T.C.
MİLLÎ EĞİTİM BAKANLIĞI

ENDÜSTRİYEL OTOMASYON TEKNOLOJİLERİ

TEMEL BİLGİSAYAR AĞLARI - 3

481BB0079

Ankara, 2012

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

İÇİNDEKİLER

AÇIKLAMALAR....ii
GİRİŞ....1
ÖĞRENME FAALİYETİ–1....3
1. IP PAKET....3
1.1 IP Paket....3
UYGULAMA FAALİYETİ....6
ÖLÇME VE DEĞERLENDİRME....8
ÖĞRENME FAALİYETİ–2....9
2. ICMP PAKET....9
UYGULAMA FAALİYETİ....12
ÖLÇME VE DEĞERLENDİRME....13
ÖĞRENME FAALİYETİ–3....14
3. İLETİM KATMANI....14
3.1. Port Numaraları....15
3.2. "netstat" komutu....16
3.3. UDP....19
3.4. TCP....19
3.5. Soket Kavramı....22
UYGULAMA FAALİYETİ....24
ÖLÇME VE DEĞERLENDİRME....25
ÖĞRENME FAALİYETİ–4....26
4. NETBIOS VE TCP/IP....26
UYGULAMA FAALİYETİ....30
ÖLÇME ve DEĞERLENDİRME....31
MODÜL DEĞERLENDİRME....32
CEVAP ANAHTARLARI....33
KAYNAKÇA....34

AÇIKLAMALAR

KOD	**481BB0079**
ALAN	**Endüstriyel Otomasyon Teknolojileri**
DAL/MESLEK	**Endüstriyel Kontrol Teknisyenliği**
MODÜLÜN ADI	**Temel Bilgisayar Ağları - 3**
MODÜLÜN TANIMI	Bu modül öğrencinin IP, TCP protokollerini kavramasını sağlayan öğrenme materyalidir.
SÜRE	40/32
ÖN KOŞUL	"Temel Bilgisayar Ağları – 2" modülünü almış olmak
YETERLİK	Temel seviye eş düzeyli bilgisayar ağı kurmak
MODÜLÜN AMACI	**Genel Amaç** Veri iletişimini hatasız olarak yapan temel eş düzeyli bilgisayar ağları kurabileceksiniz. **Amaçlar** 1. IP paketlerini inceleme işlemini ağ analiz programında hatasız olarak yapabileceksiniz. 2. TCP paketlerini inceleme işlemini ağ analiz programında hatasız olarak yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Bilgisayar laboratuvarı **Donanım:** Bilgisayar ve çevre birimleri
ÖLÇME VE DEĞERLENDİRME	Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz. Öğretmen modül sonunda ölçme aracı (çoktan seçmeli test, doğru-yanlış testi, boşluk doldurma, eşleştirme vb.) kullanarak modül uygulamaları ile kazandığınız bilgi ve becerileri ölçerek sizi değerlendirecektir.

GİRİŞ

Sevgili Öğrenci,

Bu modül ile endüstriyel otomasyon teknolojileri alanında gerekli olan network altyapısını oluşturan konulara yönelik bilgi ve teknolojiye ait temel yeterlikleri kazanacaksınız.

Günlük hayatta sıkça kullandığımız IP adresleri ve bunu oluşturan IP paketlerin yapısını öğrenecek, network trafiğinde bu paketlerin bilgisayardan bilgisayara nasıl transfer edildiğini network analiz programları kullanarak inceleyebileceksiniz.

Bu modülü başarılı bir şekilde tamamladığınızda network uzmanı olarak bir ağdaki paket trafiğini analiz edebilecek, bu sayede TCP/IP protokolünün altyapısını yeterince kavrayabileceksiniz.

ÖĞRENME FAALİYETİ–1

AMAÇ

IP paketlerini inceleme işlemini ağ analiz programında hatasız olarak yapabileceksiniz.

ARAŞTIRMA

- IP paket ile ilgili araştırma yapınız.

1. IP PAKET

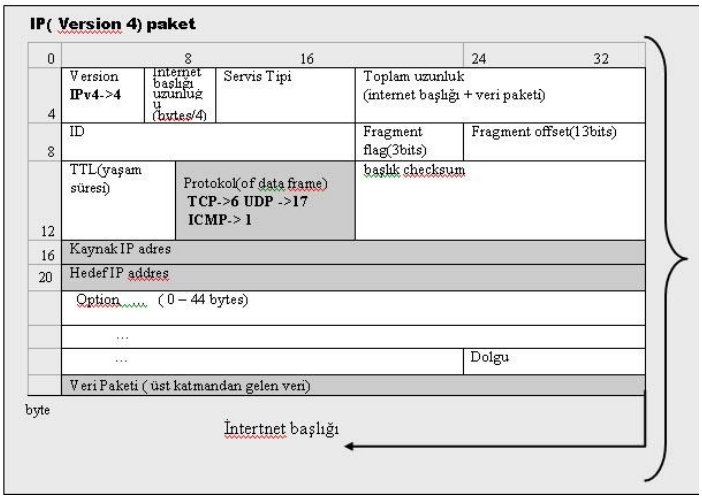
Bu bölümde içinde hedef bilgisayarın IP adresini de bulunduran IP paketini (internet protokol) ayrıntılı olarak inceleyeceğiz.

1.1 IP Paket

IP paket başlık ve IP bilgisi bölümlerinden oluşur ve paket internet katmanında yorumlanır, IPv4 32 bittir. IP paketin detaylı yapısı aşağıda belirtilmiştir.

IP paketinin genel formatı aşağıdaki gibidir.

IP Paket	
IP Başlığı	IP Verisi



Şekil 1.1: IP paket yapısı

Şimdi IP paketi oluşturan bölümleri tanıyalım.

- **Version (versiyon)**

4 bitten oluşur ve IP paketin versiyonunu gösterir.

- **Internet header length (internet başlığı uzunluğu)**

4 byte'dir. 4 bölümden oluşur (32 bit).

- **Type of service (servis tipi)**

8 bitten oluşur. Uzun süredir kullanılmamaktadır.

- **Total length (toplam uzunluk)**

16 bitten oluşur ve toplam IP datagram büyüklüğünü gösterir.

- **ID, fragment flag, fragment offset**

Üst katmanlardan gelen veri 1500 byte'den büyükse internet katmanında küçük paketlere bölünür. Bu paketlerin boyutu **MTU** (maksimum transfer unit) olarak ifade edilir. MTU içinde 1500 byte'lik "internet header" vardır.

Bölünen tüm IP paketler aynı **ID**'ye atanır ve aynı **fragment offset** değerine sahiptir.

Paket içinde fragment offset için maksimum 13 bit yer vardır. Bu nedenle maksimum veri büyüklüğü aşağıdaki şekilde hesaplanabilir.

Maksimum veri uzunluğu= 2^{13} x 8 =65536 bytes

Veri bundan daha büyük ise transport katmanı daha önceden veriyi parçalara ayırmalıdır. Bazen transport katmanı veri büyüklüğü belirtilen değerden daha küçük olduğunda bile veriyi daha küçük parçalara bölebilir.

Fragment bayrağı (fragment flag) (3 bit) değeri aşağıdaki tabloda açıklanmıştır.

bit 0	bit 1	bit 2
Kullanılmaz.	**0**: Router tarafından bölünebilir. **1**: Bölünemez.	**0**: Son paket **1**: Son değil

- **TTL (time to live, yaşam süresi)**

Hazırlanan IP paket, her bir router içinden geçtiğinde TTL değerinden bir çıkartılır. TTL değeri sıfır olduğunda IP paketi sonraki "router"de dikkate alınmaz. Bu nedenle TTL değeri IP paketin kaç tane router içinden geçebileceğini belirtir. Bu sayede paketin aynı yol üzerinde sonsuza kadar dolaşması engellenmiş olunur. Bazen aynı network içinde ikiden fazla router olması, hatalı dolaşımlara sebep olabilmektedir.

Normalde TTL değeri 128'dir. Bu değer işletim sistemine göre farklılık gösterebilir.

- **Protokol (protocol)**

8 bitten oluşur ve daha üst katmanların protokollerine kimlik için protokol numarası tanımlar.

Protokol numaraları için örnekler:

1 >>> ICMP
6 >>> TCP
17 >>> UDP
41 >>> IPv6

- **Header checksum**

16 bitten oluşur ve IP başlığını kontrol eder.

- **Kaynak adres (source address)**

32 bitten oluşur ve kaynak IP adreslerini tanımlar.

- **Hedef adres (destination address)**

32 bitten oluşur ve hedef IP adreslerini tanımlar.

