KABLOLU AĞLARDA DHCP SNOOPING VE ARP INSPECTION İLE GÜVENLİK ARTTIRIMI

VIII. ULAKNET ÇALIŞTAYI

A. Onur YURTSEVER

ODTÜ

Bilgi İşlem Daire Başkanlığı - Ağ Grubu

İçerik

- Kablolu Ağlar ve Avantajları
- Kablolu Ağlarda Statik IP Kullanımı
- Kablolu Ağlarda DHCP Kullanımı
- Kablolu Ağlarda 2. ve 3. Katmanlar Arası Güvenlik
- Kablolu Ağlarda DHCP Güvenliği
- Kablolu Ağlarda ARP güvenliği
- Kablolu Ağlarda Kaynak Adres Güvenliği
- IPv6'da 2. ve 3. Katmanlar Arası Güvenlik

Kablolu Ağlar

- Kablolu ağlarda süreklilik ve güvenlik
  - Kablolu ağ tercih nedenleri
    - Süreklilik
    - Performans
    - Kullanım kolaylığı
  - Kritik işlerde kullanım
    - Garanti edilebilen performans ve süreklilik
- Kablolu ağlarda kullanım kolaylığı
  - Kullanıcı bilgisayarlarının eklenmesi
    - Ayar gerektirmeyen tasarımlar mümkün
    - Kolay bağlantı
    - Daha az güvenlik kaygısı, daha az şifreleme ihtiyacı

Kablolu Ağlarda Statik IP Kullanımı

- Kullanım Zorlukları
  - Kullanıcı tarafında ayar gereksinimi
    - Kullanıcı açısından zorluk
    - Hatalı ayar sorunları
  - IP değiştirme zorluğu
- Gereksiz/Fazladan IP Kullanımı
  - Nadiren çalışan istemciler
  - Farklı zamanlarda çalışan istemciler
- Güvenlik Problemleri
  - ARP Poisoning
  - IP Source Spoofing
  - Yetkilendirme

Kablolu Ağlarda DHCP Kullanımı

- Kullanım kolaylıkları
  - Kullanıcı ayar gereksinimi yok
- Gereksiz IP kullanımı yok
- Belli MAC adreslerine IP vermek mümkün
- Statik IP vermek mümkün
- Güvenlik problemleri
  - Yetkisiz DHCP
    - Bilinçsiz
    - Bilinçli, saldırı amaçlı
  - ARP Poisoning
  - IP Source Spoofing
  - Yetkilendirme

Kablolu Ağlarda 2. ve 3. Katmanlar Arası Güvenlik

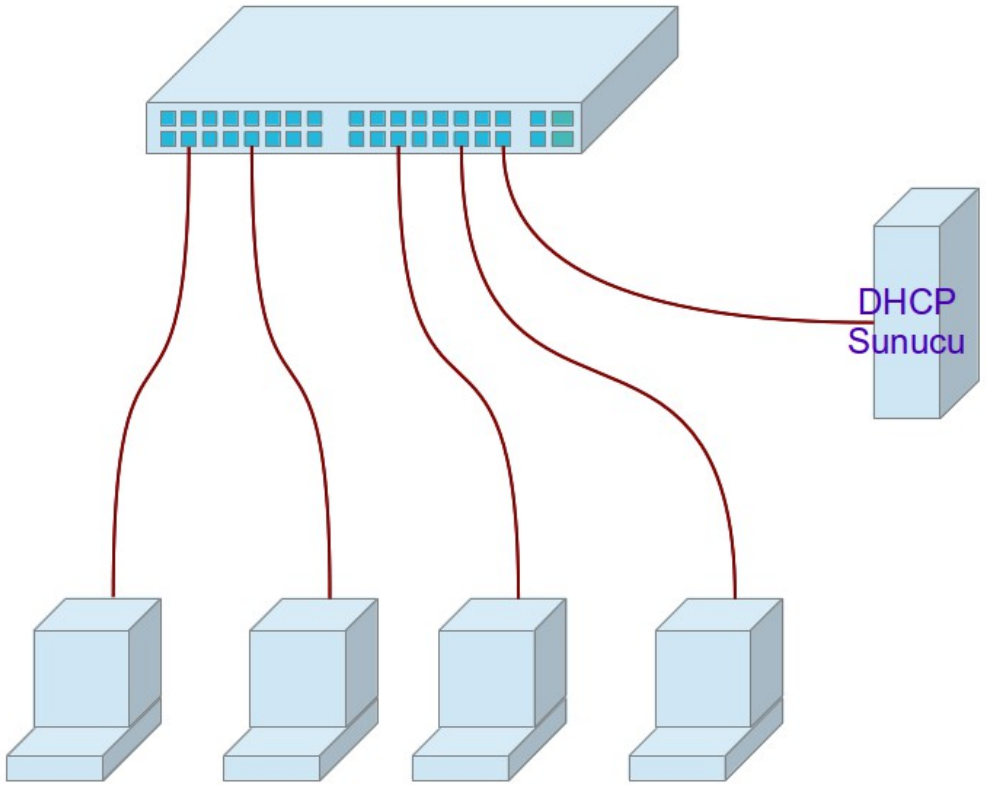
- DHCP Güvenliği
  - DHCP Snooping
  - Option 82
- ARP Güvenliği
- IP Kaynak Güvenliği

