LAN Security와 Device Hardening

1.Access Control

접근제어

- ✓ 네트워크 장비에서 다양한 인증 수행을 접근 제어
- ✓ 로컬 인증, **AAA, 802.1x**등 사용
- ✓ 인증 방식에 따라 다양한 수준의 보안 제공

로컬인증

- 가장 간단한 원격 액세스 인증 방법
  - **Console, vty line, aux port**에서 로그인 및 암호 조합 구성
  - 암호는 일반 **text**로 전송
  - 암호를 가진 사람은 누구나 접근

- **sw(config)# line vty 0 15**
- **sw (config-line)# password cisco**
- **sw (config-line)# login**

- 공유 암호 대신 로컬 **username/password** 쌍을 구성할 수 있음

- **sw(config)# username user1 secret cisco**
- **sw (config)# line vty 0 4**
- **sw (config-line)# login local**
- **sw (config-line)# no password**

SSH 구성

- **Telnet(tcp 23)**은 로그인 정보 및 데이터가 일반 **text**로 전송

- **SSH(Secure Shell:tcp 22)**의 특징
  - 원격 접근의 보다 안전한 형태
  - **Username/password**요구
  - 로컬**DB**이용한 인증가능
  - 암호화된 형태 전송

- **SSH** 구성 단계
  - **1**단계 : **ssh** 설정 확인 **(#sh ip ssh)**
  - **2**단계 : 도메인 설정 **((config)# ip domain-name cisco.com)**
  - **3**단계 : **RSA key pair** 생성 및 **ssh enable ((config)#crypto key generate rsa)**
  - **4**단계 : **line vty** 설정 변경
- **sw(config)# line vty 0 15**
- **sw(config-line)# login local**
- **sw(config-line)# transport input ssh**
  - **5**단계: **username/password** 설정 및 **ssh** 설정 확인

Switch port Hardening

- **Switch port**의 특징
  - **No shut**
  - **Auto-negotiation**
  - **Default vlan(vlan1)**
  - 특별한 설정 없이 바로 사용 가능
  - 보안상 취약

- 미사용 스위치 포트에 대한 권장사항
  - **shutdown**
  - **Access mode**로 설정
  - 사용하지 않는 **VLAN**에 소속
  - **Native VLAN** 변경

```
sw(config)# vlan 999
sw(config-vlan)# name Blackhole
sw(config-vlan)# int range fa0/1-5
sw(config-range-if)#shut
sw(config-range-if)#switchport mode
access
sw(config-range-if)#switchport access
vlan 999
```

