BÖLÜM 3

AĞ YÖNETİMİNDE KULLANILAN PROTOKOLLER

ANAHTAR KAVRAMLAR

Temel Ağ Protokolleri, TCP/IP Protokol Kümesi, Ağ Yönetim Protokolleri, Http ve Https, DHCP, DNS, SNMP

ÖĞRENME HEDEFLERİ

1. Bilgisayar ağlarının çalışma prensibini bilir
2. OSI referans modeline göre ağın çalışmasını açıklar
3. TCP/IP referans modelini bilir
4. IP protokolünü açıklar
5. TCP ve UDP protokollerini açıklar
6. http ve https protokollerinin amacını bilir
7. Ağ yönetiminde kullanılan protokolleri açıklar

ÜÇÜNCÜ BÖLÜM

GİRİŞ

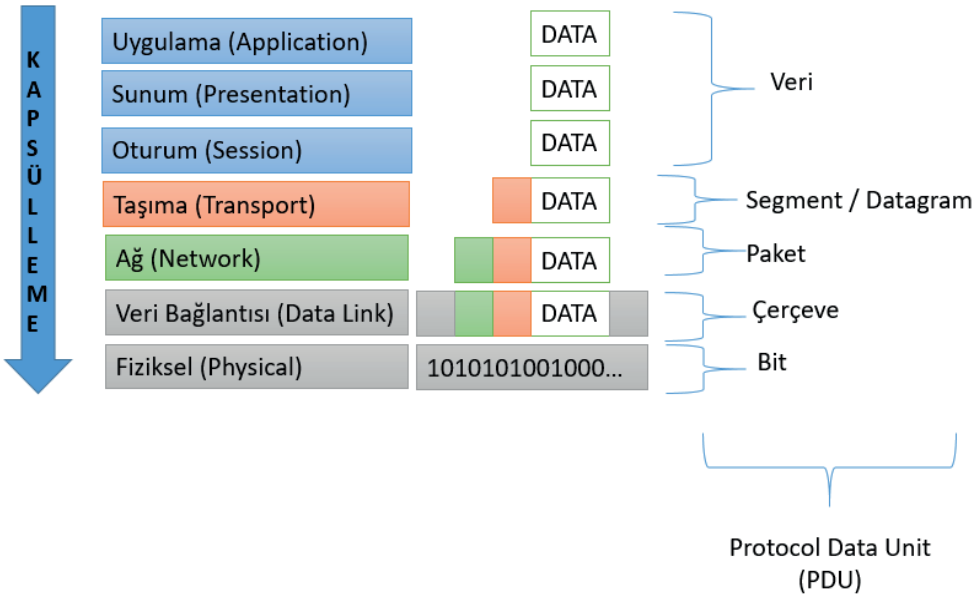
İnsanlar arasındaki iletişim esnasında geçerli olan dil, konuşma hızı, cümle yapısı, sıra beklemek, söz kesmemek, anlaşılamadığında tekrar etme ve anlaşıldığına dair onay almanın gibi kurallar, bilgisayar ağları dünyasında da önemli bir yer tutar. Bu kurallar bütünü, iletişimi hem gönderici hem de alıcı açısından anlaşılır kılmakla sorumlu olan protokoller olarak adlandırılır. Yani, protokoller, farklı üreticilerin çeşitli ürünlerinin aynı platformda uyumlu bir şekilde iletişim kurabilmesini sağlayan standartları belirler.

Bilgisayar ağları, dünyanın dört bir yanındaki bilgisayarları birbirine bağlayan ve veri iletişimini sağlayan temel altyapıları oluşturur. Bu ağlar, internetten şirket içi ağlara, kablosuz ağlardan devasa veri merkezlerine kadar çeşitli şekillerde karşımıza çıkar. Bu karmaşık ağlar, düzgün çalışmalarını sağlamak ve veri iletişimini yönetmek için belirli kurallara ve standartlara ihtiyaç duyar. Ağ protokolleri tam olarak bu noktada devreye girer.

Ağ protokolleri, bilgisayarlar arasında veri iletişimini sağlamak için kullanılan kurallar, standartlar ve işlemlerdir. Bu protokoller, veri paketlerinin nasıl yönlendirileceği, hedefe nasıl ulaştırılacağı, hataların nasıl düzeltileceği gibi detayları belirler. Ağ protokolleri, güvenli ve etkili veri iletişimini sağlamak için tasarlanmıştır.

1. REFERANS MODELLERİ

Bir ağın yönetimi ve güvenliğinin sağlanması, ağın nasıl çalıştığını, ağ protokollerinin ve iletişim standartların anlaşılmasına bağlıdır. Ağın çalışma prensibini açıklayan, ISO'nun geliştirdiği Open System Interconnection (OSI) ve Amerikan Savunma Bakanlığı'nın geliştirdiği TCP/IP adlı iki yaygın referans modeli bulunmaktadır. Her iki model de ağın çalışma sistemini adım adım açıklayan modellerdir.