- **Ekler ve dolgu (option and padding)**

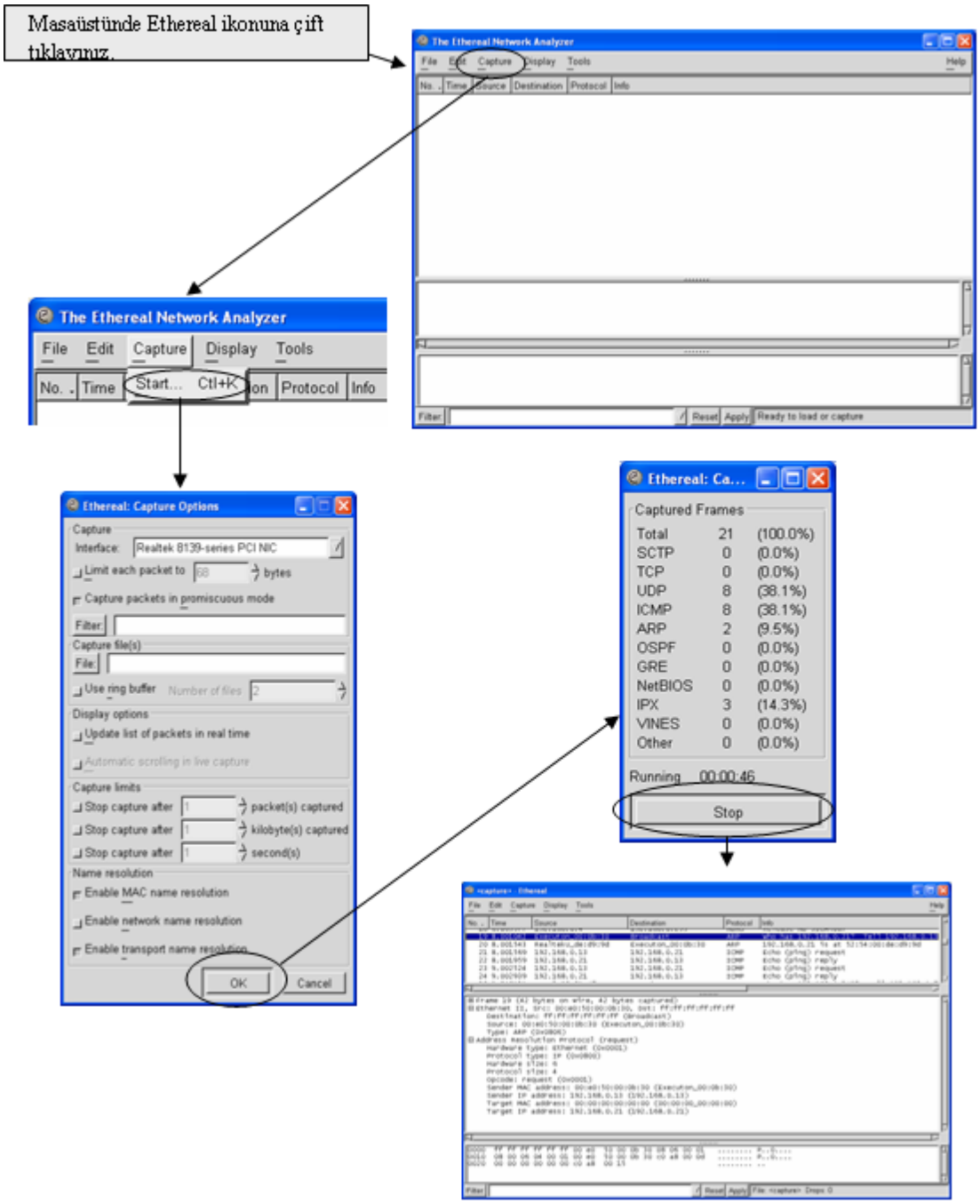
Bu bölümler genelde kullanılmaz.

UYGULAMA FAALİYETİ

Network analiz programının kurulumunu yapınız.

İşlem Basamakları	Öneriler
➢ Ethereal programını kurunuz.	➢ "**Ethereal**" ya da **"wirehark"** ücretsiz network analiz programıdır. Windows ve UNIX için kullanma imkânı vardır.
	➢ Ethereal'i kullanmak için WinPcap'i install (kurmak) etmek gerekir. ➢ Belirtilen iki dosyayı bilgisayarınıza kopyalayınız. ➢ **Ethereal-setup-0.9.9.exe** ➢ Double click **ethereal-setup-0.9.9.exe** ➢ Kurulum otomatik olarak sonlanacaktır. ➢ **WinPcap_3_0.exe** ➢ Double click **WinPcap_3_0.exe** ➢ Kurulum tamamlandıktan sonra masa üstünde "Ethereal" program ikonu görünecektir.
➢ Paket yakalama işlemini gerçekleştiriniz.	➢ Aşağıdaki paket yakalama örneğine göre paket yakalama yapabilirsiniz.

Paket yakalama:



ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin sonunda boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) IP paket 62 bitten oluşur.

2. ( ) IP'nin açılımı internet protokolüdür.

3. ( ) Paket büyüklüğü 1500 byte'den büyük ise küçük paketlere bölünür.

4. ( ) TTL değeri, paketlerin internette sonsuza kadar dolaşmasını sağlar.

5. ( ) Kaynak adres 32 bitten oluşur ve hedef IP adreslerini tanımlar.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

IP paketlerini inceleme işlemini ağ analiz programında hatasız olarak yapmak

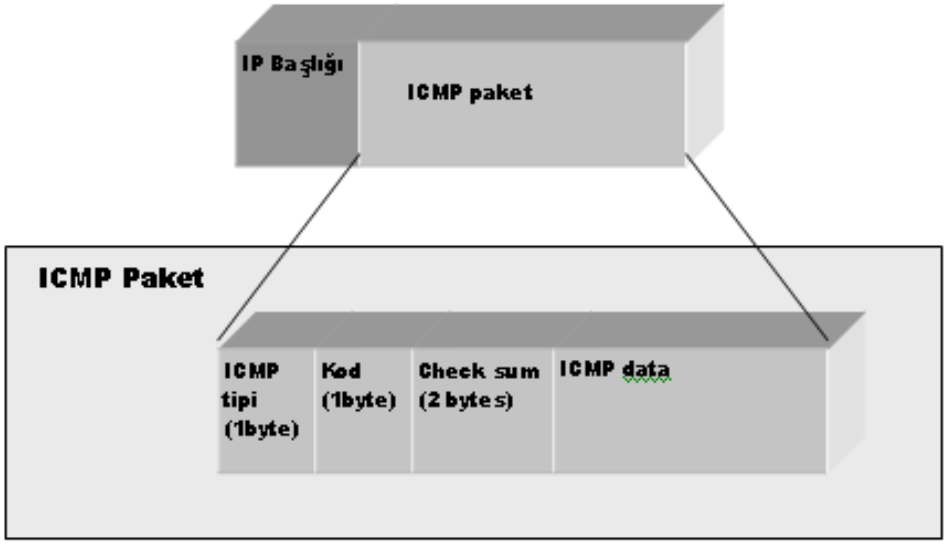
ARAŞTIRMA

- ICMP paket ile ilgili araştırma yapınız.

2. ICMP PAKET

ICMP (Internet Control Message Protocol) paketinin kullanım amacı aşağıda belirtilmiştir.

- TTL (yaşam) süresi dolduğu zaman paketin sahibine bildirim yapılması
- Herhangi bir durumda yok edilen paket hakkında bildirim sağlanması
- Parçalanmasın komutu verilmiş paket parçalandığında geri bildirim sağlanması
- Hata oluşumlarında geri bildirim sağlanması
- Paket başka bir yoldan gideceği zaman geri bildirim sağlanması



Şekil 2.1: ICMP paket

Mesaj Tipi	Açıklama
0	Echo Reply (yanıt)
3	Destination Unreachable (Hedef erişilemez.)
4	Source Quench (kaynak)
5	Redirect (yönlendirme)
8	Echo Request (istek)
11	Time Exceeded (zaman aşımı)
12	Parameter (problem)
13	Timestamp Request (istek)
14	Timestamp Reply (yanıt)
15	Information Request (istek)
16	Information Reply (yanıt)
17	Address Mask Request (istek)
18	Address Mask Reply (yanıt)

