T.C.
MİLLÎ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

TEMEL YÖNLENDİRİCİ SORUNLARI

ANKARA 2008

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**481BB0060**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**Temel Yönlendirici Sorunları**
MODÜLÜN TANIMI	Yönlendirme sorunlarını giderebilmek için bilgi ve becerilerin verildiği öğrenme materyalidir.
SÜRE	40/24
ÖN KOŞUL	TCP/IP Kontrol Mesajları modülünü almış olmak
YETERLİK	Yönlendirici sorunlarını gidermek
MODÜLÜN AMACI	**Genel Amaç** Gerekli ortam sağlandığında, temel yönlendirici sorunlarını giderebileceksiniz. **Amaçlar** **1.** Yönlendirme tablolarını görüntüleyebilecek ve yönlendirme tablolarını inceleme işlemini yapabileceksiniz. **2.** Komutları kullanarak katmanları, ağı test etme işlemini yapabileceksiniz. **3.** Komutları kullanarak sorun giderme işlemini yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam** Ağla birbirine bağlı bilgisayar laboratuvarı, yönlendirici, modem, switch, bridge, router ve simülatör programı
ÖLÇME VE DEĞERLENDİRME	Modülün içinde yer alan her öğrenme faaliyetinden sonra, verilen ölçme araçlarıyla (çoktan seçmeli test, doğru yanlış testi vb.) kazandığınız bilgileri ölçerek kendinizi değerlendireceksiniz. Modül sonunda performans testi ile kazandığınız yeterlilikleri değerlendireceksiniz.

GİRİŞ

Sevgili Öğrenci,

Bilgisayar ağı, elektronik tabanlı haberleşmenin ve bilgisayar uygulamalarının kan damarıdır. Ağ üzerinde oluşan bir sorun, tüm sistemin performansını düşürmektedir; bu yüzden çıkabilecek sorunları önceden tahmin etmek ve bu sorunların çözüm yollarını öğrenmek ağın performans düşümünü ve boşa geçen zamanı azaltacaktır.

Bu modülde; yönlendirmeyi inceleyecek, ağ testini, yönlendirici sorunlarını tespit etme konularını göreceksiniz. Öğrendiğiniz bu bilgiler doğrultusunda, yönlendirme tablolarını görüntüleyebilecek ve yönlendirme tablolarını inceleyebilecek, komutları kullanarak katmanları ağı test edebilecek ayrıca oluşan sorunları giderebileceksiniz.

Bilgisini yenileyen, artıran bireyler her zaman bir adım önde olacaklar ve gelişen teknolojiye ayak uydurabileceklerdir. Bu yüzden kendimizi yeni bilgilerle donatmalıyız ki ağ işletmenliği alanında aranan bir ağ teknisyeni olalım.

Bu modülü öğrenmek için gerekli dikkati ve özveriyi göstereceğinize eminim.

Başarılar.

ÖĞRENME FAALİYETİ–1

AMAÇ

Yönlendirme tablolarını görüntüleyebilecek ve yönlendirme tablolarını inceleme işlemini yapabileceksiniz.

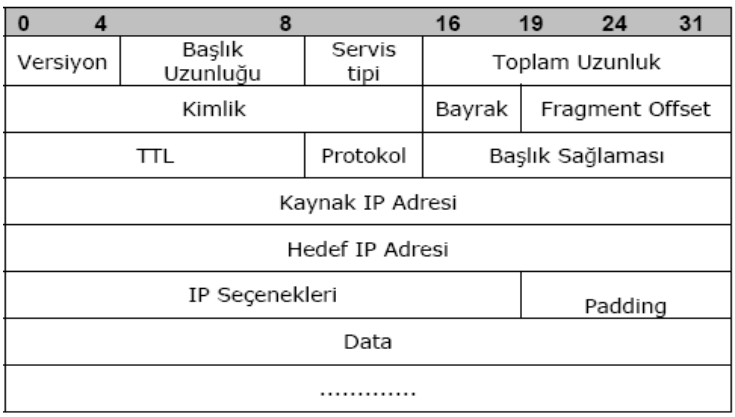
ARAŞTIRMA

- Ağ tasarımı ve yönlendirici ayarları için kullanılan simulator ve emulator programlarını araştırınız.