Şekil 1. OSI referans modeli

OSI referans modeline göre, ağın çalışması yedi adımda incelenmektedir (Şekil 1). Her adımın işlevi ve o adımda yapılması gerekenler kesin olarak belirlenmiştir. Ağın çalışma prensiplerinin belirlendiği bu adımlara "Layer (Katman)" denir. OSI'nin bu mimarisindeki katmanlar birbirinden bağımsız olarak çalışır. Bu standardizasyon sayesinde farklı üreticilerin ürünleri OSI modeline göre tasarlandığı için birbirleri ile haberleşebilir.

Application Layer (Uygulama Katmanı), kullanıcı ile etkileşimin olduğu, uygulamaların bulunduğu katmandır. Örneğin bir web sayfasına bağlanmak için Internet Explorer, Firefox, Chrome gibi bir web tarayıcı uygulaması çalıştırmak gerekir.

Presentation Layer (Sunum Katmanı), uygulama katmanından gelen verilerin şekillendirildiği (sıkıştırma, şifreleme vb.), yani karşıdaki uygulamanın ya da hizmetin anlayabileceği bir biçimde sunulmasının gerçekleştiği katmandır.

Session Layer (Oturum Katmanı), cihazlar arasında sanal oturumların kurulduğu, yönetildiği ve sonlandırıldığı katmandır.

Transport Layer (Taşıma Katmanı), üst katmanlardan gelen verilerin alt katmanları ile iletişimini sağlayan katmandır. Diğer bakış açısıyla, alt katmanlardan gelen verinin, üst katmanlarda hangi uygulama ya da servis ile iletişime geçeceğinin belirlendiği katmandır. Bu belirleme temelde bir sayı olan port numaraları ile sağlanır.

Network Layer (Ağ Katmanı), mantıksal adreslemenin yapıldığı katmandır. Burada veriyi gönderen ve alacak olan cihazların mantıksal adresleri bulunur. Mantıksal adres olarak burada Internet Protocol (IP) adresleri eklenecektir. IP adresi dışında IPX, AppleTalk gibi mantıksal adresler bulunmakla beraber büyük bir çoğunlukla IP kullanıldığı için bu kitap boyunca IP adresleri örnek olarak gösterilecektir.

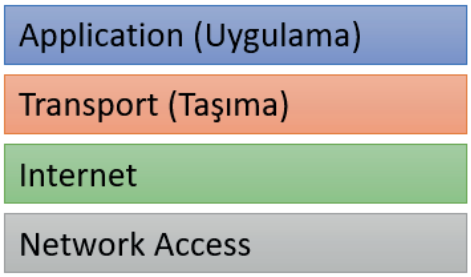
Data – Link Layer (Veri Bağı Katmanı), Veri bağlantısı olarak da adlandırılan bu katman fiziksel adreslemelerin yapıldığı yerdir. Yerel ağdaki, gönderici ve alıcı cihazların fiziksel adreslerinin belirlendiği aşamadır. Burada Fiziksel Adres olarak MAC adresleri kullanılır.

Physical Layer (Fiziksel Katman), verilerin taşınacak ortama (kablo, hava gibi) aktarılmak üzere fiziksel sinyallere dönüştürüldüğü katmandır.

OSI modeline göre çeşitli aşamalarda verilerin başına (header-başlık bilgisi) veya sonuna (trailer – art bilgi) eklenir ve bir alt katmana aktarılır. Bu sürece kapsülleme (encapsulation) denir. Her katmanda oluşan veri ve başlık/artbilgiden oluşan birime Protocol Data Unit (PDU) denir. Katmanların PDU isimleri Şekil 1'de gösterilmiştir.

Alıcı tarafta ise kapsülleme işlemin tersi gerçekleşir. Yani fiziksel ortamdan alınan sinyaller, başlık bilgileri her katmanda çıkarılıp bir üst katmana aktarılır.

TCP/IP (Transmission Control Protocol/Internet Protocol) modeli, bilgisayar ağlarındaki veri iletişimini düzenleyen ve temel protokollerin bir kombinasyonunu tanımlayan bir ağ iletişim modelidir. Bu model, veri iletişimi sürecini dört aşamada açıklar.



Şekil 2. TCP/IP modelinin dört aşaması

Uygulama (Application): Bu aşama, kullanıcı uygulamalarının ağ üzerinden iletişimini yönetir. HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) gibi uygulama protokolleri bu aşamada çalışır. OSI modelindeki 5-7 arasındaki üç katmana denk gelir.

Taşıma (Transport): Bu aşama, veri iletişiminin güvenilir ve doğru bir şekilde gerçekleşmesinden sorumludur. TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) bu aşamada çalışır.