Tablo 2.1: ICMP mesajının tipi

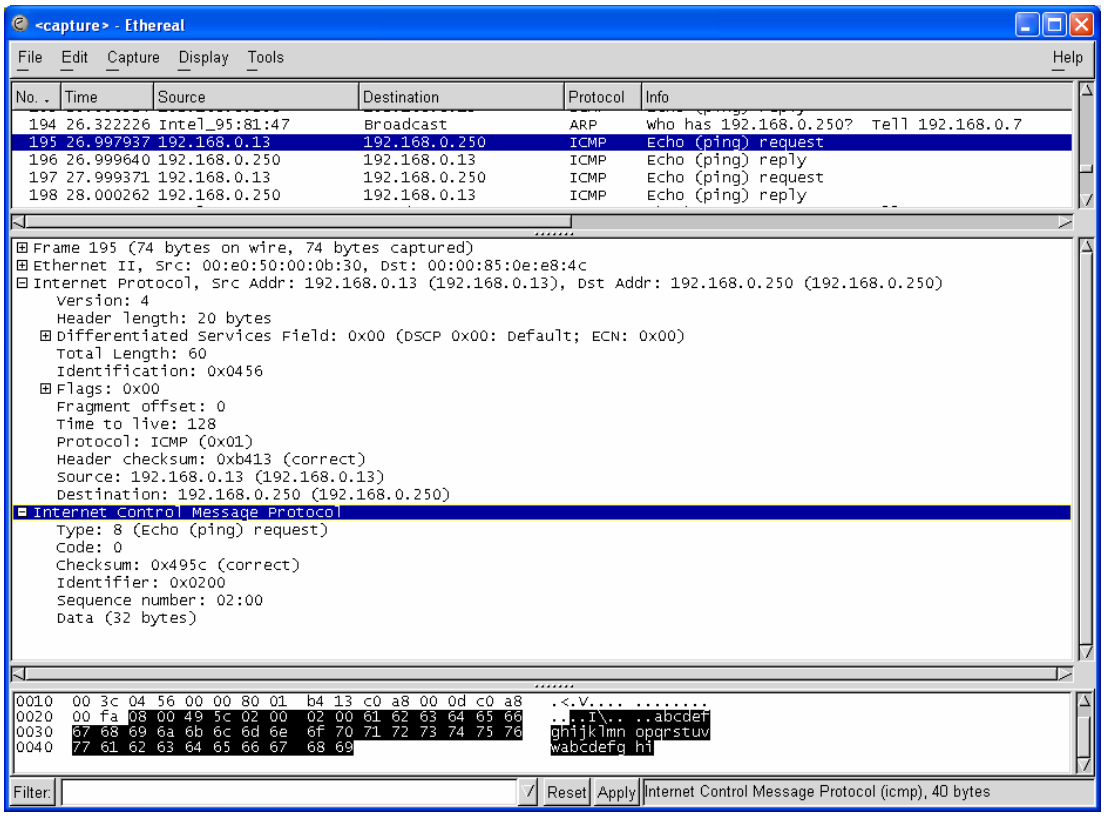
Tip 0,8: Bu kodlar IP paketin hedef bilgisayara ulaşıp ulaşmadığını doğrulamak için kullanılır. **"ICMP Echo Request Message: Type 8"** ile hedef bilgisayarın erişilebilir olup olmadığı, **"ICMP Echo Reply Message: Type 0."** mesajı ile de doğrulama yapılır.

Tip 3: Paket hedef bilgisayara teslim edilememişse router **"ICMP Destination Unreachable Message"** mesajı gönderir. Yerine ulaşamayan mesajlar için hatanın kaynağına işaret eden kodlar tanımlanır. Aşağıda ana kodlar gösterilmiştir.

Kod	Açıklama
0	Ağ erişilemez.
1	Host erişilemez.
2	Protokol erişilemez.
3	Port erişilemez.
4	Veri bölünmeli veya bölünmemelidir.
5	Kaynak yol geçersiz.

Tablo 2.2: ICMP hedef erişim mesajları

Aşağıdaki şekilde network analiz programıyla PING komutu kullanılarak elde edilmiş ICMP paketini görmektesiniz.



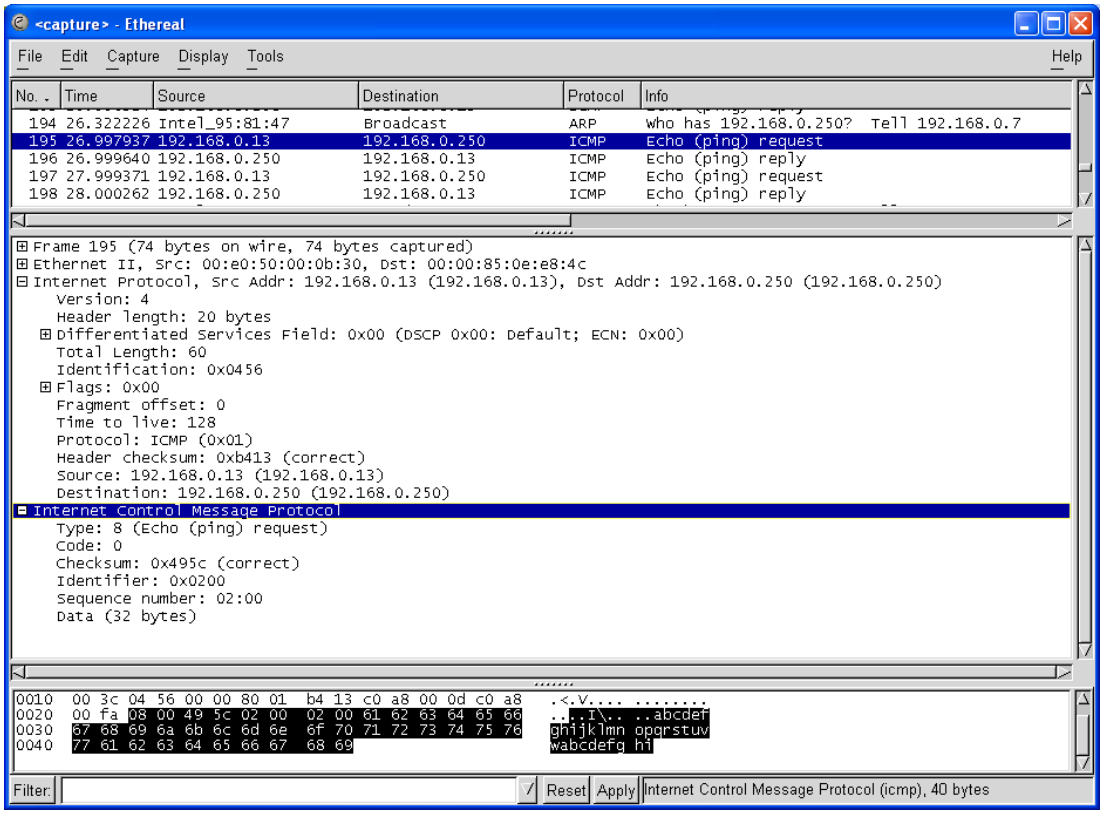
Şekil 2.2: ICMP paket analizi

UYGULAMA FAALİYETİ

Network analiz programını kullanarak ICMP paketi yakalayınız.

İşlem Basamakları	Öneriler
➢ Ethereal ya da Wireshark programını başlatınız.	➢ "Programın filtre bölümüne ICMP yazabilirsiniz.
➢ Programda yakalama işlemini başlatınız. ➢ Aynı ağda bulunan bir bilgisayarın IP numarasına ping işlemi yapınız. ➢ Yakaladığınız ICMP paketini inceleyerek tip, kod, check sum ve ICMP data bilgilerini not alınız.	➢ PING komutunun kullanımı: ***Örnek:*** PING 192.168.0.23

Aşağıda örnek bir ICMP paketi gösterilmiştir.



ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin sonunda boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) ICMP paketin amacı router'den kaynak bilgisayara hata mesajı göndermektir.

2. ( ) ICMP paketin amacı kontrol amacıyla mesaj alışverişi yapmaktır.

3. ( ) Type 0,8 mesajı, paketin hedef bilgisayara ulaşıp ulaşmadığını kontrol eder.

4. ( ) Type 3 mesajı, paket hedef bilgisayara teslim edilmişse verilir.

5. ( ) Ethereal programı, network analizi için kullanılır.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ–3

AMAÇ

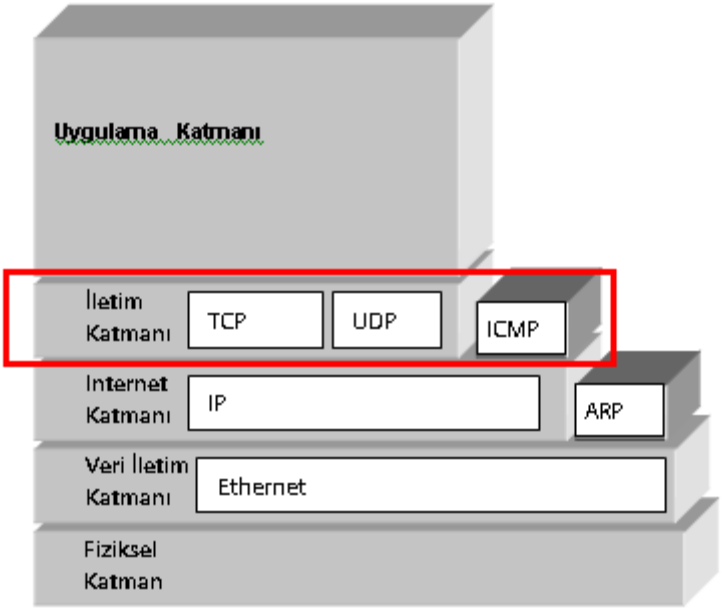
TCP paketlerini inceleme işlemini ağ analiz programında hatasız olarak yapabileceksiniz.