DHCP Güvenliği

- DHCP Snooping
  - Yetkisiz DHCP
  - Trusted Port
  - DHCP Snooping Binding
- Option 82
  - Cihaz Bilgisi
  - Port Bilgisi
  - Vlan Bilgisi

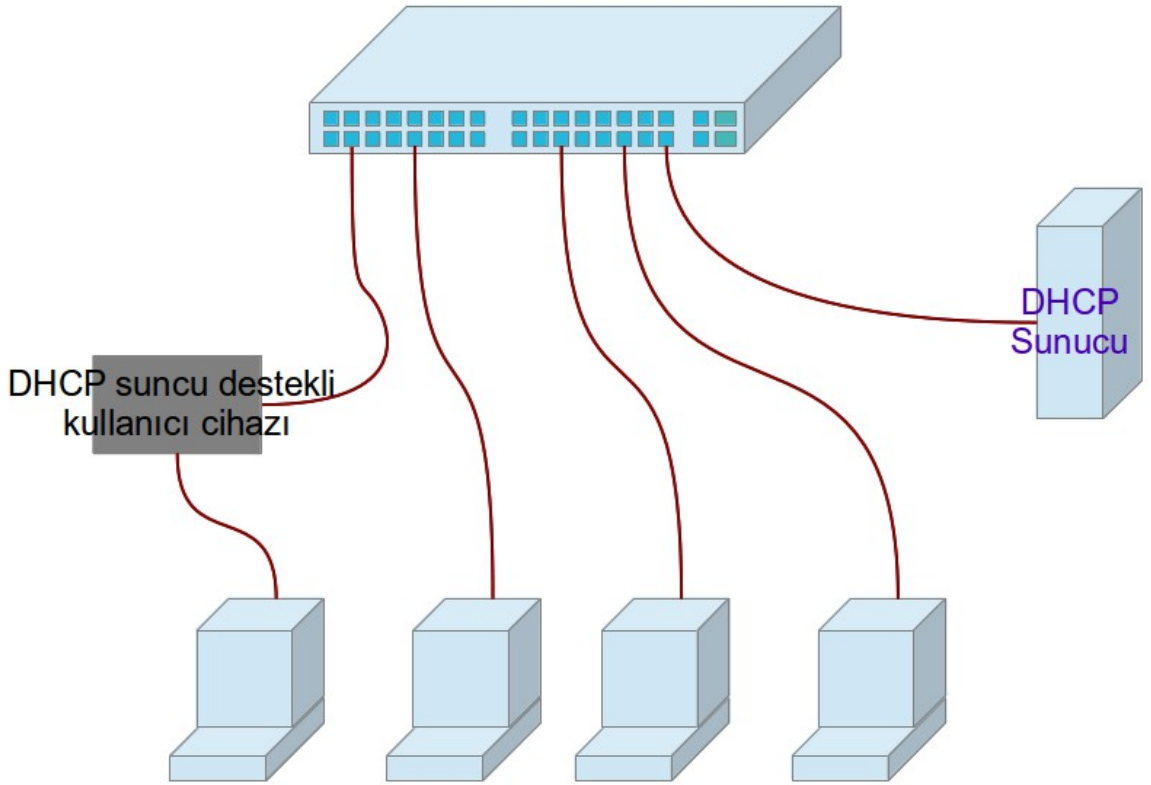
