ARP PROTOKOLÜ

Bilindiği gibi bilgisayarlarımız yere alan ağında MAC adreslerini kullanarak haberleşiyorlar. Arp (Address Resulation Protocol) -Adres çözümleme protokolü, yerel alan ağımızda cihazlarımızın birbirleri ile haberleşebilmesi için cihazların IP adreslerine karşılık gelen MAC adreslerini öğrenmelerini sağlıyor. Burada IP adresi APIPA adresi de olabilir. Öğrenilen bu adresler ARP tablosunda belirli bir süre tutulur ve bekleme süresi boyunca kullanılmazsa tablodan silinir. Bu tablonun tutulmasının nedeni ise cihazlar arasında her veri alışverişi yapılacağında tekrar tekrar adres çözümlemesi yaparak ağda gereksiz trafik oluşumunun önüne geçmektir. Tablodaki adreslerin belirli bir süre kullanılmadığında silinmesi de ARP tablosunun sınırlı bir depolama alanına sahip olmasından kaynaklanmaktadır.

Her cihazın arp tablosu vardır. Bu adresleri görmek isterseniz bilgisayarınızın komut satırına “arp -a” komutunu yazmanız yeterli olacaktır. IP adreslerinin konu olduğu bir protokol olduğundan anlaşılacağı üzere üçüncü katman protokolüdür. Şimdi ise ARP protokolünün nasıl çalıştığını açıklamaya çalışacağım.

ARP PROTOKOLÜ NASIL ÇALIŞIR?

İlk durumda yerel alan ağındaki bir bilgisayara veri gönderebilmek için gerçekleştireceği olay adımlarını bir örnek ile açıklayalım. Örnekteki istek gönderecek cihazımıza PC1 , hedef cihazımıza ise PC2 olarak değerlendiriniz.

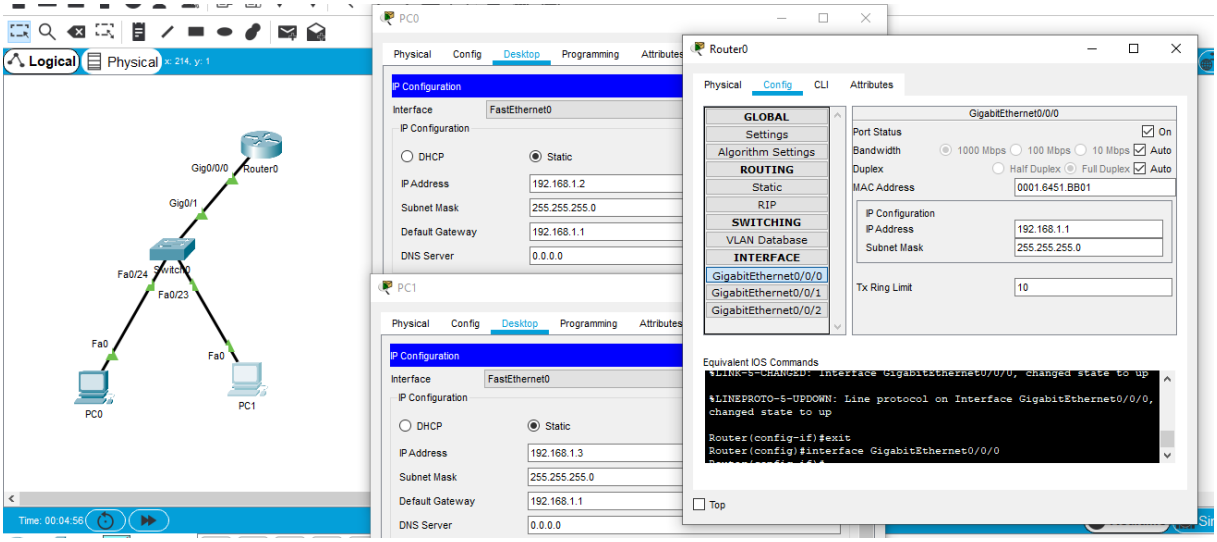
PC1 cihazımız kendi ağındaki bir cihaza bir PİNG atmak istediği zaman yapması gereken ilk adım göndereceği bilgisayarın IP adresine karşılık gelen MAC adresini kendi ARP tablosunda aratır. Hedef MAC adres kendi ARP tablosunda yoksa kaynak adresleri kendi MAC ve IP adreslerinin olduğu, hedef adres alanlarındaki ip adresi hedef cihazın IP adresi ve MAC adres alanını FF:FF:FF:FF:FF:FF olarak tanımladığı bir ARP istek paketini ağ içerisine BROADCAST yayın yapması için bırakır.