ARAŞTIRMA

- İletim (transport) katmanı ile ilgili araştırma yapınız.

3. İLETİM KATMANI

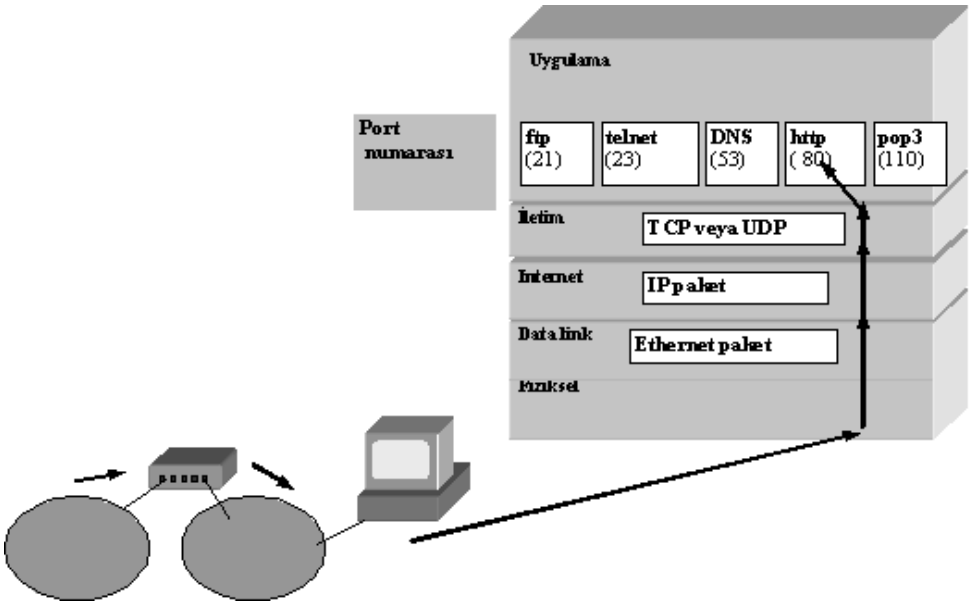
İletim katmanında, TCP (transmission control protocol) ve UDP (user datagram protocol) protokolleri kullanılır. Şimdiye kadar öğrendiğimiz katmanlar ve bu katmanlarda kullanılan protokoller aşağıdaki şekilde gösterilmiştir.



Şekil 3.1: TCP/IP'nin hiyerarşik yapısı

3.1. Port Numaraları

İnternet katmanı kullanarak belirtilen yol üzerinden IP paketi hedef bilgisayara gönderebiliriz. Fakat genellikle bilgisayarımızda birden çok program birlikte çalışmaktadır. Bu durumda hangi paketin hangi program için gönderildiğini bilmek için port numarası kullanılmalıdır. Port numarası her bir network programına atanır ve iletim katmanına gelen paketlerin dağıtılması amacıyla kullanılır. Bu nedenle UDP ve TCP protokol paketlerinde port numarası belirtilir.



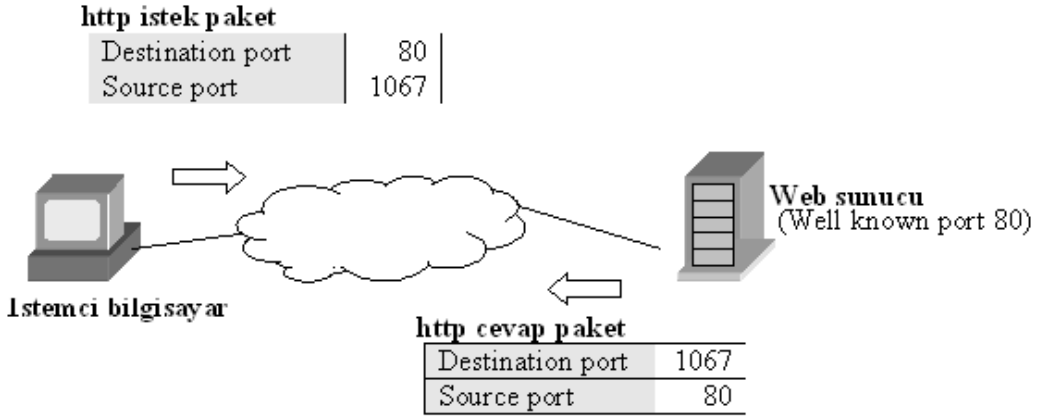
Şekil 3.2: TCP/IP ve port numaraları

16 bitlik port numarası üç bölümde incelenebilir.

Kategori	Aralık	Açıklama
Well known port (veya sistem portu)	0 – 1023	Sunucu programları (www, mail, DNS vb.) kullanır. ICANN (internet corporation for assigned names and numbers) tarafından tanımlanır.
User port (kullanıcı portu)	1024 – 49151	Sunucuya erişen istemci programları bu port numaralarını kullanır. Numaralar OS tarafından atanır.
Private port (özel port)	49152 – 65535	Özel sunucular bu port numaralarını kullanır.

Örneğin web sunucu üzerinde bulunan bir web sitesine eriştiğinizde Web Browser'in (internet explorer vb.) OS tarafından atanan **user portu** vardır. TCP protokolü kullanılarak web sunucunun 80 numaralı "**well known**" portuna istek paketi gönderilir. Web sunucu "**well known**" portundan user porta web sayfalarını gönderir.

Aşağıdaki şekli inceleyiniz.



Şekil 3.3: Port numaraları ile iletişim örneği

Server program bazen service (hizmet) olarak isimlendirilir. Her bilgisayar services isimli bir dosyaya sahiptir. Bu dosya service adı ile port numarası arasında çevirim yapar.

Windows XP'de bu dosya C:\WINDOWS\system32\drivers\etc\services içindedir. Editör (notepad vb.) programı kullanarak bu dosyanın içeriğini görebilirsiniz.

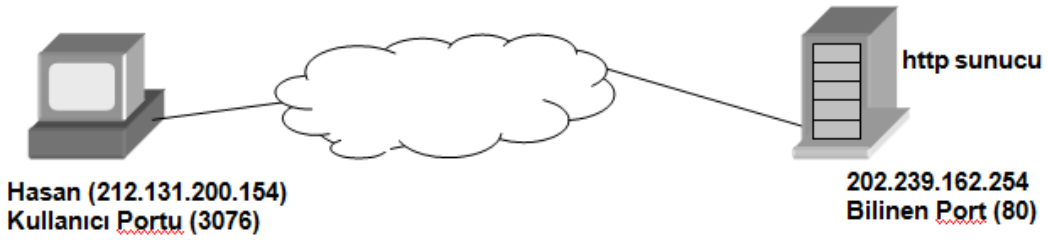
3.2. "netstat" komutu

Bilgisayarınızda hangi portun aktif olarak kullanıldığını kontrol etmek için netstat komutu kullanılır. Netstatın kulanım şeklerini inceleyelim.

- Netstat komutu ile aktif bağlantılarınızı görüntüleyelim.

(Bilgisayar adı Hasan ise)

```
C:XXX> netstat

Active connections

Proto  Local Address          Foreign Address          State
TCP    Hasan:3076             202.239.162.254:http     TIME_WAIT
```

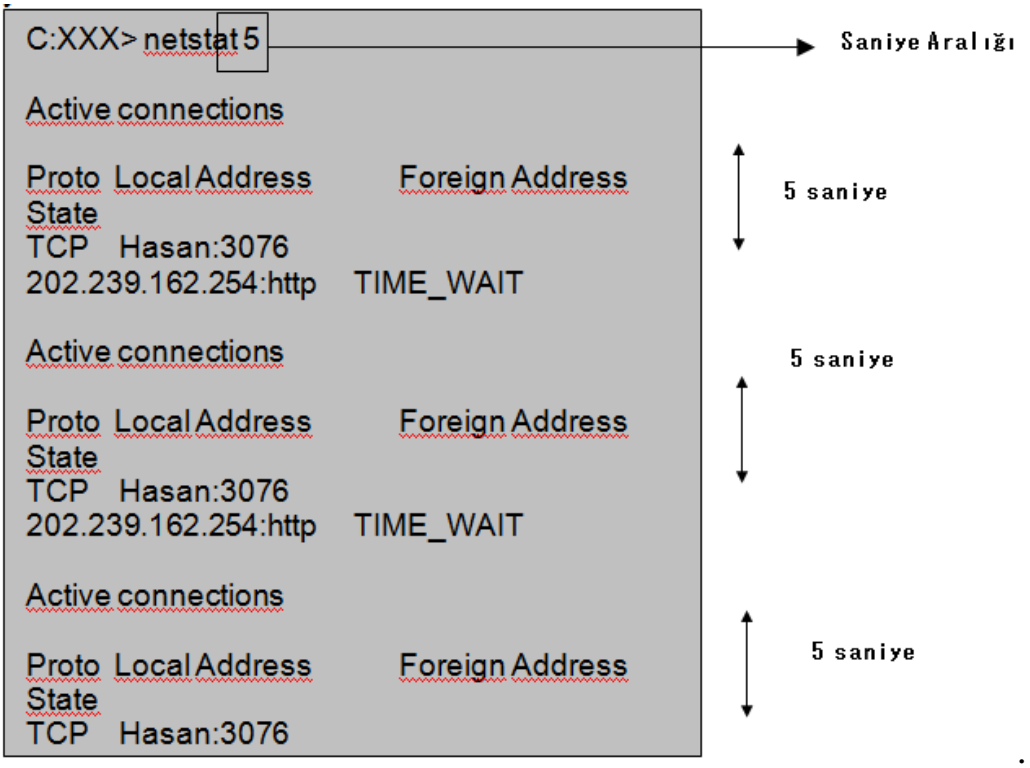


Şekil 3.4: Netstat komutu uygulaması

- Netstat –n komutu kullanarak IP adres ile birlikte görüntüleyelim.

```
C:XXX> netstat -n

Active connections

Proto  Local Address          Foreign Address         State
TCP    217.131.200.154:3076   202.239.162.254:80      TIME_WAIT
```