DHCP Güvenliği

- Normal durum



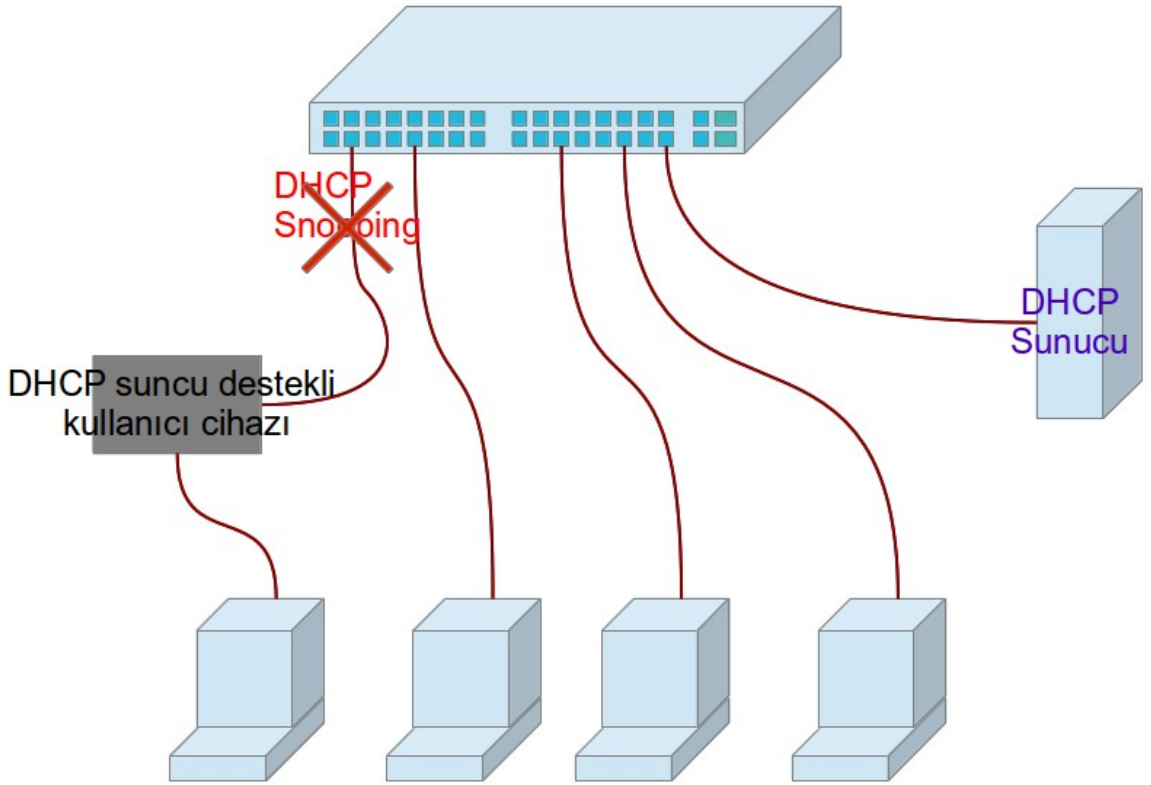
DHCP Güvenliği

- Yetkisiz DHCP (Snooping Kullanılmadığında)



DHCP Güvenliği

- Yetkisiz DHCP (Snooping Kullanıldığında)