Yerel alan ağı içerisindeki bütün cihazlar bu ARP istek paketini alır ve kendi IP adresiyle karşılaştırarak paketin kendine gelip gelmediğini anlamaya çalışır. Eğer paket kendine gelmemişse (IP adresleri uyuşmuyorsa) paketi drop eder. Paket kendine gelmiş ise (PC2) paketi açarak içerisindeki kaynak adres alanındaki adresleri hedef adres alanına yazarak kaynak adres alanına da kendi IP ve MAC adresini yazan ARP cevap paketini ağa UNICAST olarak yayınlar. Burada ayrıca dikkat edilmesi gereken noktalardan biri de gelen paketin kaynağı doğrulanmadan cevap gönderilmesidir.

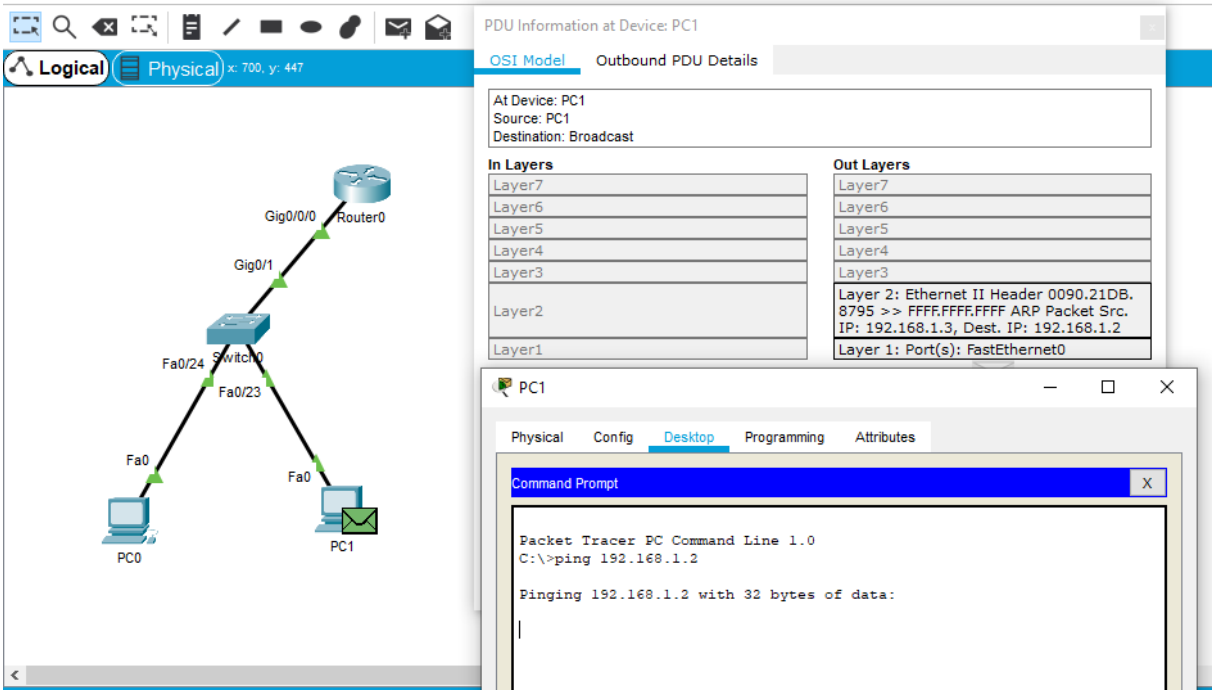
UNICAST olarak gönderilen ARP cevap paketini PC1 aldığında bu bilgileri kendi ARP tablosuna yazarak ping işlemini gerçekleştirmek için ICMP paketlerini göndermeye başlar.

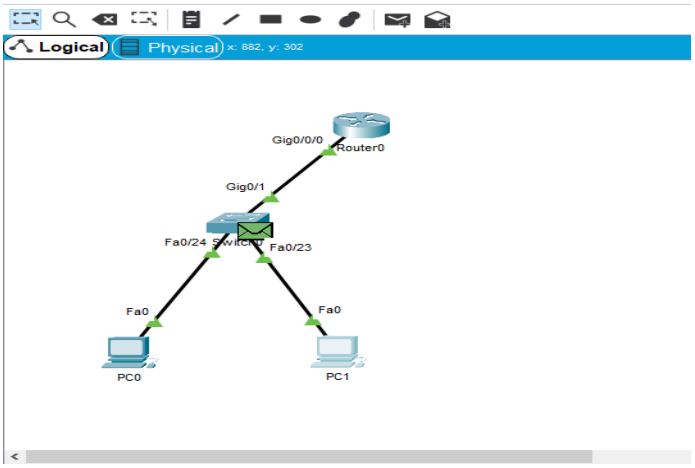
NOT : Eğer ki PC1 kendi ağı içerisinde değil de farklı bir ağdaki bilgisayara ping işlemi gerçekleştirecek olsaydı bu sefer BROADCAST olarak yayınlanan ARP istek paketindeki hedef IP adresi geçit yolunun IP adresi olacaktı. ARP sonrası ICMP paketini geçit yoluna gönderecekti. Sonrasındaki adımlar ise Bir Paketin Yolculuğu yazımda anlatılmaktadır. (BURADAN ULAŞABİLİRSİNİZ.)