- Zaman opsiyonu kullanarak belirli zaman aralıklarında kontrolü yeniler.



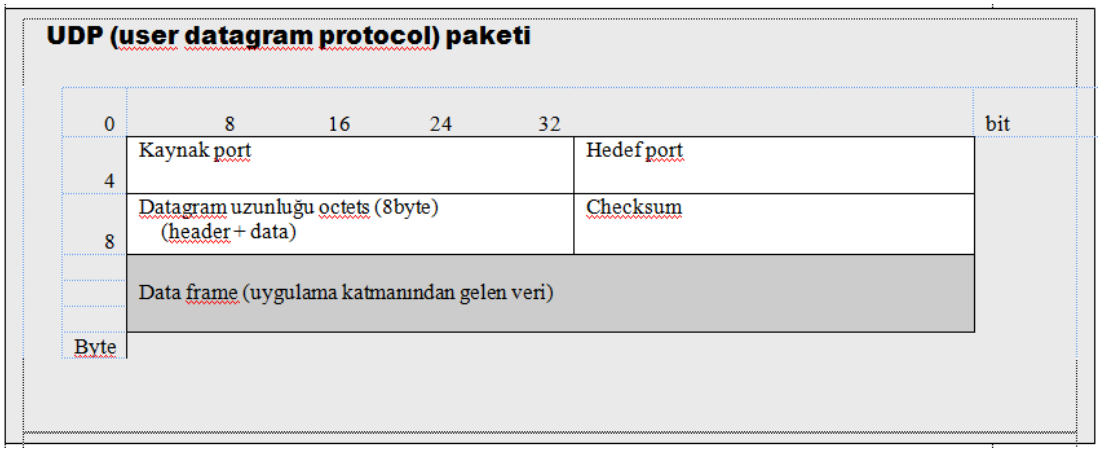
➢ Bilgisayarınızda kullanılan tüm portları kontrol edebilirsiniz. (Bilgisayar adı HOST1)

```
C:XXX> netstat -an

Active connections

Proto  Local Address          Foreign Address
TCP    0.0.0.0:135            0.0.0.0:0
TCP    0.0.0.0:445            0.0.0.0:0
TCP    0.0.0.0:1025           0.0.0.0:0
TCP    0.0.0.0:5000           0.0.0.0:0
TCP    192.168.0.15:139       0.0.0.0:0
UDP    0.0.0.0:135            *.*
UDP    0.0.0.0:445            *.*
UDP    0.0.0.0:500            *.*
UDP    0.0.0.0:1026           *.*
UDP    0.0.0.0:1027           *.*
UDP    0.0.0.0:1037           *.*
```

```
C:XXX> netstat -a

Active connections

Proto  Local Address          Foreign Address        State
TCP    HOST1:epmap            HOST1:0                LISTENING
TCP    HOST1:microsoft-ds     HOST1:0                LISTENING
TCP    HOST1:1025             HOST1:0                LISTENING
TCP    HOST1:5000             HOST1:0                LISTENING
TCP    HOST1:netbios-ssn      HOST1:0                LISTENING
UDP    HOST1:emap             *.*
UDP    HOST1:Microsoft-ds     *.*
UDP    HOST1:isakmpemap       *.*
```

3.3. UDP

UDP (user datagram protocol) paketinin detayları aşağıda gösterilmiştir. İletim katmanı paketi bazen datagram olarak isimlendirilir.



Şekil 3.5: UDP yapısı

Yukarıdaki açıklamadan görülebileceği gibi UDP basit bir yapıya sahiptir. UDP, source port ve destination port numarası haricinde kayda değer bir bilgiyi içermez. Bu basit yapısından dolayı UDP hızlı bilgi transferi amacıyla tercih edilir ve bazı uygulama katmanı protokolleri tarafından kullanılır. Genellikle ses ve video aktarım servisleri için uygundur.

3.4. TCP

- **TCP ile güvenli iletim**

UDP'den farklı olarak TCP daha güvenli bilgi aktarım imkânı verir. İletim katmanında TCP kullanıldığında tüm paketlerin kayıpsız bir şekilde iletileceğine emin olabiliriz.

Bunun için TCP, her bir pakete göndermeden önce bir sıra numarası (sequence number) verir. Bilgiyi alan bilgisayardaki TCP, bilginin eksiksiz alındığına dair acknowledged number kullanarak ACK paketini geri gönderir. Acknowledged numarası, alınan paketin data genişliğinin sıra numarasına eklenmesiyle elde edilir. Gönderici bilgisayar ACK paketi aldığında bilginin doğru olarak iletildiğini anlar.

Bu karşılıklı paket iletişiminde TCP bağımsız bir numara sistemi kullanır.

Bu numara sistemini kullanmak için iki bilgisayar arasında TCP ile iletişim kurulmalıdır.

Burada iletişim ile iki bilgisayar arasındaki özel bir ilişki ifade edilmektedir (Daha güvenilirdir ve farklı iki bilgisayarın uygulama programları söz konusudur.).

Bu nedenle TCP ile iletişimin üç aşaması vardır.

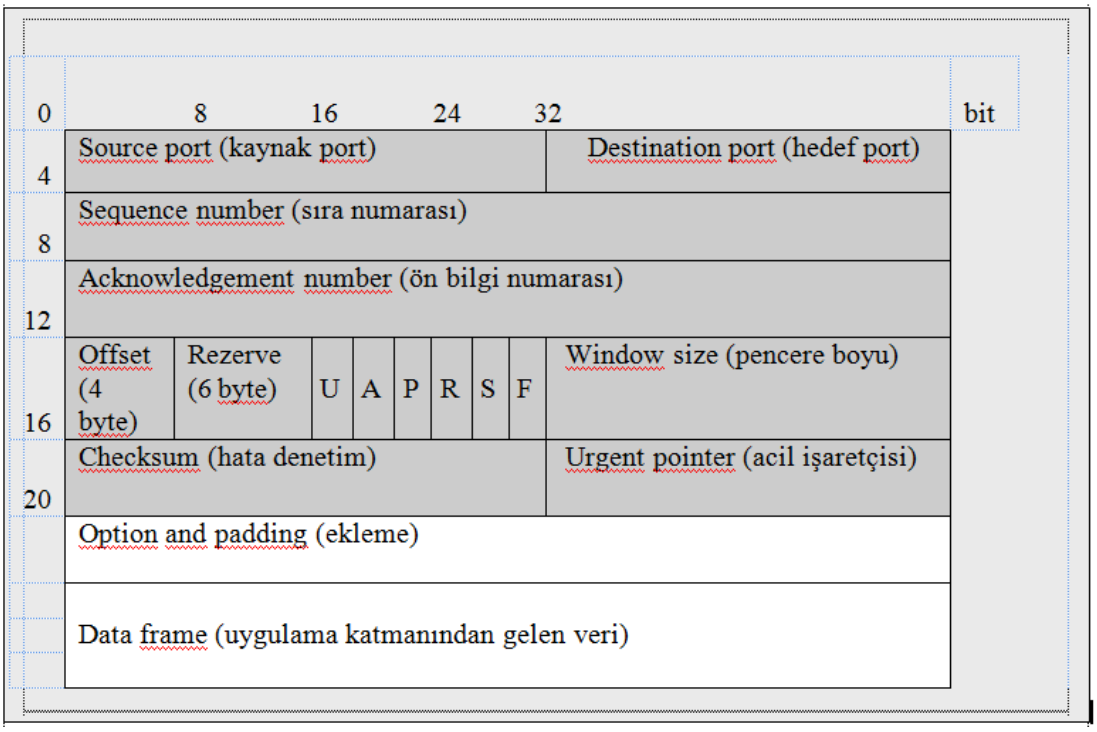
- İletişimin kurulması (establish connection)
- Veri aktarımı (data transmission)
- İletişimin kesilmesi (disconnection)

TCP protokolünü daha iyi anlamak için bu üç aşamayı çok iyi bilmeliyiz.