DHCP Güvenliği

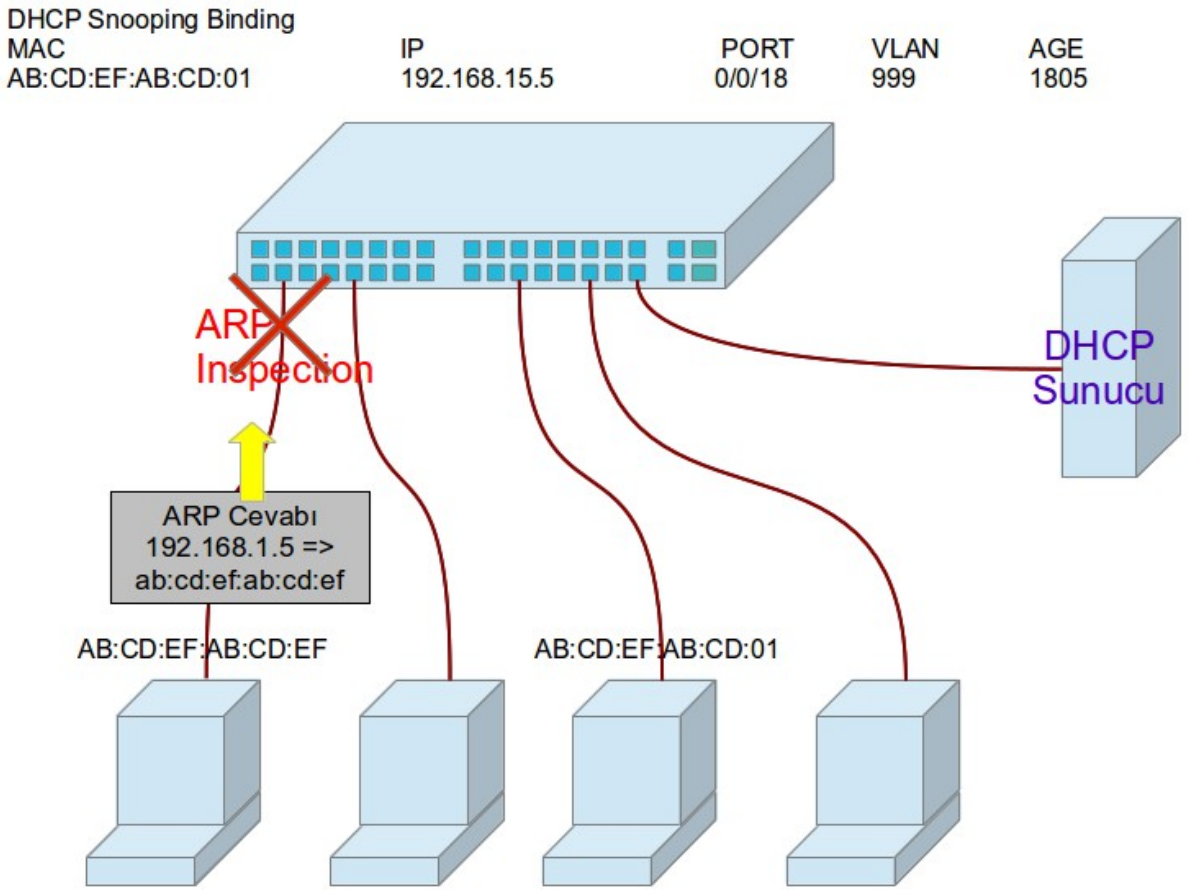
- DHCP Snooping Binding

MAC	IP	PORT	VLAN	AGE
AB:CD:EF:AB:CD:01	192.168.15.5	0/0/15	999	1805
AB:CD:EF:AB:CD:02	192.168.15.6	0/0/16	999	1810
AB:CD:EF:AB:CD:03	192.168.15.7	0/0/17	999	1845
AB:CD:EF:AB:CD:04	192.168.15.8	0/0/17	999	1812
AB:CD:EF:AB:CD:05	192.168.15.9	0/0/18	999	1803
AB:CD:EF:AB:CD:06	192.168.15.10	0/0/19	999	1840

ARP Güvenliği

- ARP Inspection
  - ARP paketlerini kontrol eder
  - Genellikle DHCP Snooping ile kullanılır
    - Static Binding de olanaklı
  - Trusted Port
  - Kontrol modları
- Kullanılmadığı durumlardaki olası sorunlar
  - Man in The Middle
  - ARP Poisoning
  - Hatalı yapılandırma kaynaklı bağlantı sorunları
    - İstemcinin bağlanamaması
    - Tüm ağın çalışamaz hale gelmesi

