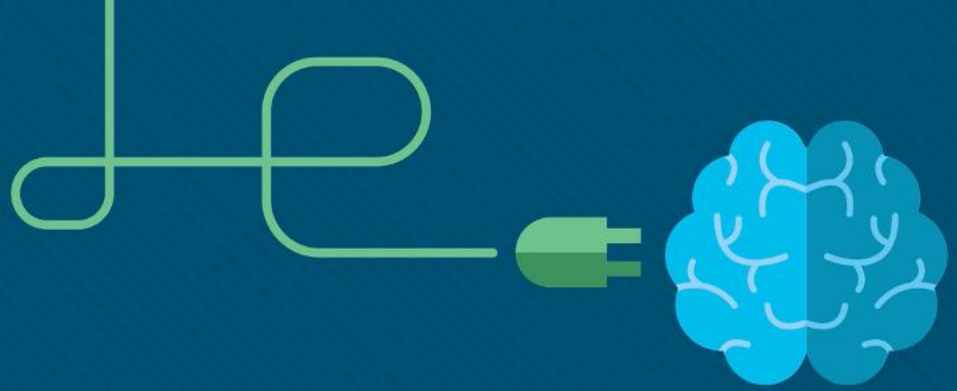


Modül 7: Adres Çözünürlük

Ağ Aygıtları ve İlk Yapılandırma (INET)

Modül Hedefleri

Modül Başlığı: Adres Çözümlemesi

Modül Amacı:ARP'nin yerel alan ağında iletişime nasıl olanak sağladığını açıklayın.

Konu Başlığı	Konu Amaç
ARP	ARP'nin amacını açıklar.

7.1 ARP

ARP Genel Bakış

• Ağınız IPv4 iletişim protokolünü kullanıyorsa, IPv4 adreslerini MAC adreslerine eşlemek için ARP'ye ihtiyacınız vardır.

• Ethernet ağındaki her IP aygıtının benzersiz bir Ethernet MAC adresi vardır.

• Bir cihaz bir Ethernet Katman 2 çerçevesi gönderdiğinde, bu iki adresi içerir:

- **Hedef MAC adresi**aynı yerel ağ segmentindeki hedef aygıtın Ethernet MAC adresidir. Hedef ana bilgisayar başka bir ağdaysa, çerçevedeki hedef adresi varsayılan ağ geçidinin (yani yönlendiricinin) adresi olur.
- **Kaynak MAC adresi**kaynak bilgisayardaki Ethernet NIC'nin MAC adresidir.

ARP Genel Bakış (Devamı)

- Aynı yerel IPv4 ağındaki başka bir ana bilgisayara bir paket göndermek için, ana bilgisayarın hedef cihazın IPv4 adresini ve MAC adresini bilmesi gerekir.

- Cihaz hedef IPv4 adresleri ya bilinir ya da cihaz adına göre çözümlenir, ancak MAC adreslerinin keşfedilmesi gerekir.

- Bir cihaz, IPv4 adresini bildiğinde yerel bir cihazın hedef MAC adresini belirlemek için ARP'yi kullanır ve ARP iki temel işlev sağlar:
  - IPv4 adreslerini MAC adreslerine çözümleme
  - IPv4'ten MAC adresine eşlemelerin bir tablosunun tutulması

ARP Fonksiyonları

- Bir paket, Ethernet çerçevesine kapsüllenmek üzere veri bağlantı katmanına gönderildiğinde, cihaz, IPv4 adresine eşlenen MAC adresini bulmak için belleğindeki bir tabloya başvurur.

- Bu tablo geçici olarak RAM belleğinde saklanır ve ARP tablosu veya ARP önbelleği olarak adlandırılır.

- Gönderen cihaz, hedef IPv4 adresini ve karşılık gelen MAC adresini bulmak için ARP tablosunu arayacaktır:
  - Paketin hedef IPv4 adresi, kaynak IPv4 adresiyle aynı ağda ise cihaz, ARP tablosunda hedef IPv4 adresini arar.
  - Hedef IPv4 adresi kaynak IPv4 adresinden farklı bir ağdaysa, cihaz varsayılan ağ geçidinin IPv4 adresini ARP tablosunda arar.