➢ **TCP Paket**

TCP (transmission control protocol) paket detayları aşağıda belirtilmiştir.

TCP (transmission control protocol) paket TCP başlığı



Şekil 3.6: TCP paket

➢ **Source port ve destination port (kaynak port ve hedef port)**

Bu konuda daha önce çalışma yapılmıştı.

➢ **Sıra numarası (sequence number)**

Başlangıçta sıra numarası TCP tarafından atanır. İletişim kuracak iki bilgisayarın yeni iletişimi fark etmesi için her bir bağlantının (Buna bazen oturum da denir.) başlangıç sıra numarası farklı olmalıdır. Bu nedenle 0 olmamalıdır ve bu numara bilgisayarın "running time" değeriyle artmalıdır (Her 4 milisaniyede 1 artması tavsiye edilir.).

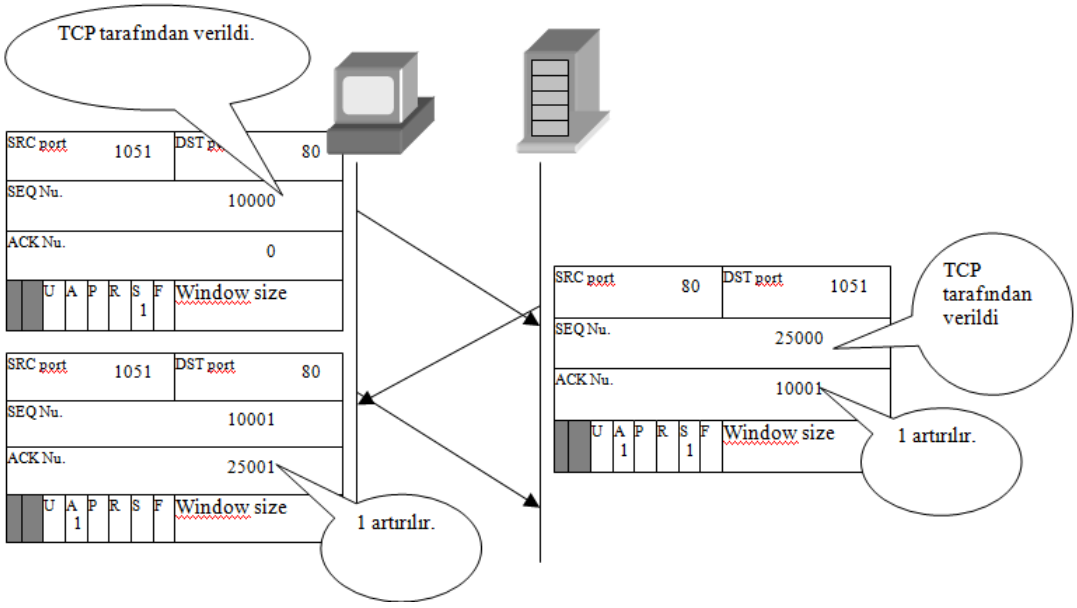
Daha sonra ikinci paketin sıra numarası aşağıdaki şekilde artırılır.

Önceki paket (previous packet)	**Sıra numarası artışı (sequence number increment)**
İletişimin kurulması, paketin alındığına dair onay verilmesi ve iletişimin kesilmesi için gönderilen paketler (Bu paketler için data genişliği 0'dır.)	**1**
Bilgi aktarımı (data transmission)	**Data genişliği**

➢ **Acknowledgement number (ön bilgi numarası)**

Acknowledgement number: Paketin alındığına dair onay numarasıdır. Yalnızca ACK flag [sayfa 46 (flags)] "1" olduğunda değişir. Alınan paket sorunsuz ise bu paketin sıra numarasına "1" eklenerek hesaplanan yeni numara "acknowledgement" numarası olarak set edilir.

Aşağıdaki TCP paket başlık örneği iletişimin kurulmasına (1. aşama) örnektir.



Şekil 3.7: İletişimin kurulması

- **Offset**

TCP paketinde verinin nereden başladığını ifade eder. 4 byte alan kaplar. TCP başlığında böyle bir seçenek olmadığında 5 byte olacaktır (5 = 20 / 4).

- **Reserved (rezerve)**

Bu bölüm daha sonra kullanılmak üzere ayrılmıştır.

- **Bayraklar (flags)**

Harf	Sembol	Karşılık gelen bit "1" olduğunda anlamı
U	URG (urgent flag)	Bu paketin acil olarak alınması gerektiğini ifade eden bilgiyi içerir. Bu "urgent pointer" tarafından belirlenir.
A	ACK (acknowledgment flag)	Acknowledgement alanını etkileyen numara
P	PSH (push flag)	Bu paket tamponlanmamalı ve hemen uygulama katmanındaki programa verilmelidir.
R	RST (rest flag)	İletişimi kesme
S	SYN (synchronize flag)	İletişimi oluşturma isteği
F	FIN (finish flag)	İletişimi kesme isteği (veri iletiminin sonu)

- **Pencere genişliği (window size)**

Bilgisayarın tamponunun genişliğini ifade eder. Diğer bilgisayar "acknowledgement" kullanmadan kesintisiz bilgi gönderebilir.

- **Check sum**

TCP başlığının bozuk olup olmadığını kontrol etmek için kullanılır.

- **Urgent pointer**

Yalnızca URG bayrağı "1" olduğunda etkilidir. Acil verinin yerini işaret eder.

3.5. Soket Kavramı

Soketler, aynı veya farklı hostlar üzerindeki süreçlerin haberleşmesini sağlayan bir haberleşme yöntemidir. Soket programlama da iki tür program oluşturulmalıdır.

İstemci (client): Hizmet isteyen soket programlara denir.
Sunucu (server): Hizmet veren soket programdır.

Bir bilgisayarda birden çok soket bulunabilir. Örneğin aynı anda hem telnet soketi hem de ftp soketi açık olabilmektedir. Soketleri birbirinden ayırmak ve istemci-sunucu ikilisini birbiri ile buluşturmak için her soket programın PORT numarası vardır.

Örneğin *ftp*nin port numarası 21'dir. Bir ftp istemci, ftp sunucunun 21. portta çalıştığını bildiğinden doğrudan onunla temasa geçer. Telnet 23.u portta çalıştığından telnet sunucu ile ftp sunucu karışmaz. 1-1024 arasındaki portlar standarttır ve yalnız root tarafından kullanılabilir.

- **Socket türleri**

Çeşitli soket türleri vardır. Bunlardan yalnızca en çok kullanılan üçü burada anlatılacaktır. Bunlar "Stream Soketler" , "Datagram Soketler" ve "Raw Soketler" dir. Bunlar programlarda sırasıyla SOCK_STREAM, SOCK_DGRAM ve SOCK_RAW isimleri ile kullanılır.

Programda socket() açarken türü belirtilir. Stream soketlere bağlantı yönelimli (connection oriented) soketler, Datagram soketlere ise bağlantısız (connectionless) soketler denir.

Stream soketler, TCP/IP protokolunun taşıma katmanında bulunan TCP'yi (Transmission Control Protocol) kullanır. Datagram soketler ise yine aynı katmandaki UDP'yi (User Datagram Protokol) kullanır.

Bu iki türün özellikleri ve aralarındaki temel farkları şöyle sıralayabiliriz.

- Stream soketler verileri sıralı gönderir, datagram soketleri sıralı göndermeyebilir.

- Stream soketler veri bütünlüğünü garanti eder, Datagram soketler veri bütünlüğünü garanti etmez (TCP bir paketi gönderdiği zaman, karşı taraf paketi aldığını haber vermeden, kendini o paketi göndermiş saymaz ve tekrar gönderir. Ayrıca paketin doğru gidip gitmediğini anlamak için başlık bilgisinde checksum kontrol bilgisi tutar. UDP'de checksum kontrol bilgisi tutar ancak checksum yanlışsa aynı paketi tekrar istemez.).

- Stream soketler, işlem bitene kadar kesintisiz bir bağlantı kurar. Datagram soketler ise bağlantı kurmaz. Sadece veri göndereceği zaman bağlantı kurar ve işi bitince bağlantıyı koparır.

UYGULAMA FAALİYETİ

Netstat komutu ile ilgili uygulamalar gerçekleştiriniz.