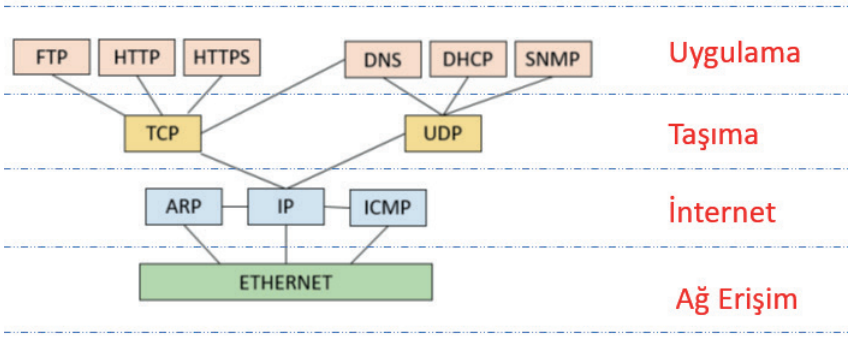
Internet (Internet): Bu aşama, veri paketlerinin kaynak adresinden hedef adresine yönlendirilmesini sağlar. IP (Internet Protocol) bu katmanda çalışır ve ağdaki farklı cihazlar arasındaki veri iletişimini yönlendirir.

Ağ Erişim (Network Access): Bu aşama, ağ donanımını ve fiziksel bağlantıyı yönetir. Ethernet veya Wi-Fi gibi teknolojileri içerir ve veri paketlerinin doğru cihazlara iletildiğinden emin olur.

TCP/IP modeli, internet üzerinde veri iletişimini standartlaştırmak ve farklı cihazların birbiriyle iletişim kurabilmesini sağlamak için kullanılır.

2. TEMEL AĞ PROTOKOLLERİ

Ağ ve internet ortamındaki cihazların sorunsuz çalışabilmesi standartlara ve dolayısıyla protokollere bağlıdır. Günümüzde internet ağlarında en yaygın kullanılan protokoller TCP/IP (Transmission Control Protocol/Internet Protocol) adı verilen bir protokol kümesinde toplanmıştır. Bu protokol kümesinde farklı işlevleri gören ve farklı amaçlara hizmet eden birçok protokol yer almaktadır (Şekil 3). TCP ve IP bu protokollerden en önemli sayılabilecek ikisidir. Bu nedenle protokol kümesinin adı TCP/IP olarak adlandırılır.



Şekil 3. TCP/IP modeline göre bazı protokoller ve Ethernet

TCP/IP protokol kümesi, bilgisayar ağlarında veri iletişimini sağlamak ve farklı cihazlar arasında güvenli ve doğru veri transferini kolaylaştırmak amacıyla tasarlanmıştır. Bu küme, veri paketlerini bölerek, ileterek ve yeniden birleştirerek verilerin güvenli ve hatasız bir şekilde iletilmesini sağlar. Ayrıca, TCP/IP kümesi, cihazlar arasındaki benzersiz kimlikleri yönetir, veri yollarını belirler ve internet üzerinden iletişimi standardize eder. Sonuç olarak, TCP/IP kümesi, dünya genelindeki bilgisayarlar arasındaki etkili ve güvenilir iletişimi mümkün kılan temel bir yapı sağlar. Aşağıda bu TCP/IP kümesinde yer alan temel protokollerden bazıları kısaca açıklanmıştır.

IP : "Internet Protocol" kısaltmasıyla bilinen bir iletişim protokolüdür ve bilgisayar ağlarında veri paketlerini yönlendirmek ve iletmek için kullanılır. IP, verilerin kaynak cihazdan hedef cihaza güvenli ve doğru bir şekilde iletilebilmesini sağlayan anahtar rolü oynar.

Bilgisayar ağlarındaki iletişimde IP'nin adresleme, yönlendirme, paketleme ve rotalama gibi birçok rolü bulunmaktadır. *Adresleme* rolünde, her cihaza benzersiz bir tanımlayıcı olan bir IP adresi atanır. IP adresleri, cihazların ağ içindeki konumlarını belirtir. Bu adresleme sayesinde, veri paketleri doğru hedefe yönlendirilebilir.

GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Bir arkadaşınıza bir paketi kargoladığınızı düşünün. Bu kargonun arkadaşınıza sorunsuz ulaşabilmesi için alıcı adresi yazan yere arkadaşınızın bulunduğu konumu yazmalısınız. Bu konum adresinin benzersiz olduğuna dikkat edin. Ayrıca paketi teslim ettiğiniz noktadan arkadaşınıza ulaşıncaya kadar çeşitli toplama noktalarından geçtiğine dikkat edin. Benzer işlemler IP iletişiminde de geçerlidir. Ağ ortamında gönderdiğiniz bir verinin doğru alıcıya gidebilmesi için benzersiz bir adrese ihtiyacı vardır. Bilgisayar ağlarındaki bu adrese IP adresi denir ve hedef cihazın konumunu belirler. Kargo örneğindeki gibi, IP paketlerinin içerisine gömülen veriler çeşitli toplama noktalarından geçer ve nihai olarak hedef cihaza ulaşır.