Olay adımlarını Packet Tracer uygulamasında simüle edilmiş adımları aşağıda gösterilmiştir. Uygulama için yapılandırma aşağıdaki gibidir. (NOT sadece ARP çalışmasını gözlemlemek için sadece ARP paketlerini filtreledim.)

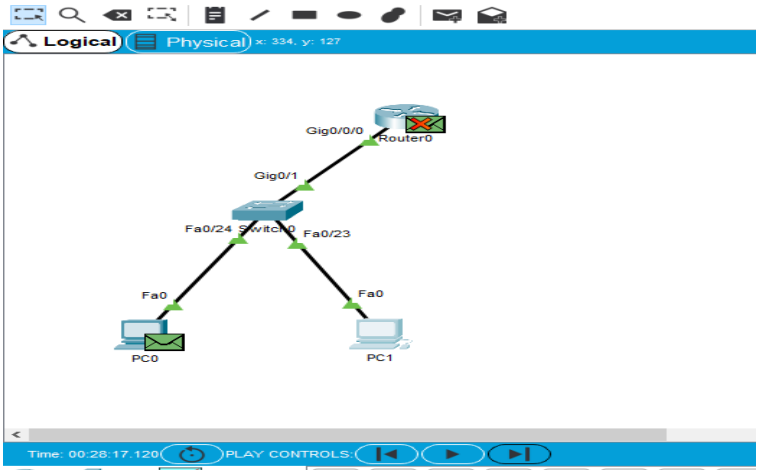


PC1 cihazından ping attığımızda öncelikle hedefin MAC adresini öğrenmek için ARP istek paketini içeriği yukarıda anlatıldığı gibi doldurularak ağa bırakılıyor.

