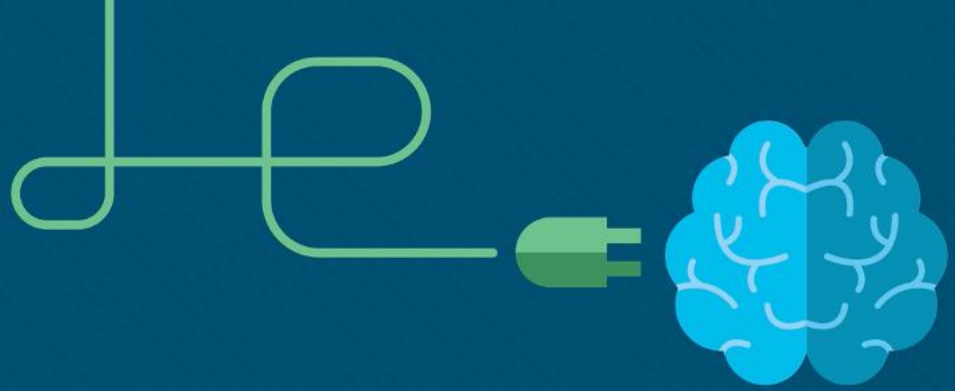


Modül 15: Taşımacılık

Katman

Ağ Temelleri (BNET)

Modül Hedefleri

Modül Başlığı: Taşıma Katmanı

Modül Amacı:Müşterilerin internet hizmetlerine nasıl eriştiğini açıklayın.

Konu Başlığı	Konu Amaç
TCP ve UDP	TCP ve UDP taşıma katmanı fonksiyonlarını karşılaştırın.
Liman Numaraları	TCP ve UDP'nin port numaralarını nasıl kullandığını açıklayın.

15.1 TCP ve UDP

Video - TCP ve UDP İşlemi

Bu videoda iki taşıma katmanı protokolü olan TCP ve UDP incelenmektedir.

15.2 Port Numaraları

Video - Taşıma Katmanı Port Numaraları

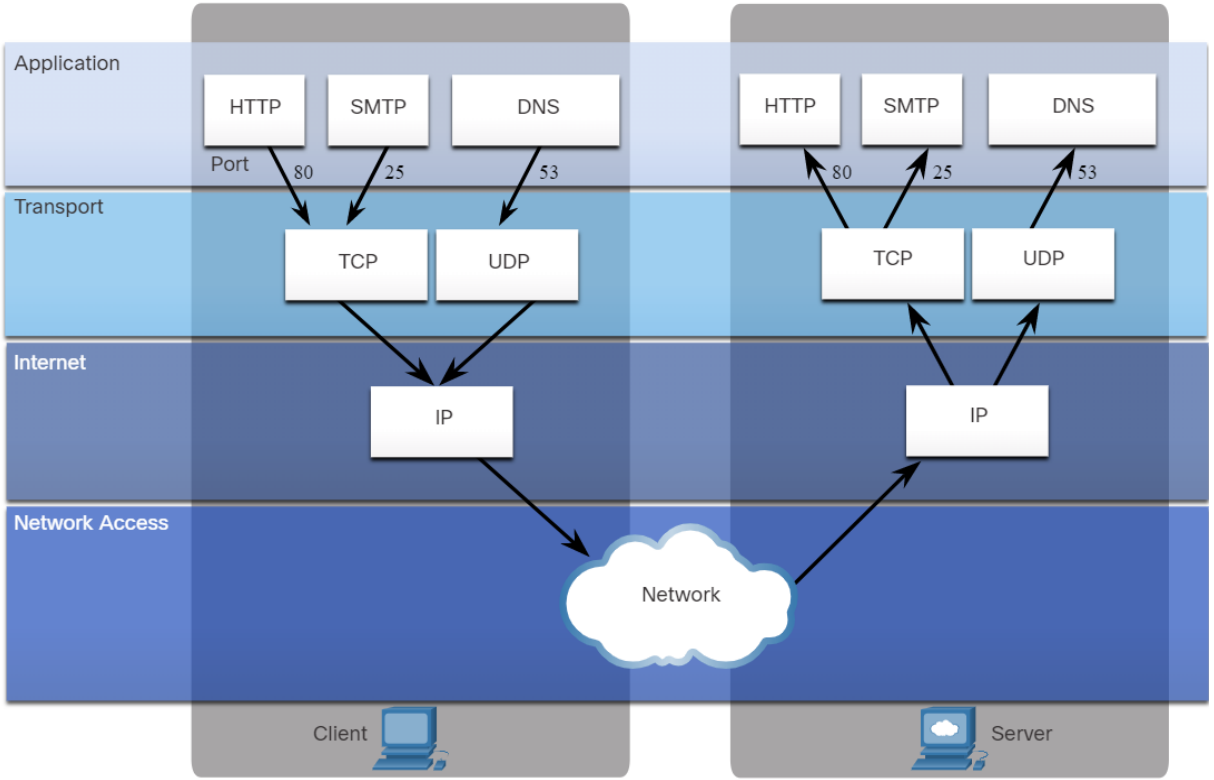
Bu videoda, taşıma katmanı bağlantı noktası numaralarının, iletim hedefi ve kaynağı olan konuşmaları ve uygulamaları tanımlamak için nasıl kullanıldığı incelenmektedir.