Cihazların konumu belirleyen IP adresleri 32-bitlik sayılardır. Ancak günlük hayatta adresleri bit olarak yazmak hataya neden olabileceğinden, bu 32-bitlik sayı bayt bayt ayrılır ve her bir bayt onluk sayı sistemine dönüştürülür. Ardından bu onluk gösterimler arasına "." konur. Örnek bir IP adresi aşağıdaki gibidir:

32-bitlik gösterim	11000000101010000000001100000111
Noktalı ondalık gösterim	192.168.3.7

IP'nin ağ iletişimindeki diğer bir fonksiyonu *paketlemedir*. Bilgisayar ağları üzerinden gönderilmek istenen veri, IP protokolü tarafından yönlendirilebilir paketlere bölünür. Her paket, hedefe ulaştırılması gereken verinin bir parçasını içerir. Bu paketler, ağ üzerinden ayrı ayrı iletilir ve ardından hedefte yeniden birleştirilir. IP'nin *yönlendirme* işlevinde, veri paketleri kaynaktan hedefe doğru yönlendirir. Verileri taşıyan bu IP paketlerinin ağdaki en iyi yolu izleyerek hedefe ulaştırılması sağlanır. En iyi yol seçimi, birçok etmene bağlı olabilir. Bu işlem ağdaki trafik yoğunluğu, maliyet ve diğer faktörleri değerlendirerek yönlendiricilerdeki yönlendirme tablosuna göre gerçekleştirilir.

IP, bilgisayarlar arasında güvenli, düzenli ve doğru veri iletişimini sağlayarak, modern internet ve bilgisayar ağlarının temelini oluşturur. Bu protokol, internetin ve küresel ağların çalışmasını mümkün kılar.

TCP : İnternet ve ağ iletişiminde verilerin uygulamalar arasında taşınmasından sorumlu olan güvenilir bir protokoldür. Yani verinin hangi uygulamadan çıkıp hedef cihazdaki hangi uygulamaya gideceğini belirler. Hedef ve kaynak uygulamalar port numaraları olarak adlandırılan sayılar aracılığıyla belirlenir. TCP'nin güvenilir olması veri paketlerinin sıralı, onaylı ve hatasız bir şekilde gönderilip alınmasını sağlayacak şekilde tasarlanmış olmasındandır. TCP protokolü, veri transferi sırasında bir dizi özel özelliği yönetir. Bu özellikler aşağıda maddeler halinde gösterilmiştir.

• Güvenilir Veri Transferi: TCP, veri paketlerinin güvenli bir şekilde kaynaktan hedefe ulaşmasını sağlamak için güvenilir veri iletimini yönetir. Veri paketleri, hedef cihaza ulaşmadan önce kaynak cihazda yeniden oluşturulur ve varsa hatalar düzeltilir.

• Sıralı Veri İletimi: TCP, veri paketlerinin hedefe gönderildikleri sırayla alınmasını sağlar. Bu, veri paketlerinin kaynaktan gönderildikleri sırayla hedefe ulaşmasını sağlayarak veri bütünlüğünü korur.

• Akış Kontrolü: TCP, veri transferi sırasında alıcı cihazın veri akışını kontrol etmesine olanak tanır. Bu özellik, alıcı cihazın kendi hızında veri almasını ve aşırı yüklenme durumlarının önlemesini sağlar.

• Bağlantı Yönetimi: TCP, veri transferi başlamadan önce ve iletim esnasında bağlantıyı yönetir. İletişim kurma, veri transferi ve bağlantıyı sonlandırma gibi aşamaları düzenler.

• Hata Tespiti ve Düzeltme: TCP, veri paketlerinin iletim sırasında kaybolduğunu veya bozulduğunu tespit eder. Bu hataları düzeltmek veya kaybolan paketleri yeniden göndermek için gerekli mekanizmaları içerir.

• Akış Denetimi: TCP, ağdaki trafiği dengelemek için akış kontrolü yapabilir. Bu, ağ üzerindeki yoğunluğu düzenler, böylece ağdaki cihazlar arasındaki veri transferi dengelenir.

TCP, internet üzerindeki veri iletişiminin temelini oluşturan protokollerden biridir. Web sayfalarının, dosyaların, e-postaların ve diğer verilerin güvenli bir şekilde transfer edilmesini sağlamak için yaygın olarak kullanılır.

UDP (User Datagram Protocol): Verilerin uygulamalar arasında taşınmasını sağlayan diğer bir

protokol de UDP protokolüdür. TCP ile benzer şekilde port numaralarını kullanarak kaynak ve hedef uygulamaları tanımlar. Ancak UDP oldukça basit bir yapıdadır ve TCP kadar yetenekli bir protokol değildir. Bu nedenle genelde TCP ile karşılaştırılarak yapamadıkları ile açıklanır. Örneğin TCP kullanan uygulamalarda paket kayıpları TCP tarafından yeninden gönderim ile telafi edilebilir, ancak UDP için bu özellik söz konusu değildir. TCP ile kıyaslandığında en önemli avantajı, ek özellikleri olmadığından hızlı olmasıdır. Bu nedenle paket kayıplarının önemsenmediği durumlarda UDP kullanılabilir. Ağ yönetiminde UDP kullanan birçok protokol ve uygulama yer almaktadır. DNS, SNMP gibi protokollerin yanı sıra, genelde ses ve video trafikleri UDP protokolünü kullanır.