- Her iki durumda da arama, cihazın IPv4 adresi ve buna karşılık gelen MAC adresi için yapılır.

ARP Fonksiyonları (Devamı)

• ARP tablosunun her girişi veya satırı, bir IPv4 adresini bir MAC adresine bağlar.

• İki değer arasındaki ilişkiye harita adını veriyoruz.

• Bu, tabloda bir IPv4 adresini bulabileceğiniz ve karşılık gelen MAC adresini keşfedebileceğiniz anlamına gelir.

• ARP tablosu, LAN üzerindeki cihazlara ait eşlemeleri geçici olarak kaydeder (önbelleğe alır).

• Cihaz IPv4 adresini bulursa, çerçevede hedef MAC adresi olarak karşılık gelen MAC adresini kullanır.

• Cihaz bir giriş bulamazsa ARP isteği gönderir.

Video - ARP İşlemi - ARP Talebi

- Bir cihazın bir IPv4 adresiyle ilişkili MAC adresini belirlemesi gerektiğinde, bir ARP isteği gönderir ve ARP tablosunda IPv4 adresi için bir girişi olmaz.
- ARP mesajları, IPv4 başlığı olmaksızın doğrudan bir Ethernet çerçevesinin içine kapsüllenir.
- ARP isteği, aşağıdaki başlık bilgilerini kullanarak bir Ethernet çerçevesine kapsüllenir:
  - **Hedef MAC adresi**–LAN üzerindeki tüm Ethernet NIC'lerinin ARP isteğini kabul etmesini ve işlemesini gerektiren FF-FF-FF-FF-FF-FF yayın adresidir.
  - **Kaynak MAC adresi**–ARP isteğinin göndericisinin MAC adresi.
  - **Tip**-ARP mesajlarının tip alanı 0x806'dır.
- ARP istekleri, switch tarafından tüm portlardan (alıcı port hariç) gönderilen yayınlardır.

- LAN üzerindeki tüm Ethernet NIC'leri yayın işlemini gerçekleştirir ve ARP isteğini işlenmek üzere işletim sistemine iletmelidir.
- Her cihaz, hedef IPv4 adresinin kendi adresiyle eşleşip eşleşmediğini görmek için ARP isteğini işlemelidir.
- LAN üzerindeki yalnızca bir cihaz, ARP isteğindeki hedef IPv4 adresiyle eşleşen bir IPv4 adresine sahip olacak, dolayısıyla diğer hiçbir cihaz yanıt vermeyecektir.
- Bu videoda bir MAC adresine yönelik ARP isteği ele alınacaktır.

Video - ARP Operasyonu - ARP Cevap

- Yalnızca ARP isteğiyle ilişkili hedef IPv4 adresine sahip cihaz bir ARP yanıtıyla yanıt verecektir.

- ARP yanıtı, aşağıdaki başlık bilgilerini kullanarak bir Ethernet çerçevesine kapsüllenir:
  - **Hedef MAC adresi**–ARP isteğinin göndericisinin MAC adresi.
  - **Kaynak MAC adresi**–ARP cevabının göndericisinin MAC adresi.
  - **Tip**-ARP mesajlarının tip alanı 0x806'dır.
- Yalnızca başlangıçta ARP isteğini gönderen cihaz tekli yayın ARP yanıtını alacak ve IPv4 adresini ve karşılık gelen MAC adresini ARP tablosuna ekleyecektir.
- Bu IPv4 adresine yönelik paketler artık karşılık gelen MAC adresini kullanarak çerçevelere kapsüllenebilir.
- Bir çerçeve oluşturulamadığı için ARP isteğine hiçbir cihaz yanıt vermezse paketi düşürür.
- ARP tablosundaki girdilerin bir zaman damgası vardır, dolayısıyla bir cihaz zaman damgası süresi dolmadan önce belirli bir cihazdan bir çerçeve almazsa, ARP tablosu bu cihaz için girdiyi kaldırır.
- Ayrıca, statik harita girişleri bir ARP tablosuna girilebilir (nadiren yapılır), ancak bunlar zamanla geçerliliğini yitirmez ve manuel olarak kaldırılmalıdır.
- Bu videoda bir ARP isteğine yanıt olarak verilen bir ARP cevabı ele alınacaktır.