TCP ve UDP Port Numaraları

- İnternet üzerinden bir günde eriştiğimiz birçok hizmet vardır. DNS, web, e-posta, FTP, IM ve VoIP, istemci/sunucu sistemlerinin dünya çapında sağladığı hizmetlerdir. Büyük veri merkezlerinde tek bir sunucu veya birkaç sunucu bu hizmetleri sağlayabilir.

- Bir mesaj TCP veya UDP kullanılarak iletildiğinde, talep edilen protokoller ve hizmetler şekilde gösterildiği gibi bir port numarasıyla tanımlanır. Bir port, bir istemci ve sunucu arasındaki belirli konuşmaları takip etmek için her segmentteki sayısal bir tanımlayıcıdır. Bir ana bilgisayarın gönderdiği her mesaj hem bir kaynak hem de bir hedef portu içerir.

TCP ve UDP Port Numaraları (Devamı)



TCP ve UDP Port Numaraları (Devamı)

- Bir sunucu bir ileti aldığında, sunucu istemci tarafından hangi hizmetin talep edildiğini belirlemelidir. Bir hedef bağlantı noktası, her hizmet için internette kayıt yaptıran bir istemciyi onu kullanacak şekilde önceden yapılandırır. Bir örnek, HTTP web hizmetleri için iyi bilinen bağlantı noktası olan 80 numaralı bağlantı noktasını kullanarak web sunucularına istekler göndermek üzere önceden yapılandırılmış web tarayıcısı istemcileridir.

- Bağlantı noktaları, İnternet Atanmış İsimler ve Sayılar Şirketi (ICANN) olarak bilinen bir kuruluş tarafından atanır ve yönetilir. Bağlantı noktaları üç kategoriye ayrılır ve sayıları 1 ile 65.535 arasında değişir:
  - **Tanınmış Limanlar**-Tipik ağ uygulamalarıyla ilişkili hedef portlar iyi bilinen portlar olarak tanımlanır. Bu portlar 1 ila 1023 aralığındadır.
  - **Kayıtlı Limanlar**-Kaynak veya hedef portları 1024 ile 49151 arasındaki portlardır. Kuruluşlar bunları IM uygulamaları gibi belirli uygulamaları kaydetmek için kullanabilirler.
  - **Özel Limanlar**-Kaynak portları genellikle 49152 ile 65535 arasındaki portları kullanır. Herhangi bir uygulama bu portları kullanabilir.

TCP ve UDP Port Numaraları (Devamı)

- Bazı uygulamalar hem TCP hem de UDP kullanabilir. Örneğin, istemciler bir DNS sunucusuna istek gönderdiğinde DNS UDP kullanır. Ancak, iki DNS sunucusu arasındaki iletişim her zaman TÇP.

- Tam port numaralarını ve ilişkili uygulama listesini görüntülemek için IANA web sitesinde port kayıt defterini arayın.

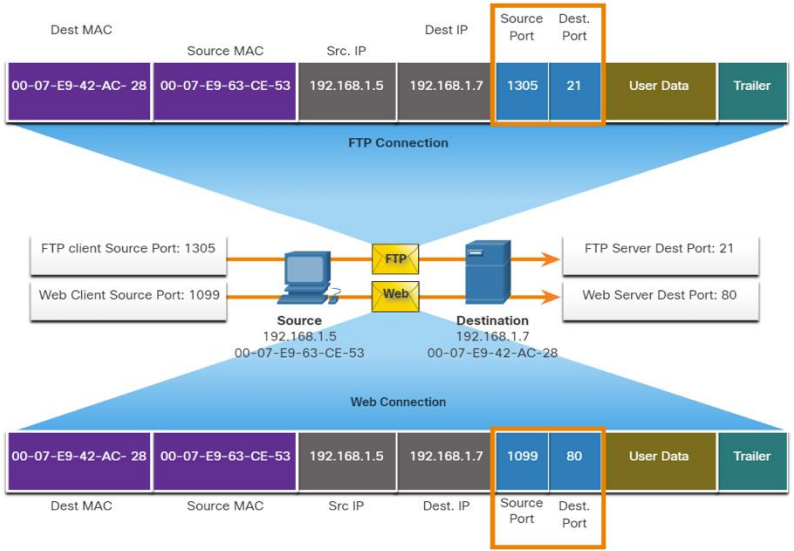
TCP ve UDP Port Numaraları (Devamı)