DİKKAT EDELİM

UDP paket kayıplarını telafi etmek için bir mekanizma içermez ancak UDP kullanan diğer protokoller bu telafiyi yapabilirler.

HTTP/HTTPS (Hypertext Transfer Protocol/Secure Hypertext Transfer Protocol): Son kullanıcıların en çok yaptığı işlemlerden biri web sayfalarında gezinmektir. Bu durumda http protokolü çalışır ve web tarayıcı kullanarak iletişimi başlatan (istemci) ile web hizmetini veren (sunucu) arasında istemci-sunucu mimarisinde birtakım kurallar çerçevesinde iletişim gerçekleşir.

HTTP, web tarayıcıları ve sunucular arasında metin, grafik, ses, video gibi içeriklerin iletilmesini sağlayan protokoldür. HTTPS ise bu iletişimi şifreleyerek güvenli hale getirir.

Şekil 4. http isteği ve cevabı

İstemci tarafından gönderilen http isteğine (*http request*) sunucu tarafından yanıtlar (*http response*) verilir ve veri takası gerçekleşir. Böylece istenilen sunucudan web sayfası talep edilmiş olur. Şekil 4'te yer alan örnekte, google.com adresine http isteği gönderilmesi gösterilmiştir.

ARAŞTIRALIM

http ile https arasındaki fark nedir? Güvenlik ve yönetim açısından araştırınız.

DNS (Domain Name System): DNS, insanların anlayabileceği domain isimlerini (örneğin, www.ankara.edu.tr) IP adreslerine çeviren bir protokoldür. Bu sistem, internet üzerindeki adreslerin daha kolay hatırlanabilmesini sağlar.

SMTP/POP3/IMAP (Simple Mail Transfer Protocol/Post Office Protocol/Internet Message Access Protocol): Bu protokoller, e-posta iletişimini yönetmek için kullanılır. SMTP, e-postaları göndermek için, POP3 ve IMAP ise e-postaları almak için kullanılır.

FTP (File Transfer Protocol): FTP, dosyaların bir bilgisayardan diğerine transfer edilmesini sağlayan bir protokoldür. Büyük dosyaların paylaşımı ve güncellenmesi için kullanılır.

Ağ protokollerinin etkili yönetimi, ağın güvenliği, performansı ve verimliliği açısından kritiktir. Ağ yöneticileri, ağ trafiğini izler, güvenlik önlemlerini uygular, hataları giderir ve ağ performansını optimize eder. Ağ protokollerinin doğru bir şekilde yapılandırılması ve yönetilmesi, bilgisayar ağlarının sağlıklı ve güvenli bir şekilde çalışmasını sağlar.

Bilgisayar ağlarının yönetimi için kullanılan ağ protokolleri ve bu protokollerin etkili bir şekilde yönetilmesi, modern dünyada bilgi paylaşımı ve iletişimin temelini oluşturur. Bu protokoller, internet, iş ağları, veri merkezleri ve diğer birçok alandaki iletişimi mümkün kılar, böylece dünya genelindeki bilgisayar sistemleri birbiriyle etkileşimde bulunabilir ve bilgi paylaşabilir.

3. AĞ YÖNETİMİ PROTOKOLLERİ

Ağ yönetimi için tasarlanmış protokoller, ağ trafiğini izleme, hataları teşhis etme, performansı optimize etme, güvenlik önlemlerini uygulama ve diğer ağ yönetim görevlerini gerçekleştirmek için kullanılan özel protokollerdir. Ağ yönetimi için tasarlanmış bazı önemli protokoller aşağıda verilmiştir.

*SNMP (Simple Network Management Protocol):*SNMP, ağ cihazlarının durumunu izlemek, hataları teşhis etmek ve yönetmek için kullanılan bir protokoldür. SNMP uyumlu cihazlar, ağ yöneticilerinin bu cihazlarla iletişim kurarak performans verilerini toplamasını sağlar.

NetFlow: Cisco tarafından geliştirilmiş bir ağ trafiği analizi protokolüdür. Ağ trafiğini izlemek, analiz etmek ve kapasite planlaması yapmak için kullanılır. NetFlow, ağdaki trafiği detaylı bir şekilde inceleyerek performans problemlerini tespit etmeye yardımcı olur.