İşlem Basamakları	Öneriler
➢ Netstat komutunu zaman aralığı fonksiyonu ile birlikte kullanarak bağlantı kontrolü yapınız.	➢ Netstat komutunun kullanım şeklini netstat –h komutu ile öğrenebilirsiniz.
➢ Komutu başlattıktan sonra bilgisayarınızdan WWW servere erişiniz ve bilgisayarınızda netstat komut uygulamasını takip ediniz. ➢	
➢ UDP (DNS) veya TCP (WWW server erişimi veya dosya kopyalarken vb.) paket yakalayınız ve bunları inceleyiniz.	➢ Paket yakalama işlemi için yine "ethereal" ya da "wireshark" programlarını kullanabilirsiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin sonunda boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Netstat komutu aktif portları görebilmek için kullanılır.

2. ( ) Netstat –n komutu ile host adları şeklinde listelenme yapılır.

3. ( ) Netstat –an ile tüm aktif portları listeletebiliriz.

4. ( ) UDP haberleşme TCP ye göre daha yavaştır.

5. ( ) TCP iletişimi güvenli bir iletişimdir.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ–4

AMAÇ

TCP paketlerini ağ analiz programında hatasız olarak incelemek

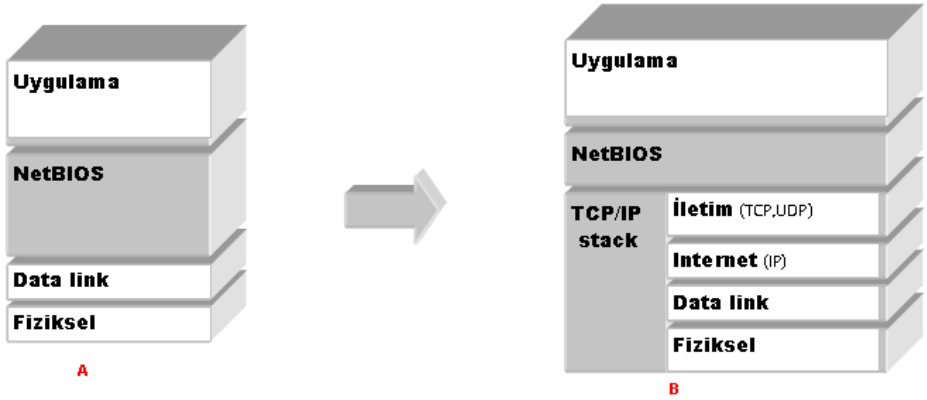
ARAŞTIRMA

- NBT hakkında araştırma yapınız.

4. NETBIOS VE TCP/IP

Başlangıçtan bu yana Microsoft TCP/IP'den farklı bir network protokolü kullanmaktadır. Bu sistem NetBIOS olarak isimlendirilir.

TCP/IP'de olduğu gibi NetBIOS'da da datalink katman için MAC adres kullanılır. Çünkü her iki protokolde aynı ethernet kartı(LAN card) kullanır. Fakat NetBIOS'da IP adres yerine NetBIOS name kullanılır. NetBIOS name bilgisayar adı ile aynıdır.



Şekil 4.1: A. Geleneksel Microsoft Network-------B. NetBIOS ile TCP/IP

Yalnızca bir ağ için NetBIOS kullanışlı bir sistemdir, fakat ağlar arası iletişimde ya da sürekli internet erişimi istenen yerlerde çok iyi olduğu söylenemez. Bu nedenle Microsoft, NetBIOS üzerinde bazı değişiklikler yaparak TCP/IP üzerinde çalışma imkânı sağlanmıştır.

Bu durum "NetBIOS over TCP/IP (NBT)" olarak isimlendirilmiştir ve Windows XP'nin default (varsayılan) durumu olarak belirlenmiştir.

Bu nedenle NBT, TCP paket ya da UDP paket içinde NetBIOS name veya port numarası ve IP paket içinden de IP adres kullanır.

Microsoft bu yeni düzenlemeyi yaptığında eski NetBIOS protokolünü de kullanılabilir yaptı. Bu sistem de NetBEUI olarak isimlendirildi.

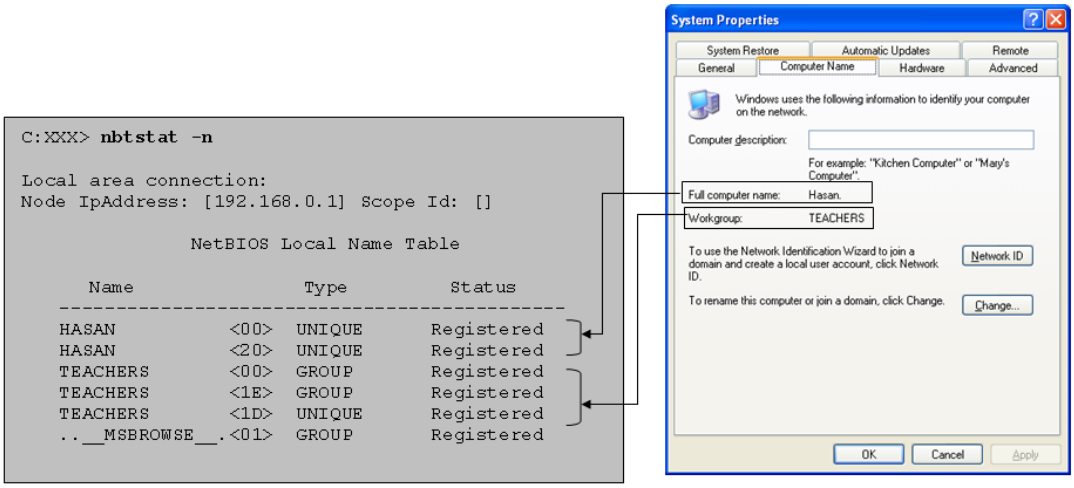
- **Name table**

Microsoft Network'te her makine bir isim tablosuna (Name table) sahiptir. Nbtstat komutu ile bu isim tablosunu görebiliriz.

- Bilgisayarınızda "Name table" ağa bağlanmadan önce aşağıdaki gibi olabilir.^

```
C:XXX> nbtstat -n

Local area connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

- Ağa bağlandıktan sonra bilgisayarınızda "Name table"



Şekil 4.2: nbtstat komutu

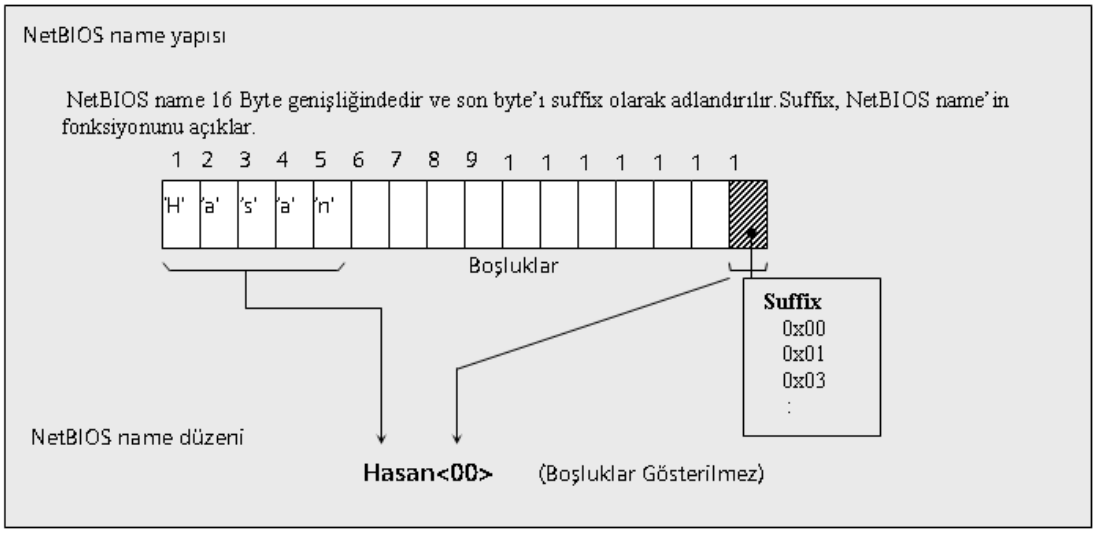
- Bilgisayarınızdan diğer bir bilgisayarın name tablosunu görmek için bilgisayar adı (-a parametresi ile) ya da IP adres (-A parametresi ile) kullanabilirsiniz.

