Ağ Yöneticileri Derneği
CCNA3 LAB 11 - PROJE ÇÖZÜMÜ
"Port Security" ve "DHCP Snooping" Uygulaması

AYD CCNA2v7
PORT SECURITY ve DHCP SNOOPING

PC-PT
PC1
Fa0/1
Gi0/1
VLAN3
Gi0/1
Fa0/1

Server-PT
YETKILI DHCP SERVER

IP: 192.168.3.201
SM: 255.255.255.0
DG: 192.168.3.1
DNS:8.8.8.8

Fa0/2
2960-24TT
SW1
Fa0/3
2960-24TT
SW2
Fa0/2

Layer3 IP Bilgisi:
Tüm kullanıcılar
VLAN3: 192.168.3.0/24 uzayında

PC-PT
PC2
PC-PT
PC3

HEDEFLER:
- Son kullanıcı portlarına ek switch
 takılıp kontrolsüz kullanıcı bağlanmaması için
port-security konfigurasyonu yapılacak.
- Kullanılmayan portlar kapatılacak.
- Yetkisiz DHCP sunucusu bağlanması
önlenmesi için DHCP Snooping özelliği
devreye alınacak.

Server-PT
YETKISIZ DHCP SERVER

IP: 192.168.3.202
SM: 255.255.255.0
DG: 192.168.3.1
DNS:8.8.8.8

// ADIM1:   SW1 ve SW2'de VLAN konfigurasyonu

//SW1
Switch> **enable**
Switch# **conf t**
Switch(config)# **hostname SW1**
SW1(config)# **vlan 3**
SW1(config-vlan)#**name KULLANICILAR**
SW1(config-vlan)# **exit**

SW1(config)# **interface range FastEthernet 0/1 - 3**
SW1(config-if-range)# **switchport mode access**
SW1(config-if-range)# **switchport access vlan 3**
SW1(config)# **interface Gi 0/1**
SW1(config-if)# **switchport mode access**
SW1(config-if)# **switchport access vlan 3**
SW1(config-if-range)# **end**

```
SW1#show vlan brief

VLAN Name            Status   Ports
---- --------------- -------- ------------------------------
1    default         active   Fa0/4, Fa0/5, Fa0/6, Fa0/7
                              Fa0/8, Fa0/9, Fa0/10, Fa0/11
                              Fa0/12, Fa0/13, Fa0/14, Fa0/15
                              Fa0/16, Fa0/17, Fa0/18, Fa0/19
                              Fa0/20, Fa0/21, Fa0/22, Fa0/23
                              Fa0/24, Gig0/2
3    KULLANICILAR    active   Fa0/1, Fa0/2, Fa0/3, Gig0/1
```

SW1(config)# **interface range FastEthernet** 0/4-24
SW1(config-if-range)# **shutdown**
SW1(config-if-range)# **end**
SW1# **wr**
Building configuration...
[OK]

//SW2
Switch> **enable**
Switch# **conf t**
Switch(config)# **hostname SW2**
SW2(config)# **vlan 3**
SW2(config-vlan)#**name KULLANICILAR**
SW2(config-vlan)# **exit**

SW1(config)# **interface range FastEthernet 0/1 - 2**
SW1(config-if-range)# **switchport mode access**
SW1(config-if-range)# **switchport access vlan 3**
SW1(config)# **interface Gi 0/1**
SW1(config-if)# **switchport mode access**
SW1(config-if)# **switchport access vlan 3**
SW1(config-if-range)# **end**

SW1(config)# **interface range FastEthernet** 0/3-24
SW1(config-if-range)# **shutdown**
SW1(config-if-range)# **end**
SW1# **wr**
Building configuration...
[OK]

//SW1
SW1(config)#interface FastEthernet 0/1
SW1(config-if)# switchport port-security   // port-security açıldı. default'ta max:1MAC, ihlalde port kapatılır.
SW1(config-if)# switchport port-security maximum 1
SW1(config-if)# switchport port-security violation protect

SW1(config)#interface range FastEthernet 0/2 - 3
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 1
SW1(config-if)# switchport port-security violation protect

TÜM SEÇENEKLER:
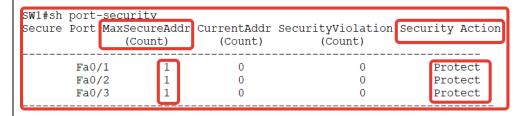SW1(config-if)# **switchport port-security violation protect**
PORT AÇIK KALACAK, LOG TUTULMAYACAK, BELİRTİLEN ADRESTEN FAZLA BAĞLANAN KİŞİLERE İZİN VERİLMEYECEK.
SW1(config-if)# **switchport port-security violation restrict**
PORT AÇIK KALACAK, LOG SUNUCUSUNA LOG İLETİLECEK,BELİRTİLEN ADRESTEN FAZLA BAĞLANAN KİŞİLERE İZİN VERİLMEYECEK.
SW1(config-if)# **switchport port-security violation shutdown** (default mode)
PORT "SHUTDOWN" KAPATILACAK.

```
SW1#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
             (Count)       (Count)      (Count)
--------------------------------------------------------------------------
     Fa0/1        1            0              0           Protect
     Fa0/2        1            0              0           Protect
     Fa0/3        1            0              0           Protect
--------------------------------------------------------------------------
```

- Yetkisiz DHCP sunucusu IP dağıtmaktadır. Bu sunucu herhangi bir porta takılı bir bilgisayar olabilir.
- IP Dağıtımının önüne geçmek için **DHCP Snooping** özelliği devreye alınacak. DHCP Snooping özelliği açıldıktan sonra sadece **trusted** portlardan DHCP Sunucu paketleri iletilebilir.

SW1(config)# **ip dhcp snooping**
SW1(config)# **interface Gi 0/1**
SW1(config-if)# **ip dhcp snooping trust**
SW1(config-if)# **exit**
SW1(config)# **ip dhcp snooping vlan 3**
SW1(config)# **end**
SW1#

SW1# **show ip dhcp snooping**

Switch DHCP snooping is enabled
DHCP snooping is configured on following **VLANs: 3**
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface   Trusted   Rate limit (pps)
---------------------- -------   ----------------
GigabitEthernet0/1   **yes**   unlimited

SW2(config)# **ip dhcp snooping**
SW2(config)# **interface Fa 0/1**
SW2(config-if)# **ip dhcp snooping trust**
SW2(config-if)# **exit**
SW2(config)# **ip dhcp snooping vlan 3**
SW2(config)# **end**
SW2#

SW2# **show ip dhcp snooping**

Switch DHCP snooping is enabled
DHCP snooping is configured on following **VLANs: 3**
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface   Trusted   Rate limit (pps)
---------------------- -------   ----------------
FastEthernet0/1   **yes**   unlimited

//Bundan sonra SW2'deki "YETKİSİZ DHCP SUNUCUSU" IP talebine cevap vermek istediğinde Fa 0/2 portu UNTRUSTED olduğu için Switch SUNUCU'nun gönderdiği DHCP paketlerini bloklayacak. PC'lerde DHCP'den IP adresi alınması sağlandığında gerçek YETKİLİ DHCP SUNUCU tarafından IP adresi atandığı görülebilir.