에 설정된 암호를 사용하거나 없으면 인증을 하지 않고 접속하게 한다. (만약의 경우 콘솔 접속이 불가능해지는 것을 방지)

○ 802.1X 인증 관련 설정

```
SW(config)# aaa authentication dot1x default group radius
SW(config)# aaa authorization network default group radius
SW(config)# dot1x system-auth-control
```

- RADIUS 서버를 이용하여 802.1X 인증을 하겠다는 설정
- RADIUS 서버에서 Vlan을 할당받거나 이용자별 ACL을 다운받기 위한 설정
- 스위치에 802.1X 인증을 활성화

○ 포트에 802.1X 인증 활성화

```
SW(config)# int f0/1
SW(config-if)# switchport mode access
SW(config-if)# dot1x port-control auto
```

- 정적인 스위치포트 설정
- 802.1X 포트의 상태를 지정

  auto: 802.1X 동작

  force-authorized: 강제 인증 = 항상 인증된 상태. 어떤 장비라도 접속해 네트워크 사용가능

  force-unauthorized: 강제 불인증 = 해당 포트 사용 못하게 설정

○ Guest VLAN 설정

```
SW(config)# vlan 999
SW(config-vlan)# name Guest-VLAN
```

```
SW(config)# int f0/1
SW(config)# dot1x guest-vlan 999
```

- 802.1X 인증 기능이 없는 장비들에게는 **Guest VLAN**이 할당된다. Guest VLAN에서 사용할 수 있는 네트워크 자원은 별도로 지정한다.

○ 제한 VLAN 할당

```
SW(config)# vlan 998
SW(config-vlan)# name Auth-Fail-VLAN

SW(config)# int f0/1
SW(config-if)# dot1x auth-fail vlan 998
```

- 회사 방문자와 같이 802.1X 인증기능이 있지만, 이용자명과 암호를 모르는 사람들을 위한 **Auth-Fail VLAN**을 만든다. Guest VLAN과 마찬가지로 Auth-Fail VLAN에서 사용할 수 있는 네트워크 자원은 별도로 지정한다.

○ 제한 VLAN 사용자를 위한 설정

```
SW(config)# ip access-list extended InternetOnly
SW(config-ext-nacl)# permit udp any host 255.255.255.255 eq 67
SW(config-ext-nacl)# permit icmp any host 1.1.1.254 echo-replay
SW(config-ext-nacl)# deny ip any 1.0.0.0 0.255.255.255
SW(config-ext-nacl)# permit ip any any

SW(config)# int vlan 998
SW(config-if)# ip access-group InternetOnly in
```

- Auth-Fail VLAN에서 사용할 수 있는 네트워크 자원 등은 별도로 지정한다.
- 예를 들어, 사내 IP 대역이 1.0.0.0/8이고, 게이트웨이 및 DHCP 서버가 1.1.1.254인 경우, Auth-Fail VLAN 사용자가 인터넷만 하게 설정할 경우

○ IAB 설정

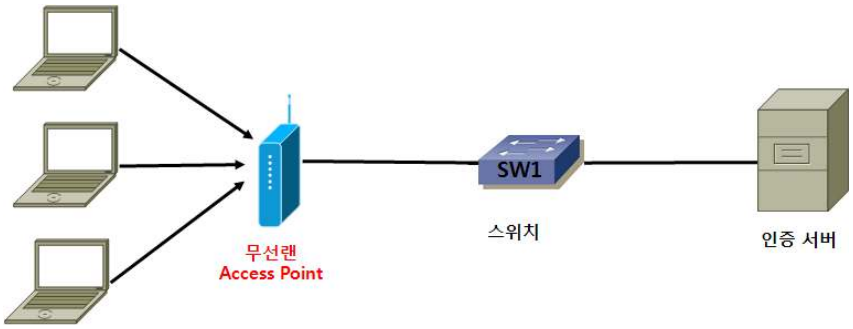
```
SW(config)# vlan 1000
SW(config-vlan)# name Critical

SW(config)# int f0/1
SW(config-if)# dot1x critical vlan 1000
```

- **Critical Port**: Radius 서버가 다운되어 인정을 못받은 포트
- **IAB(Inaccessible Authentication Bypass)**: 크리티컬 포트에 특정한 Vlan을 할당하는 것
- 크리티컬 포트에 할당한 Vlan에서 사용할 수 있는 네트워크 자원 등은 별도로 지정하는 것이 좋다.
- dot1x critical 명령 다운에 Vlan 번호를 지정하지 않으면 포트에 switchpot access vlan 명령어로 설정된 Vlan이 설정된다.

○ 802.1 복수 호스트 지원 설정

SW(config)# int f0/1

SW(config-if)# **dot1x host-mode multi-host**



- 스위치의 F0/1 포트에 무선랜 Access Point가 연결되어 있다면 해당 포트로 복수개의 장비가 접속되어야 한다. 이때에는 복수개의 호스트를 지원할 수 있도록 설정해야 한다.

○ 802.1X 관련 설정 확인

SW# show dot1x

○ 802.1X 관련 설정 및 동작 확인

SW# show dot1x int f0/1 details

○ 802.1X 관련 통계 확인

SW# show dot1x int f0/1 statistics