AAA

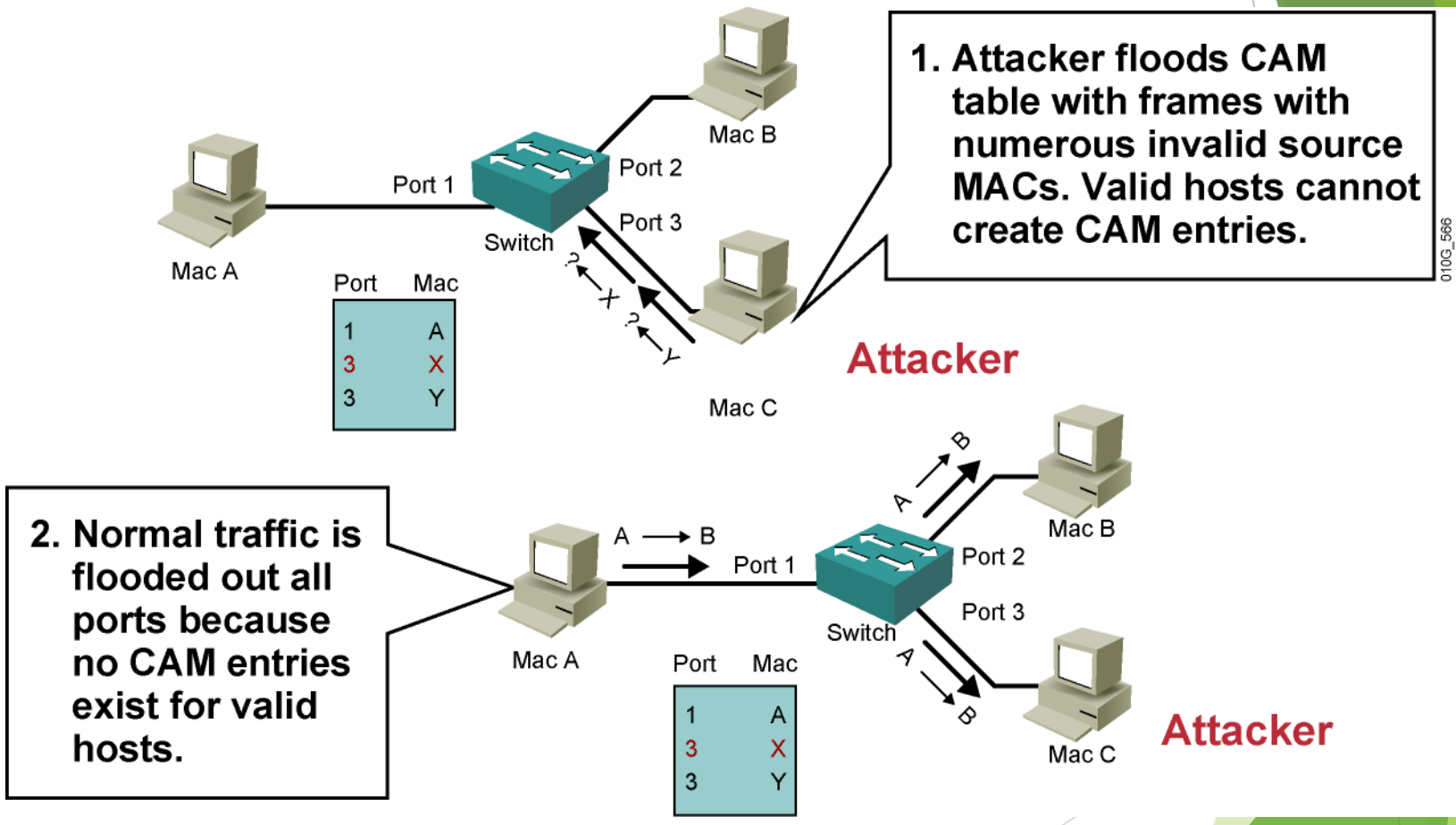
- 로컬 인증은 확장성이 떨어짐.
- 외부 서버 이용
- **Cisco**는 **AAA** 프레임워크 지원
- **Cisco** 장비는 두가지 **AAA** 인증 프로토콜 지원
  - **TACACS+**
  - **RADIUS**

802.1x

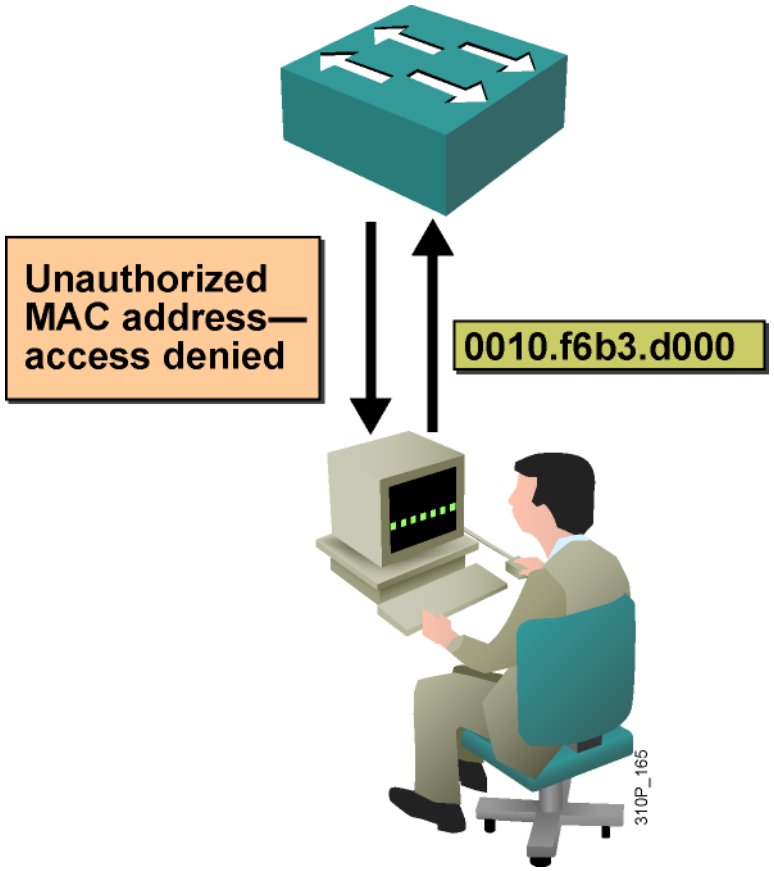
- 표준 포트 기반 접근 제어 및 인증 프로토콜
- 스위치, **AP**등 **LAN**에서 사용 가능한 장비를 통한 임의의 접근 제어
- **802.1x** 지원 포트에 연결되는 장비 사용자는 **username/password** 필요
- **802.1x** 구성요소
  - **Client(supplicant)**
  - **Switch(authenticator)**
  - **Authentication Server**

2. Port Security

MAC Flooding Attack



Port Security



- Port security는 Port로 접근하는 MAC주소의 수를 제한한다.