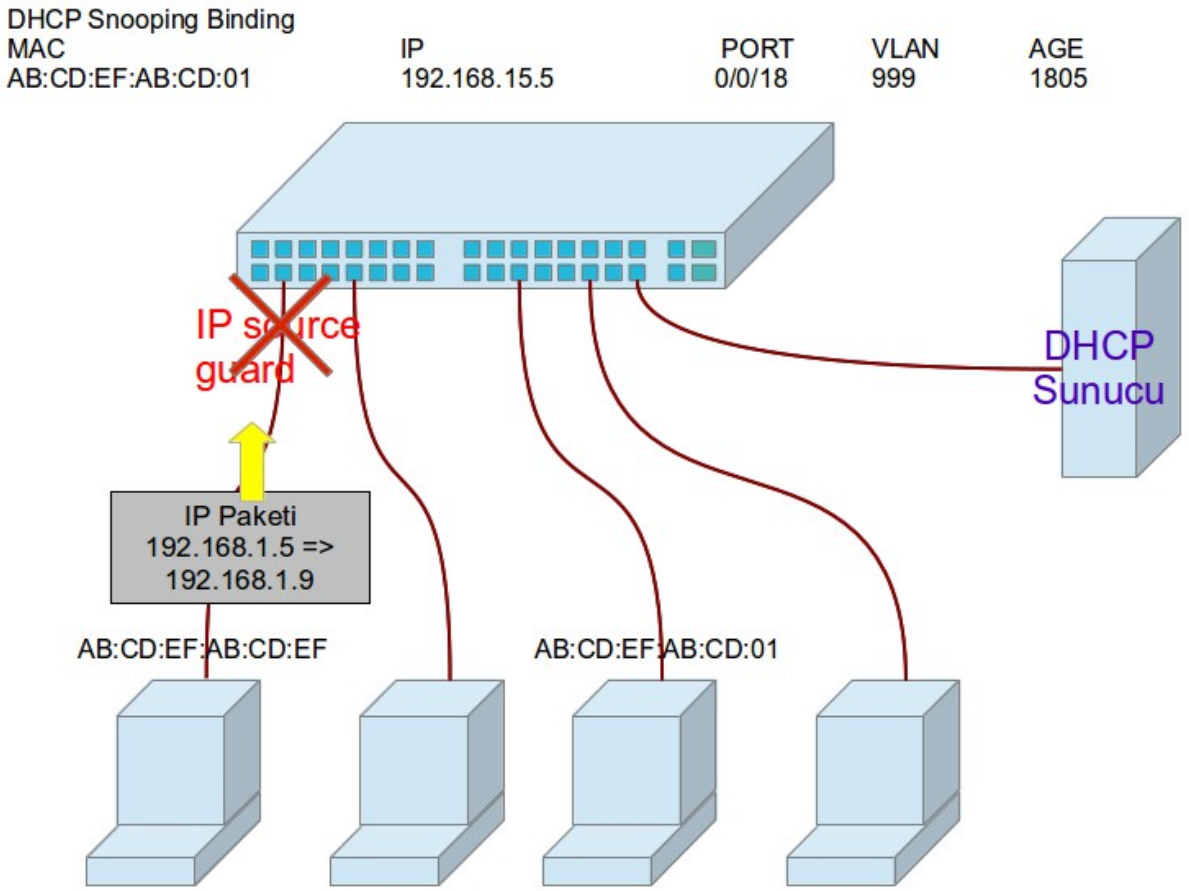
ARP Güvenliği



IP Kaynak Adres Kontrolü

- IP Source Guard
  - IP paketlerinin kaynak adreslerini kontrol eder
  - Genellikle DHCP Snooping ile beraber kullanılır
    - Static Binding de olanaklı
  - Trusted Port
- Kullanılmadığı durumlardaki sorunlar
  - Kaynak yanıltan DOS saldırıları
  - DDOS görünümlü DOS saldırıları
  - Sahte kaynak ile kaynak IP sahibine DOS

IP Kaynak Adres Kontrolü



IPv6

- Henüz gelişme aşamasında
- IPv6 First Hop Security
  - DHCP6 Snooping
  - ND Snooping
- IPv6 kullanılmasa bile önemli

Teşekkürler...

Sorular ?