```
C:XXX> nbtstat -a mustafa

Local area connection:
Node IpAddress: [192.168.0.1] Scope Id: []

                NetBIOS Remote Machine Name Table

      Name               Type         Status
   ---------------------------------------------
   MUSTAFA        <00>  UNIQUE       Registered
   MUSTAFA        <20>  UNIQUE       Registered
   TEACHERS       <00>  GROUP        Registered
   TEACHERS       <1E>  GROUP        Registered
   MUSTAFA        <03>  UNIQUE       Registered
   TURGAY         <03>  UNIQUE       Registered

   MAC Address = 00-40-26-70-35-BC
```

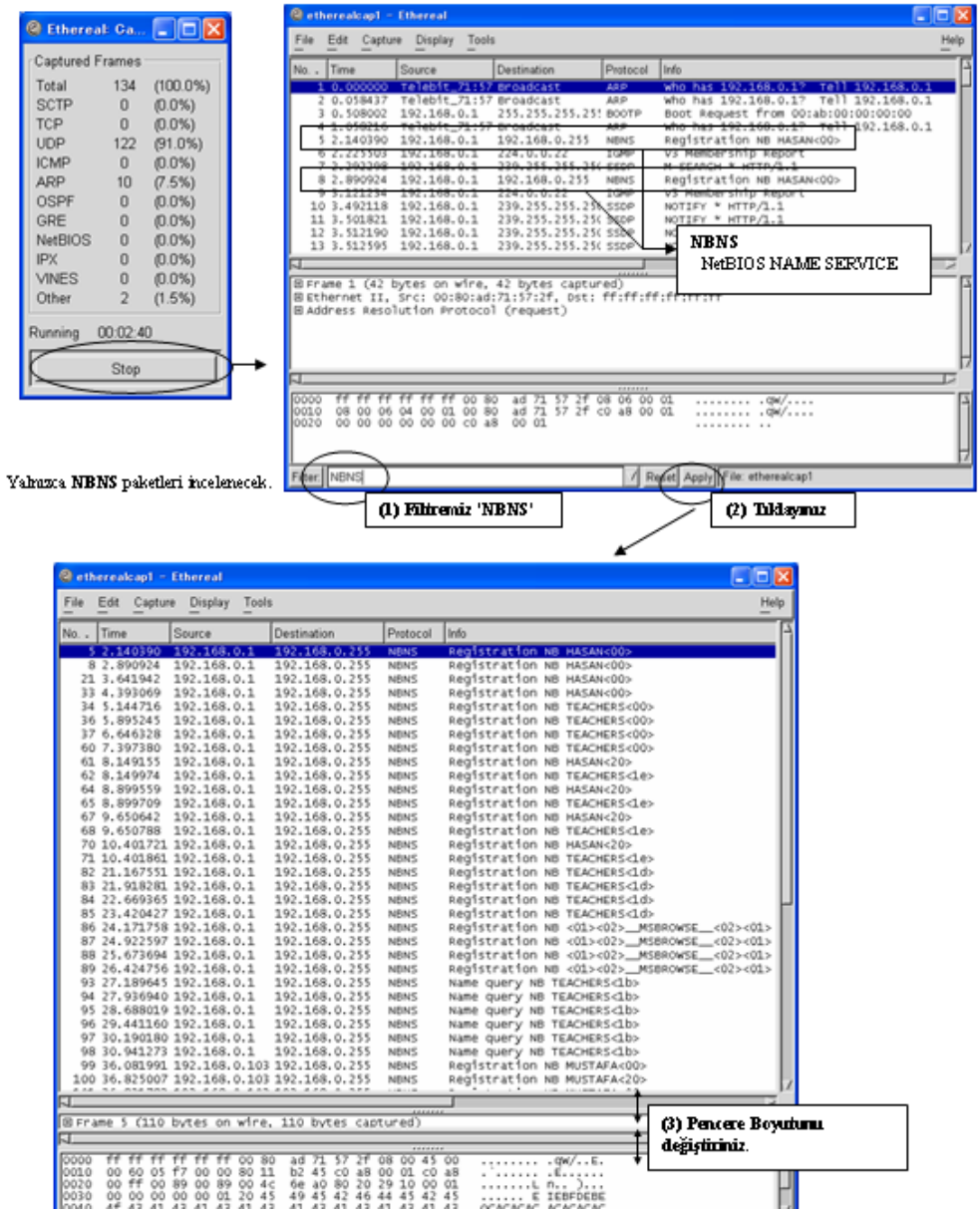
```
C:XXX> nbtstat -A 192.168.0.3

Local area connection:
Node IpAddress: [192.168.0.1] Scope Id: []

                NetBIOS Remote Machine Name Table

      Name               Type         Status
   ---------------------------------------------
   MUSTAFA        <00>  UNIQUE       Registered
   MUSTAFA        <20>  UNIQUE       Registered
   TEACHERS       <00>  GROUP        Registered
   TEACHERS       <1E>  GROUP        Registered
   MUSTAFA        <03>  UNIQUE       Registered
   TURGAY         <03>  UNIQUE       Registered

   MAC Address = 00-40-26-70-35-BC
```

- **NetBIOS name**

Name tablosunda computer name ve workgroup name ile birlikte ek olarak birçok bilgi de görülmektedir. Bilgisayar adı ile birlikte tırnak içindeki numara (computer name and <XX>) NetBIOS name olarak isimlendirilir. NetBIOS name çeşitli servis hizmetleri sunmak amacıyla kullanılır. NetBIOS name hakkında detaylı bilgi aşağıda belirtilmiştir.



Aşağıda cross kablo ile birbirine bağlanmış iki bilgisayarın iletişiminde yakalanan paketler görülmektedir. Bu iki bilgisayarın iletişiminde birçok paketin hareket ettiğini görmektesiniz. Biz şu anda yalnızca NBNS (NetBIOS name service) paketleriyle ilgileneceğiz.



Başlangıçta tüm NetBIOS isimleri için registration paketi (kayıt paketi) yayımlanır. Bu paketler önce ağ içinde IP broadcast (IP yayını) yapılır. Eğer aynı NetBIOS isimli bilgisayar varsa kaydeden bilgisayar bu bilgisayardan cevap paketi alır. (Tabi ki workgroup adı farklı olduğunda NetBIOS isimi aynı olabilir.) Registration paketine cevap gelmezse, aynı isimli bilgisayar olmadığı anlamına gelir ve NetBIOS name başarıyla kaydedilmiş olur.

UYGULAMA FAALİYETİ

Bilgisayarınız ile ağa bağlanmadan önce ve ağa bağlandıktan sonra “Name table” sorgulaması yapınız.

İşlem Basamakları	Öneriler
➢ Ağa bağlı değil iken nbtstat komutunu kullanınız.	➢ Terminal komutlarına dikkat ediniz.
➢ Sonuçları word belgesi içerisine yapıştırınız.	➢ Komut parametrelerine dikkat ediniz.
➢ “Ağ kablosunu bağlayınız ve tekrar nbtstat komutunu kullanınız.	
➢ Sonuçları word belgesi içerisine yapıştırınız.	

ÖLÇME ve DEĞERLENDİRME

Aşağıdaki cümlelerin sonunda boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Microsoft TCP/IP'den farklı bir network protokolü kullanmaktadır. Bu system NetBIOS olarak isimlendirilir.

2. ( ) NetBIOS'da da datalink katmanı için IP adres kullanılır.

3. ( ) NetBIOS ağlar arası iletişimde oldukça kullanışlıdır.

4. ( ) NetBEUI, NetBIOS ile TCP /IP sentezlenmesinden ortaya çıkmıştır.

5. ( ) nbtstat komutu bilgisayarınızdaki aktif "Name table" ı görmek için kullanılır.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise "Modül Değerlendirme" ye geçiniz.

MODÜL DEĞERLENDİRME

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet,** kazanamadıklarınız için **Hayır** kutucuklarına (X) işareti koyarak kontrol ediniz.

Değerlendirme Ölçütleri	**Evet**	**Hayır**
1. Network analiz programını kurabiliyor musunuz?		
2. Analiz programı ile IP paketi yakalayabiliyor musunuz?		
3. Netstat komutunu kullanabiliyor musunuz?		
4. Bilgisayarınızdaki aktif "Name table" görüntüleyebiliyor musunuz?		

DEĞERLENDİRME

Değerlendirme sonunda "Hayır" şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetlerini tekrar ediniz. Bütün cevaplarınız "Evet" ise bir sonraki modüle geçmek için öğretmeninize başvurunuz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

1.	**Yanlış**
2.	**Doğru**
3.	**Doğru**
4.	**Yanlış**
5.	**Yanlış**

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

1.	**Yanlış**
2.	**Doğru**
3.	**Doğru**
4.	**Yanlış**
5.	**Doğru**

ÖĞRENME FAALİYETİ-3'ÜN CEVAP ANAHTARI

1.	**Doğru**
2.	**Yanlış**
3.	**Doğru**
4.	**Yanlış**
5.	**Doğru**

ÖĞRENME FAALİYETİ-4'ÜN CEVAP ANAHTARI

1.	**Doğru**
2.	**Yanlış**
3.	**Yanlış**
4.	**Doğru**
5.	**Doğru**

KAYNAKÇA

- MASUDA Yoichi, Bülent VARDAL, Web Sistem Uygulamaları – Jica–Meb Endüstriyel Otomasyon Teknolojileri Kurulum Projesi, Eylül, 2004.
- MASUDA Yoichi, İbrahim APA, Endüstriyel Otomasyon Teknolojileri Bilgisayar Ağları, Jica–Meb Endüstriyel Otomasyon Teknolojileri Kurulum Projesi Ağustos 2005.