Port Security 구성 단계

- 1단계 : access 모드로 설정
- 2단계 : 포트 보안 설정
- 3단계 : 최대 허용 MAC 수 설정
- 4단계 : 보안 위반시 Action {protect | restrict | shutdown} 정의
- 5단계 : MAC 학습 방법 정의

Port Security 구성예

```
sw(config)# interface range fa 0/1 - 5
sw(config-if-range)# switchport mode access
sw(config-if-range)# switchport port-security
sw(config-if-range)# switchport port-security maximum 1
sw(config-if-range)# switchport port-security violation restrict
sw(config-if-range)# switchport port-security mac-address sticky
```

```
sw# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)       (Count)
Fa0/1           1             1             0              Restrict
Fa0/2           1             0             0              Restrict
Fa0/3           1             0             0              Restrict
Fa0/4           1             0             0              Restrict
Fa0/5           1             0             0              Restrict
                                    :
```

Port Security 구성확인

```
Switch#show port-security
```

- 모든 **Port**의 **Port-Security** 정보 확인

```
Switch#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                   (Count)        (Count)       (Count)
-----------------------------------------------------------------------

Fa5/1                 11             11             0             Shutdown
Fa5/5                 15             5              0             Restrict
Fa5/11                5              4              0             Protect
-----------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
```

3. LAN Threat Mitigation

LAN Threat

- LAN 공격의 종류
  - VLAN 공격
  - DHCP 공격
  - ARP 공격
- LAN 공격을 완화 시키는 기본 설정
  - Native VLAN
  - 관리 VLAN

VLAN 공격

- **VLAN 공격**
  - **Spoofing DTP 메시지**
  - **Rogue 스위치 이용 트렁크 활성화**
  - **Double-tagging 공격**

- **VLAN 공격 완화 방법**
  - **1단계 : 트렁크 포트가 아닌 포트에 대해 DTP 기능 비활성화(switchport mode access)**
  - **2단계 : 사용되지 않는 포트는 사용되지 않는 VLAN으로 설정(switchport access vlan 999)**
  - **3단계 : 트렁크 포트는 수동으로 활성화(switchport mode trunk)**
  - **4단계 : 트렁킹 포트에 대한 DTP 기능 비활성화(switchport nonegotiate)**
  - **5단계 : 네이티브 VLAN을 VLAN 1이 아닌 다른 VLAN으로 설정(switchport trunk native vlan 86)**

DHCP 공격

- **DHCP 공격**
  - **DHCP Starvation 공격(gobbler)**
  - **DHCP Spoofing 공격**
- **DHCP Snooping**
  - **Trusted ports**
  - **Untrusted ports, server messages**
  - **Untrusted ports, client messages**
  - **Rate limiting : 초당 받는 DHCP 메시지의 수 제한**

DHCP snooping 설정

```
sw(config)# ip dhcp snooping
sw(config)# interface f0/1
sw(config-if)# ip dhcp snooping trust
sw(config-if)# interface range f0/6 - 10
sw(config-if-range)# ip dhcp snooping limit rate 6
sw (config-if)# exit
sw(config)# ip dhcp snooping vlan 2

sw# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 2
:
sw# show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------- ---------- ------------- ---- ----------------
00:01:23:B5:6F:89  192.168.10.10   193185     dhcp-snooping 2    FastEthernet0/6
```

ARP 공격

- Gratuitous ARP
  - ARP Spoofing
  - ARP Poisoning
  - MITM
- DAI(Dynamic ARP Inspection)
  - DHCP Snooping 요구

DAI 설정

```
sw(config)# ip dhcp snooping
sw(config)# ip dhcp snooping vlan 2
sw(config)# ip arp inspection vlan 2
sw(config)# interface fa0/1
sw(config-if)# ip dhcp snooping trust
sw(config-if)# ip arp inspection trust

sw(config)# ip arp inspection validate dst-mac
sw(config)# ip arp inspection validate ip
sw(config)# do show run | include validate
ip arp inspection validate ip
sw(config)# ip arp inspection validate src-mac dst-mac ip
sw(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
```