ICMP (Internet Control Message Protocol): Bir ağ ortamında gerek sorun giderme için gerek iletişimin varlığının doğrulanması için kontrol edilmesi ihtiyacı vardır. ICMP, bu amaç doğrultusunda geliştirilmiş, belirli bir IP'nin erişilebilir olup olmadığını doğrulamak için kullanılan bir protokoldür. Erişimin olup olmadığının yanı sıra, erişim ile ilgili, erişiminin olmamasının olası nedeni, erişilen cihaza ve uzaklığına dair çeşitli bilgiler de sunan yararlı bir protokoldür. Ağ yöneticileri, ICMP mesajlarını kullanarak ağdaki bazı problemleri teşhis edebilirler. Örneğin belirli bir IP'nin veya alan adının erişilebilir olup olmadığını doğrulamak için kullanılan ping komutu, ICMP protokolünü kullanır.

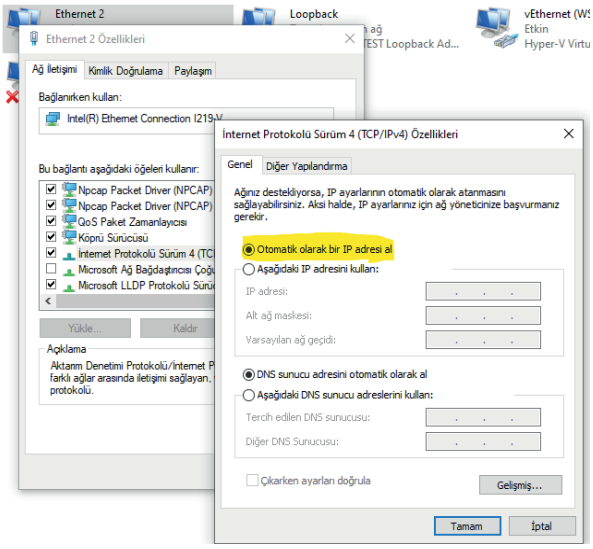
```
C:\>ping www.google.com

Pinging www.google.com [142.250.184.132] with 32 bytes of data:
Reply from 142.250.184.132: bytes=32 time=21ms TTL=53
Reply from 142.250.184.132: bytes=32 time=21ms TTL=53
Reply from 142.250.184.132: bytes=32 time=22ms TTL=53
Reply from 142.250.184.132: bytes=32 time=22ms TTL=53

Ping statistics for 142.250.184.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 22ms, Average = 21ms
```

Şekil 5. ping komutu ile erişilebilirlik kontrolü

Şekil 5'te yer alan örnekte www.google.com adresinin erişilebilir olup olmadığı sorgulanmış (ping www.google.com) ve gelen cevaptan uzaktaki sunucunun erişilir olduğu görülmüştür. Şekilde kontrol için 4 ICMP paketi gönderilmiş ve hepsinden kayıpsız (%0 loss) cevap alınmıştır.

DHCP (Dynamic Host Configuration Protocol): Bilgisayar ağlarında cihazların benzersiz IP adreslerinin olması gerektiğini hatırlayın. Ayrıca sağlıklı bir iletişim cihazların ağının sınırlarını belirlemesini sağlayan *maske*, ağdan çıkış noktasını (ağ geçidi - gateway) ve DNS sunucusunun adresinin de tanımlı olması gerekir. Bu parametreler cihazlara elle verilebilir. Ancak özellikle çok sayıda cihazın bulunduğu ağlarda bu bilgilerin elle verilmesi zaman alıcı ve hataya neden olabilir. Bu nedenle cihazların bu parametreleri dinamik olarak almasını sağlayan DHCP isimli bir protokol geliştirilmiştir.

DHCP, ağdaki cihazlara otomatik olarak IP adresi ve diğer ağ konfigürasyon bilgilerini atayan bir protokoldür. Bu, ağ yöneticilerinin IP adresi tahsisini otomatikleştirmelerine ve merkezi olarak yönetmelerine olanak tanır.



Şekil 6. DHCP kullanarak otomatik IP alma

Şekil 6'daki görüntüde gösterildiği gibi "Otomatik olarak bir IP adresi al" seçeneği seçildiğinde cihazlar DHCP protokolünü kullanarak gerekli bilgileri bir sunucudan alır. Örneğin ev ortamında sıklıkla kullanılan ADSL modem-yönlendiriciler, varsayılan olarak DHCP hizmeti verecek şekilde tasarlanmıştır. Yani bir ev ağı için ADSL modem aynı zamanda bir DHCP sunucusudur. Kurumsal büyük ağlarda ise genelde bu işlem için bağımsız sunucular kullanılır.

RADIUS (Remote Authentication Dial-In User Service): RADIUS, ağ kaynaklarına erişim yetkisini doğrulamak için kullanılan bir protokoldür. Özellikle büyük ölçekli ağlarda, merkezi bir sunucu üzerinden kimlik doğrulama ve yetkilendirme işlemlerini sağlar.

SSH (Secure Shell) : SSH, uzaktaki bilgisayarlara güvenli bir şekilde erişim sağlamak için kullanılan bir ağ protokolüdür. SSH, verilerin şifrelenmesini ve güvenli bir şekilde iletilmesini sağlayarak, kullanıcıların uzak sunuculara güvenli bir şekilde bağlanmasına ve komutlarını uzaktaki sunucularda çalıştırmasına olanak tanır.