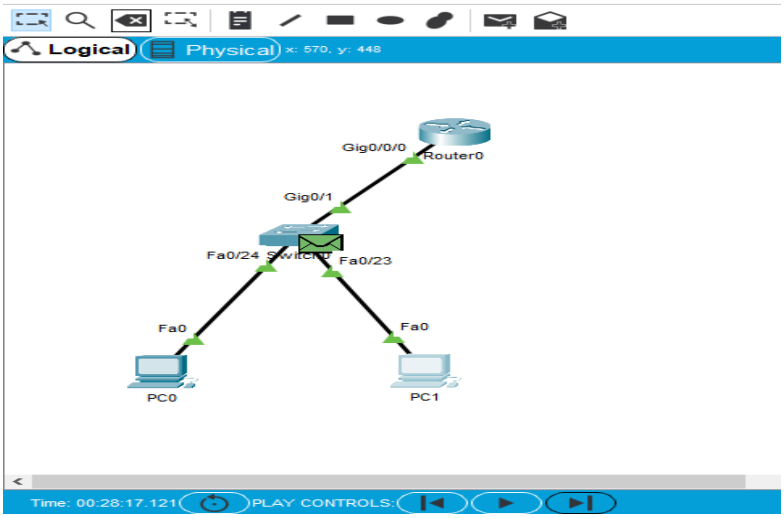




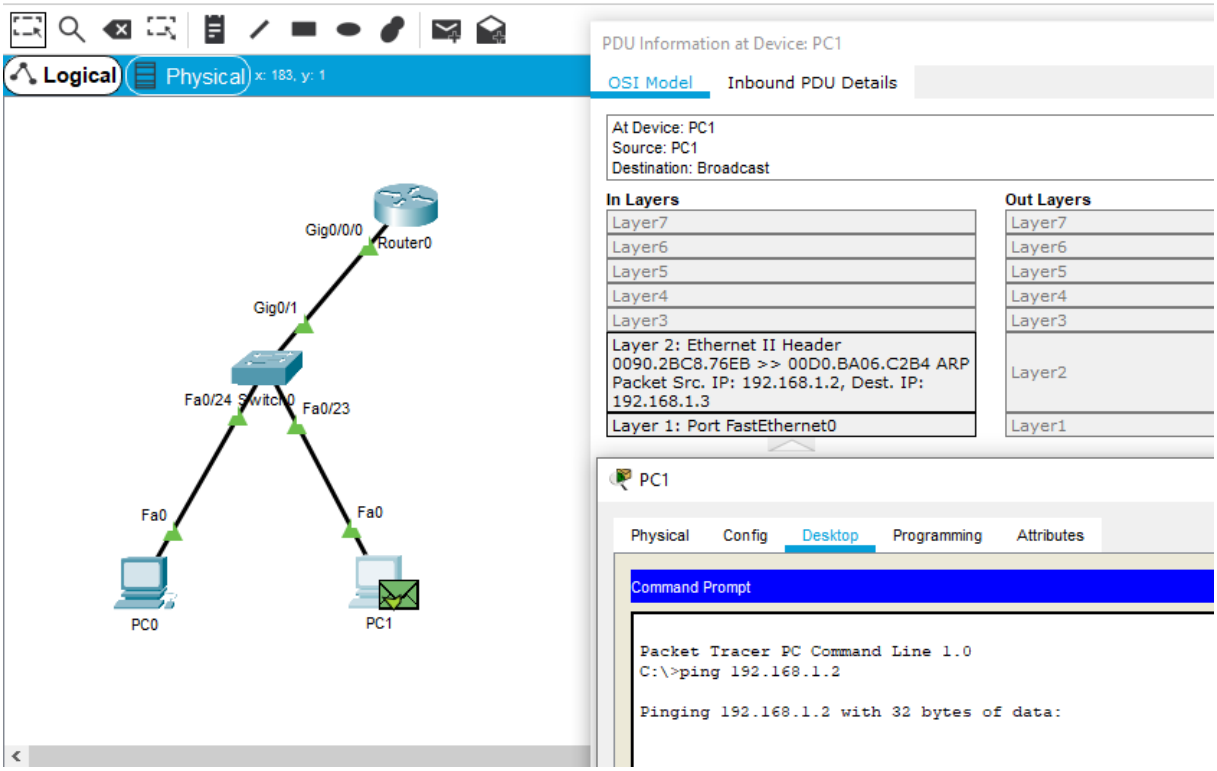
ARP istek paketlerini alan yerel alan ağındaki cihazlar ARP paketindeki adreslere bakarak kendine gelip gelmediğini anlıyor. Kendine gönderilmediğini anlayan cihazlar ARP istek paketini drop ediyorlar.



Kendine geldiğini anlayan PC0 bilgisayarı ise ARP cevap mesajını hazırlayıp ARP istek paketini gönderen bilgisayara gönderiyor.



Arp cevap paketinin içeriği aşağıdaki gibidir. Bu adımdan sonra PC0 bilgisayarıyla veri alışverişi yapabilir.



ARP PROTOKOLÜNE YÖNELİK SADIRILAR

1-ARP Spoofing (ARP Sahtekarlığı)

ARP sahtekarlığı (zehirlenmesi) saldırısı, IP-MAC adresi eşlemesinde hedef aldığı cihazın MAC adresi ile saldırgan bilgisayarın IP adresinin eşlemesini sağlayarak gerçekleştirilir. Bunun anlamı yerel alan ağı içerisinde (dış ağdan gelen paketler de yerel alan ağına girdiklerinde geçit yolu hedef MAC adresini saldırgan bilgisayarı olarak gördüğü için paketler yine saldırgan bilgisayarına yönlendirilecektir.) hedef alınan bilgisayara gönderilecek her paketin artık saldırgan bilgisayarına gönderilmesidir. Saldırgan bu durumu kullanarak hedef bilgisayara gönderilen her paketi kendi üzerine alarak hedef cihaza yönlendirmeden önce görebilmesi ve hatta manipüle edebilmesini sağlar. Bu yapı, ortadaki adam saldırısının (MİTM) yanı sıra hizmet reddi saldırısında da kullanılabilmektedir (gelen paketleri hedef bilgisayara yönlendirmediğimiz sürece bağlantı kuramayacaktır.).

Bu saldırının uygulaması ve analizine buradan ulaşabilirsin.

KAYNAKLAR

https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.49#:~:text=It%20is%20used%20to%20associate,access%20to%20one's%20sensitive%20data.

https://www.veracode.com/security/arp-spoofing#:~:text=ARP%20spoofing%20is%20a%20type,or%20server%20on%20the%20network.

https://www.imperva.com/learn/application-security/arp-spoofing/