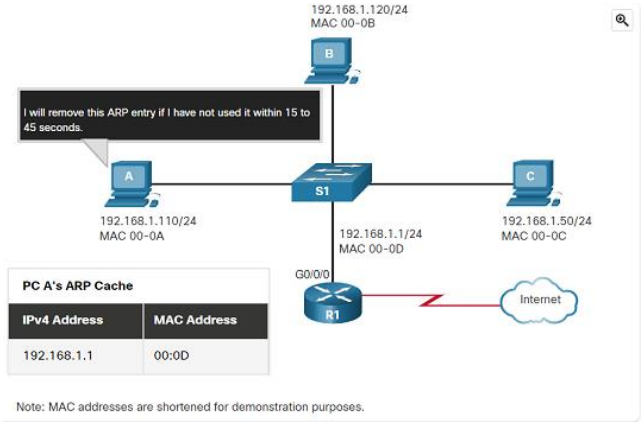
Video - Uzaktan İletişimde ARP Rolü

- Hedef IPv4 adresi kaynak IPv4 adresiyle aynı ağda değilse, kaynak aygıtın çerçeveyi varsayılan ağ geçidine (yerel yönlendiricinin arayüzü) göndermesi gerekir.
- Bir kaynak aygıt başka bir ağda IPv4 adresli bir pakete sahip olduğunda, bu paketi yönlendiricinin hedef MAC adresini kullanarak bir çerçeveye kapsüller.
- Ana bilgisayarların IPv4 yapılandırması, varsayılan ağ geçidinin IPv4 adresini depolar.
- Bir ana bilgisayar bir hedef için bir paket oluşturduğunda, iki IPv4 adresinin konumunun aynı Katman 3 ağında olup olmadığını belirlemek için hedef IPv4 adresini ve kendi IPv4 adresini karşılaştırır.

- Hedef ana bilgisayar aynı ağda değilse, kaynak, varsayılan ağ geçidinin IPv4 adresine sahip bir giriş için ARP tablosunu kontrol eder.
- Giriş yoksa, varsayılan ağ geçidinin MAC adresini belirlemek için ARP sürecini kullanır.
- Bu videoda bir ARP isteğinin bir ana bilgisayara varsayılan ağ geçidinin MAC adresini nasıl sağlayacağı anlatılacaktır.

Bir ARP Tablosundan Girişleri Kaldırma

- Belirli bir süre boyunca ARP kullanmayan her cihaz için bir ARP önbellek zamanlayıcısı bunu kaldırır.
- Süreler cihazın işletim sistemine göre farklılık göstermektedir.
- Örneğin, daha yeni Windows işletim sistemleri, şekilde gösterildiği gibi, ARP tablosu girişlerini 15 ila 45 saniye arasında depolar.
- Komutların kullanılmasıyla ARP tablosundaki bazı veya tüm girdiler manuel olarak da kaldırılabilir.
- Bir girdiyi kaldırdıktan sonra, haritayı ARP tablosuna girmek için ARP isteği gönderme ve ARP yanıtı alma işlemi tekrar gerçekleşmelidir.



Cihazlardaki ARP Tabloları

- **ip arp'yi göster**Şekilde görüldüğü gibi, bir Cisco yönlendiricisinde ARP tablosunu görüntülemek için komut kullanılır.