Liman Numarası	Taşımacılık	Uygulama Protokolü
20	TKP	Dosya Aktarım Protokolü (FTP) - Veri
21	TKP	FTP - Kontrol
22	TKP	Güvenli Kabuk (SSH)
23	TKP	Telnet
25	TKP	Basit Posta Aktarım Protokolü (SMTP)
53	UDP, TCP	Alan Adı Sistemi (DNS)
67	UDP	Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) - Sunucu
68	UDP	DHCP - İstemci
69	UDP	Basit Dosya Aktarım Protokolü (TFTP)
80	TKP	Hipermetin Aktarım Protokolü (HTTP)
110	TKP	Posta Ofisi Protokolü sürüm 3 (POP3)
143	TKP	İnternet İleti Erişim Protokolü (IMAP)
161	UDP	Basit Ağ Yönetim Protokolü (SNMP)
443	TKP	Hipermetin Aktarım Protokolü Güvenli (HTT)

Soket Çiftleri

- Kaynak ve hedef portlar segmentin içine yerleştirilir. Segmentler bir IP paketi içinde kapsüllenir. IP paketi, kaynağın ve hedefin IP adresini içerir. Kaynak IP adresi ve kaynak port numarası veya hedef IP adresi ve hedef port numarasının birleşimi soket olarak bilinir.

- Şekildeki örnekte PC'nin hedef sunucudan aynı anda FTP ve web servisleri talep ettiği görülmektedir.



Soket Çiftleri (Devamı)

- Örnekte, PC tarafından oluşturulan FTP isteği, Katman 2 MAC adreslerini ve Katman 3 IP adreslerini içerir. İstek ayrıca kaynak bağlantı noktası numarası 1305'i (ana bilgisayar tarafından dinamik olarak oluşturulur) ve hedef bağlantı noktasını tanımlar ve bağlantı noktası 21'deki FTP hizmetlerini tanımlar.

- Ana bilgisayar aynı Katman 2 ve Katman 3 adreslerini kullanarak sunucudan bir web sayfası da talep etti. Ancak, ana bilgisayar tarafından dinamik olarak oluşturulan 1099 kaynak bağlantı noktası numarasını ve 80 numaralı bağlantı noktasındaki web hizmetini tanımlayan hedef bağlantı noktasını kullanır.

- İstemcinin talep ettiği sunucu ve hizmet, soketi tanımlamak için kullanır. Bir istemci soketi, 1099'un kaynak bağlantı noktası numarasını temsil ettiği şekilde şöyle görünebilir: 192.168.1.5:1099

- Bir web sunucusundaki soket 192.168.1.7:80 olabilir

Soket Çiftleri (Devamı)

- Bu iki soket birlikte bir soket çifti oluşturmak üzere birleşir: 192.168.1.5:1099, 192.168.1.7:80

- Soketler, bir istemcide çalışan birden fazla işlemin birbirinden ayırt edilmesini ve sunucu işlemine yapılan çeşitli bağlantıların birbirinden ayırt edilmesini sağlar.

- Kaynak bağlantı noktası numarası, istekte bulunan uygulama için bir dönüş adresi görevi görür. Taşıma katmanı, bu bağlantı noktasını ve isteği başlatan uygulamayı takip eder, böylece yanıt döndüğünde doğru uygulamaya iletilebilir.

netstat Komutu

- Açıklanamayan TCP bağlantıları önemli bir güvenlik tehdidi oluşturabilir. Bir şeyin veya birinin yerel ana bilgisayara bağlandığını gösterir. Bazen, hangi etkin TCP bağlantılarının açık olduğunu ve bir ağ ana bilgisayarında çalıştığını bilmek gerekir. Netstat, bu bağlantıları doğrulamak için kullanılabilen önemli bir ağ yardımcı programıdır. Aşağıda gösterildiği gibi, kullanımda olan protokolleri, yerel adresi ve bağlantı noktası numaralarını, yabancı adresi ve bağlantı noktası numaralarını ve bağlantı durumunu listelemek için netstat komutunu girin.

```
C:\> netstat

Active Connections

  Proto Local Address          Foreign Address            State
  TCP   192.168.1.124:3126     192.168.0.2:netbios-ssn    ESTABLISHED
  TCP   192.168.1.124:3158     207.138.126.152:http       ESTABLISHED
  TCP   192.168.1.124:3159     207.138.126.169:http       ESTABLISHED
  TCP   192.168.1.124:3161     sc.msn.com:http            ESTABLISHED
  TCP   192.168.1.124:3166     www.cisco.com:http         ESTABLISHED
(output omitted)
C:\> netstat
```

netstat Komutu (Devamı)

- Varsayılan olarak,**netstat**komut, IP adreslerini etki alanı adlarına ve port numaralarını iyi bilinen uygulamalara çözümlemeye çalışacaktır.**-N**seçeneği IP adreslerini ve port numaralarını sayısal biçimde görüntüleyebilir.