Bu protokoller, ağ yöneticilerinin ağlarını izlemek, güvenliği sağlamak, hataları teşhis etmek ve ağ performansını optimize etmek için kullandığı önemli araçlardır. Bu protokoller, modern ağ yönetimi için temel taşlar olarak kabul edilir.

BÖLÜM ÖZETİ

İnternet ağlarındaki cihazların sorunsuz çalışabilmesi için protokoller ve standartlar yer alır. TCP/IP protokolü, veri iletişimini sağlamak, güvenli ve doğru veri transferini kolaylaştırmak amacıyla tasarlanmıştır. IP, veri paketlerini yönlendirme ve iletim için kullanılırken, TCP verilerin güvenli taşınmasından sorumludur. UDP ise veri iletimi için kullanılan basit bir protokoldür, ancak paket kayıplarını telafi etme özelliği yoktur ve hızlı iletim sağlar. Bu protokoller, internet ve ağ iletişiminin temelini oluşturur. Open System Interconnection (OSI) ve TCP/IP olmak üzere iki yaygın referans modeli yer almaktadır. OSI modeli, ağın çalışmasını yedi adımda inceler: Uygulama Katmanı, Sunum Katmanı, Oturum Katmanı, Taşıma Katmanı, Ağ Katmanı, Veri Bağı Katmanı ve Fiziksel Katman. Her katman belirli bir işlevi yerine getirir ve verilerin iletimini sağlar. Bu katmanlar, farklı cihazlar arasında iletişimi standardize eder ve veri iletimi sürecini açıklar. Kapsülleme (encapsulation) adı verilen bir süreçle veriler, her katmanda başlık bilgileriyle birlikte taşınır ve Protocol Data Unit (PDU) adını alan birime dönüşür. Alıcı tarafta ise kapsülleme işlemi tersine çevrilir ve veriler bir üst katmana aktarılır. Bu model, ağ iletişiminin temel prensiplerini açıklar. Diğer bir referans modeli de Uygulama, Taşıma, İnternet ve Ağ Erişimi isimli 4 aşamadan oluşan TCP/IP modelidir. Bilgisayar ağlarındaki iletişimi sağlayan temel protokollerden olan IP (Internet Protocol) adresleme, yönlendirme, paketleme ve rotalama gibi önemli rolleri üstlenir ve bilgilerin güvenli ve doğru bir şekilde iletilmesini sağlar. TCP (Transmission Control Protocol) ise verilerin güvenilir bir şekilde taşınmasından sorumludur ve güvenilir veri transferi, sıralı veri iletimi, akış kontrolü, bağlantı yönetimi, hata tespiti ve düzeltme, akış denetimi gibi özellikleri yönetir. UDP (User Datagram Protocol) ise daha basit bir yapıda olup hızlı veri transferine olanak tanır. Diğer önemli protokoller arasında HTTP/ HTTPS (web sayfalarının iletişimi), DNS (domain isimlerinin IP adreslerine çevrilmesi), SMTP/POP3/ IMAP (e-posta iletişimi) ve FTP (dosya transferi) yer alır. Bu protokoller, bilgisayar ağlarının sağlıklı ve güvenli bir şekilde çalışmasını sağlamak için kullanılır ve ağ yöneticileri tarafından dikkatlice yönetilir. Ağ yönetimi için çeşitli protokoller kullanılır. SNMP, ağ cihazlarının durumunu izlemek ve yönetmek için kullanılırken, NetFlow ağ trafiğini analiz etmek ve kapasite planlaması yapmak için kullanılır. ICMP, ağlardaki erişim sorunlarını teşhis etmek için kullanılır, örneğin, “ping” komutu ICMP protokolünü kullanarak belirli bir IP adresine erişilebilirlik kontrolü yapar. DHCP, ağdaki cihazlara otomatik olarak IP adresleri ve diğer ağ konfigürasyon bilgilerini atayan bir protokoldür. RADIUS, ağ kaynaklarına erişim yetkisini doğrulamak için kullanılırken, SSH güvenli bir şekilde uzaktaki bilgisayarlara erişim sağlamak için kullanılır. Bu protokoller, ağ yöneticilerinin ağlarını izlemek, güvenlik sağlamak, hataları teşhis etmek ve ağ performansını optimize etmek için kullandığı araçlardır.