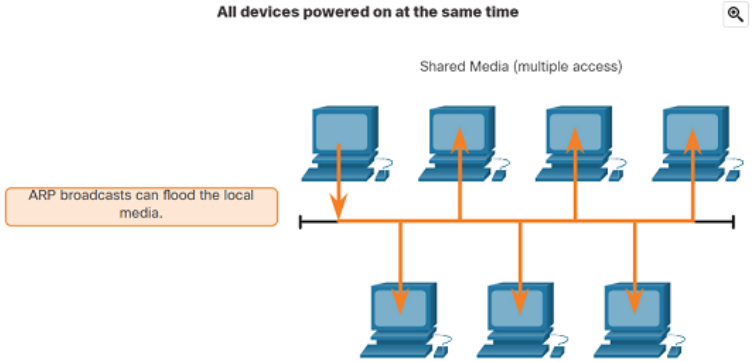
```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225         -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226         1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

- **arp- bir**Windows 10 PC'de ARP tablosunu görüntülemek için aşağıdaki komut kullanılır.

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
Internet Address      Physical Address      Type
192.168.1.1           c8-d7-19-cc-a0-86     dynamic
192.168.1.101         08-3e-0c-f5-f7-77     dynamic
192.168.1.110         08-3e-0c-f5-f7-56     dynamic
192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
192.168.1.126         24-77-03-45-5d-c4     dynamic
192.168.1.146         94-57-a5-0c-5b-02     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

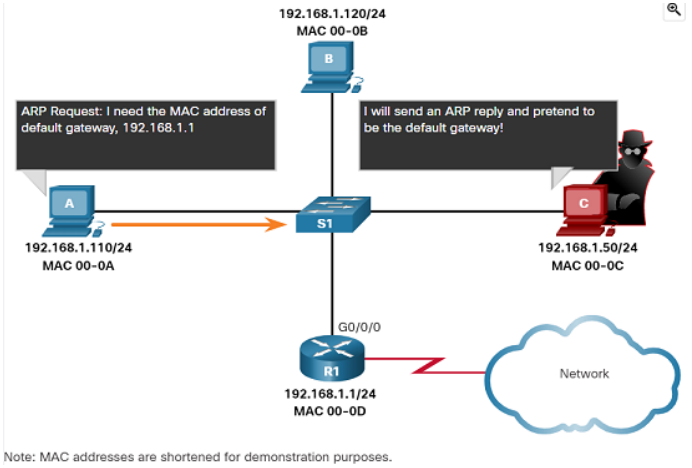
ARP Sorunları - ARP Yayınları ve ARP Sahteciliği

- Bir yayın çerçevesi olarak, yerel ağdaki her cihaz bir ARP isteği alır ve işler.
- Tipik bir iş ağında bu yayınların ağ performansı üzerinde çok az etkisi olacaktır.
- Birkaç cihazın çalıştırılıp hepsinin aynı anda ağ hizmetlerine erişmeye başladığını varsayalım. Bu durumda, şekilde gösterildiği gibi, kısa bir süre için performansta bir miktar düşüş olabilir.
- Cihazlar ilk ARP yayınlarını gönderdikten ve gerekli MAC adreslerini öğrendikten sonra, ağ üzerindeki herhangi bir etki en aza indirilecektir.



ARP Sorunları - ARP Yayınları ve ARP Sahteciliği (Devamı)

- Bazı durumlarda ARP kullanımı potansiyel bir güvenlik riskine yol açabilir.
- Bir tehdit aktörü, ARP zehirleme saldırısı gerçekleştirmek için ARP sahteciliğini kullanabilir.
- Şekilde gösterildiği gibi, bir tehdit aktörü tarafından varsayılan ağ geçidi gibi başka bir cihaza ait bir IPv4 adresine yönelik bir ARP isteğine yanıt vermek için kullanılan bir tekniktir.
- Tehdit aktörü kendi MAC adresiyle bir ARP yanıtı gönderir.
- ARP yanıtının alıcısı, ARP tablosuna yanlış MAC adresini ekleyecek ve bu paketleri tehdit aktörüne gönderecektir.
- Kurumsal düzeydeki anahtarlamalar, dinamik ARP denetimi (DAI) olarak bilinen azaltma tekniklerini içerir.



Note: MAC addresses are shortened for demonstration purposes.

Paket İzleyici - ARP Tablosunu İnceleyin

Bu Paket İzleyici etkinliğinde aşağıdaki hedefleri tamamlayacaksınız:

- Bir ARP Talebini İnceleyin
- Bir Anahtar MAC Adresi Tablosunu inceleyin
- Uzaktan İletişimlerde ARP Sürecini İnceleyin

Lab - Wireshark'ta ARP Trafiğini Görüntüle

Bu aktivitede aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Wireshark'ta ARP Verilerini Yakalayın ve Analiz Edin
- Bölüm 2: Bilgisayardaki ARP önbellek girişlerini görüntüleyin