15.3 Taşıma Katmanı Özet

Bu Modülde Neler Öğrendim?

- UDP, alındı onayı gerektirmeyen bir 'en iyi çaba' teslimat sistemidir. UDP, akışlı ses ve VoIP gibi uygulamalarda tercih edilir. Onaylar teslimatı yavaşlatır ve yeniden iletimler istenmez. Paketler kaynaktan hedefe giden bir yol izler. Birkaç paket kaybolabilir, ancak genellikle fark edilmez.

- TCP paketleri kaynaktan hedefe giden bir yol izler. Ancak, paketlerin her birinin bir sıra numarası vardır. TCP, bir mesajı segment olarak bilinen küçük parçalara ayırır. Segmentler sırayla numaralandırılır ve paketler halinde birleştirilmek üzere IP sürecine geçirilir.

- TCP, belirli bir uygulamadan belirli bir ana bilgisayara gönderilen segment sayısını takip eder. Gönderici belirli bir süre içinde bir onay almazsa, segmentlerin kaybolduğunu varsayar ve bunları yeniden iletir. Yalnızca kaybolan mesaj kısmı yeniden gönderilir, tüm mesaj değil.

Bu Modülde Neler Öğrendim? (Devamı)

- Bir port numarası, bir mesaj TCP veya UDP kullanılarak iletildiğinde talep edilen protokolleri ve hizmetleri tanımlar. Bir port, bir istemci ve sunucu arasındaki konuşmaları takip eden her segmentteki sayısal bir tanımlayıcıdır. Bir ana bilgisayarın gönderdiği her mesaj hem bir kaynak hem de bir hedef portu içerir.

- Bir sunucu bir mesaj aldığında, sunucu istemci tarafından hangi hizmetin talep edildiğini belirlemelidir. Her hizmet için internette kayıtlı bir hedef bağlantı noktası, istemcilerin kullanması için önceden yapılandırılır.

Bu Modülde Neler Öğrendim? (Devamı)

- Bağlantı noktaları, ICANN olarak bilinen bir kuruluş tarafından atanır ve yönetilir. Bağlantı noktaları üç kategoriye ayrılır ve sayıları 1 ile 65.535 arasında değişir:

  - **Tanınmış Limanlar**-Ortak ağ uygulamalarıyla ilişkili hedef bağlantı noktaları iyi bilinen bağlantı noktaları olarak tanımlanır. Bu bağlantı noktaları 1 ila 1023 aralığındadır.
  - **Kayıtlı Limanlar**-Kaynak veya hedef portları 1024 ile 49151 arasındaki portları kullanabilir. Kuruluşlar bunları IM uygulamaları gibi belirli uygulamaları kaydetmek için kullanabilir.
  - **Özel Limanlar**-Kaynak portları 49152'den 65535'e kadar olan portları kullanabilir. Herhangi bir uygulama bu portları kullanabilir.

- Gönderen cihaz, iki cihaz arasındaki bir konuşmayı tanımlamak için kaynak bağlantı noktası numarasını dinamik olarak üretir. Bu işlem, birden fazla konuşmanın aynı anda gerçekleşmesine olanak tanır. Bir cihazın bir web sunucusuna aynı anda birden fazla HTTP hizmet isteği göndermesi yaygındır. Her ayrı HTTP konuşması, kaynak bağlantı noktalarına göre izlenir.

Bu Modülde Neler Öğrendim? (Devamı)

- İstemci, hedef sunucuya bir servis isteği bildirmek için segmente bir hedef port numarası yerleştirir. Bir sunucu, 80 numaralı portta web servisleri gibi aynı anda birden fazla servis sunabilirken, 21 numaralı portta FTP bağlantısı kurulumu sağlayabilir.

- Açıklanamayan TCP bağlantıları önemli bir güvenlik tehdidi oluşturabilir. Bir şeyin veya birisinin yerel ana bilgisayara bağlandığını gösterebilir. Bazen, ağ tabanlı bir ana bilgisayarda hangi etkin TCP bağlantılarının açık ve çalışır durumda olduğunu bilmek gerekir.

- Netstat, bu bağlantıları doğrulamak için kullanılabilen hayati bir ağ yardımcı programıdır. netstat komutu, kullanımda olan protokolleri, yerel adresi ve bağlantı noktası numaralarını, yabancı adresi ve bağlantı noktası numaralarını ve bağlantı durumunu listeler.