GÖZDEN GEÇİRELİM

1. **TCP/IP protokol kümesi ne amaçla tasarlanmıştır?**
   a) Video oyunlarını desteklemek için
   b) Veri iletişimini sağlamak ve güvenli veri transferini kolaylaştırmak için
   c) Müzik indirmek için
   d) Sadece e-posta gönderimi için

2. **IP adresi nedir ve ne amaçla kullanılır?**
   a) Bilgisayarların renk kodu
   b) Cihazlara benzersiz bir tanımlayıcı atanması için
   c) Yemek tarifleri saklamak için
   d) İnternet tarayıcılarını güncellemek için

3. **UDP protokolünün en büyük avantajı nedir?**
   a) Hızlı iletim sağlamak
   b) Paket kayıplarını telafi etme yeteneği
   c) Verileri şifreleme yeteneği
   d) Bağlantıyı sürdürme süresi

4. **OSI modeline göre, aşağıdaki katmanlardan hangisi kullanıcı ile etkileşimin olduğu uygulamaların bulunduğu katmandır?**
   a) Transport Layer (Taşıma Katmanı)
   b) Network Layer (Ağ Katmanı)
   c) Application Layer (Uygulama Katmanı)
   d) Data – Link Layer (Veri Bağı Katmanı)

5. **Ağ iletişiminde verilerin başlık bilgileriyle birlikte taşınması sürecine ne ad verilir?**
   a) Kriptografi
   b) Kapsülleme (Encapsulation)
   c) Modülasyon
   d) Kod çözme

6. **TCP/IP modelinde verilerin sinyallere dönüştürülmesi hangi aşamada gerçekleşir?**
   a) Uygulama
   b) Taşıma
   c) İnternet
   d) Ağ Erişim

7. **IP (Internet Protocol) protokolü hangi aşamada kullanıcılara benzersiz tanımlayıcı olan IP adresi atar ve veri paketlerini doğru hedefe yönlendirilmesini sağlar?**
   a) Adresleme rolünde
   b) Paketleme işlevinde
   c) Rotalama aşamasında
   d) Yönlendirme işlevinde

8. **TCP (Transmission Control Protocol) protokolü hangi özelliğiyle veri paketlerinin sıralı, onaylı ve hatasız bir şekilde gönderilip alınmasını sağlar?**
   a) Hata Tespiti ve Düzeltme
   b) Akış Denetimi
   c) Güvenilir Veri Transferi
   d) Bağlantı Yönetimi

9. **DHCP protokolü aşağıdakilerden hangisini gerçekleştirir?**
   a) Ağ trafiğini izleme
   b) Ağdaki cihazların benzersiz IP adreslerini otomatik olarak atama
   c) Ağ kaynaklarına erişim yetkisini doğrulama
   d) Uzaktaki bilgisayarlara güvenli bir şekilde erişim sağlama

10. **RADIUS protokolü hangi amaçla kullanılır?**
   a) Uzaktaki bilgisayarlara güvenli bir şekilde erişim sağlama
   b) Ağ kaynaklarına erişim yetkisini doğrulama
   c) Ağdaki cihazların benzersiz IP adreslerini otomatik olarak atama
   d) Ağ trafiğini izleme

Yanıt Anahtarı: 1-B, 2-B, 3-A, 4-C, 5-B, 6- D, 7-A, 8-C, 9-B, 10-B

Kaynakça

Comer, D. E. (2018). The Internet book: everything you need to know about computer networking and how the Internet works. CRC Press.

Edelman, J., Lowe, S. S., & Oswalt, M. (2018). Network Programmability and Automation: Skills for the Next-Generation Network Engineer. O'Reilly Media. https://books.google.com.tr/books?id=PjJKDwAAQBAJ

GUPTA, P. C. (2006). Data Communication and Computer Networks. PHI Learning. https://books.google.com.tr/books?id=-kNn_p6WA38C

Halsall, F. (1995). Data communications, computer networks and open systems. Addison Wesley Longman Publishing Co., Inc.

Kurose, J., & Ross, K. (2018). Computer Networking: A Top-Down Approach, Global Edition. Pearson Education. https://books.google.com.tr/books?id=IUh1DQAAQBAJ

Mitrou, N. (2004). Networking 2004: Networking Technologies, Services, and Protocols ; Performance of Computer and Communications Networks ; Mobile and Wireless Communications ; Third International IFIP-TC6 Networking Conference, Athens, Greece, May 9 - 14, 2004 ; Proceedings. Kluwer Academic Publishers.

Newman, M. (2018). Networks. Oxford university press.

Robertazzi, T. G. (2000). Computer networks and systems: queueing theory and performance evaluation. Springer Science \& Business Media.

Bergel C. Bilgisayar Ağları Ve Güvenlik. Sakarya University Journal of Science. 2004; 8(1): 5-8.

Sütçü, C. "Bilgisayar ve Bilgisayar Ağları". Marmara İletişim Dergisi 5 (1994): 145-152

Okuma Listesi

https://www.sbb.gov.tr/wp-content/uploads/2022/08/Bilgisayar-Aglari-ile-Ilgili-Suclar-Siber-Suclar-Oguz-Turhan.pdf

https://acikders.ankara.edu.tr/pluginfile.php/155273/mod_resource/content/0/1.1.%20A%C4%9F%20T%C3%BCrleri.pdf

https://www.kaspersky.com.tr/resource-center/threats/trojans

https://www.trendmicro.com/tr_tr/what-is/ransomware.html