7.2 Adres Çözümlemesi Özet

Bu Modülde Neler Öğrendim?

- Aynı yerel IPv4 ağındaki başka bir ana bilgisayara bir paket göndermek için, ana bilgisayarın hedef cihazın IPv4 adresini ve MAC adresini bilmesi gerekir.
- Bir cihaz, IPv4 adresini bildiğinde yerel bir cihazın hedef MAC adresini belirlemek için ARP'yi kullanır.

- ARP iki temel işlevi yerine getirir: IPv4 adreslerini MAC adreslerine çözümlemek ve IPv4 ile MAC adresi eşlemelerinin bir tablosunu tutmak.
- Gönderen cihaz, hedef IPv4 adresini ve karşılık gelen MAC adresini bulmak için ARP tablosunu arayacaktır.
- Paketin hedef IPv4 adresi, kaynak IPv4 adresiyle aynı ağda ise cihaz, ARP tablosunda hedef IPv4 adresini arar.
- Aksi takdirde cihaz varsayılan ağ geçidinin IPv4 adresini ARP tablosunda arayacaktır.
- ARP tablosunun her girişi veya satırı, bir IPv4 adresini bir MAC adresine bağlar.
- ARP isteği, aşağıdaki başlık bilgilerini kullanarak bir Ethernet çerçevesine kapsüllenir: hedef MAC adresi (yayın adresi FF-FF-FF-FF-FF-FF), kaynak MAC adresi (ARP isteğinin göndericisinin MAC adresi) ve tür (0x806).
- ARP istekleri, switch tarafından tüm portlardan (alıcı port hariç) gönderilen yayınlardır.
- Yalnızca ARP isteğiyle ilişkili hedef IPv4 adresine sahip cihaz bir ARP yanıtıyla yanıt verecektir.

Bu Modülde Neler Öğrendim? (Devamı)

- ARP cevabını aldıktan sonra cihaz, IPv4 adresini ve ilgili MAC adresini ARP tablosuna ekleyecektir.

- Hedef IPv4 adresi kaynak IPv4 adresiyle aynı ağda değilse, kaynak aygıtın çerçeveyi varsayılan ağ geçidine (yerel yönlendiricinin arayüzü) göndermesi gerekir.
- Bir kaynak aygıt başka bir ağda IPv4 adresli bir pakete sahip olduğunda, bu paketi yönlendiricinin hedef MAC adresini kullanarak bir çerçeveye kapsüller.
- Ana bilgisayarların IPv4 yapılandırması, varsayılan ağ geçidinin IPv4 adresini depolar.
- Hedef ana bilgisayar aynı ağda değilse, kaynak, varsayılan ağ geçidinin IPv4 adresine sahip bir giriş için ARP tablosunu kontrol eder.
- Giriş yoksa, varsayılan ağ geçidinin MAC adresini belirlemek için ARP sürecini kullanır.
- Her cihaz için bir ARP önbellek zamanlayıcısı, belirli bir süre boyunca cihazı kullanmayan ARP girişlerini kaldırır.
- show ip arp komutu bir Cisco yönlendiricisinde ARP tablosunu görüntülemek için kullanılır.
- Windows 10 PC'de ARP tablosunu görüntülemek için arp- komutu kullanılır.
- Bir yayın çerçevesi olarak, yerel ağdaki her cihaz bir ARP isteği alır ve işler.
- Bazı durumlarda ARP kullanımı potansiyel bir güvenlik riskine yol açabilir çünkü bir tehdit aktörü ARP zehirlenmesi saldırısı gerçekleştirmek için ARP sahteciliğini kullanabilir.