1.YÖNLENDİRMENİN İNCELENMESİ

1.1. Paketlerin İletimini İnceleme

İletişim kuran iki bilgisayar arasındaki verinin nasıl iletildiğinden bahsedelim. Örneğin, arkadaşınıza bir dosya göndereceksiniz. Göndereceğiniz dosyayı bir yazılım kullanarak (MSN, Google Talk vb.) gönderirsiniz. Göndereceğiniz bu dosya FTP protokolü tarafından veriye dönüştürülür. Daha sonra dosyadaki yazılar, şekiller ve fotoğraflar ASCII ve GIF gibi standartlar tarafından ortak bir formata dönüştürülür. Ortak bir formata dönüşmüş olan verinin gönderilmesi için bir protokol yardımıyla oturum numarası verilir ve karşı taraftaki bilgisayarla iletişim için sanal oturum açılır. Veri, gönderileceği yere hazır hale getirilmeye başlanır ve aktarım başlığı (transport header) eklenerek parçalara bölünür. Parçalara ayrılmış veri, ağ başlığı eklenerek paketlere dönüştürülür. Ağ katmanı da ağ başlığını (network header) ekleyerek veriyi pakete dönüştürür. Paketin yapısı aşağıdaki gibidir:



Şekil 1.1: Paket yapısı

Versiyon: Kullanılan IP versiyonu (4 bit)

IP Başlık Uzunluğu: Başlığın uzunluğu (4 bit)

Servis Tipi: Üst katmanların belirlediği önemlilik seviyesi (8 bit)

Toplam Uzunluk: Data ve başlık dahil toplam uzunluk (16 bit)

Kimlik: Datagramı tanımlayan bir tamsayı (16 bit)

Bayrak: Fragmentasyon Kontrol bilgisi (3 bit)

Fragment Offset: Datagram parçalarını birleştirme bilgisi (16 bit)

TTL: Paketin yaşam süresi-geçmiş olduğu hopların sayısı (8 bit)

Protokol: Üst-katman protokolünü tanımı (8 bit)

Başlık Sağlaması: IP başlığının doğruluğu (16 bit)

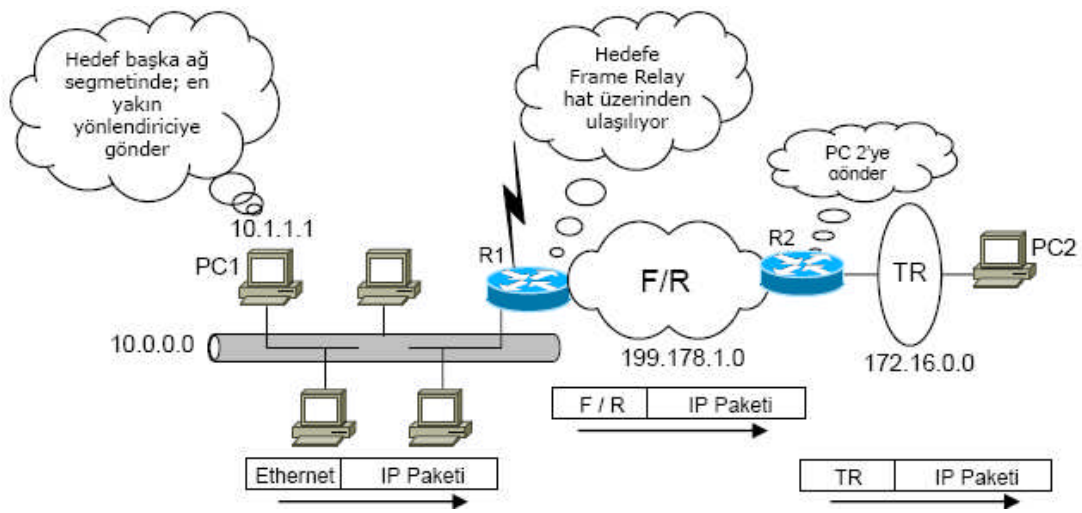
Kaynak ve Hedef Adresleri: Hedef ve Kaynak bilgisayar IP adresi (32+32 bit)

IP Seçenekleri: Güvenlik gibi seçenekler (Değişken Uzunluk)

Data: Maksimum 64 KB Üst katman bilgisi

Padding: IP başlığını 32 bit katlarına ulaştırmak için konulan sıfırlar

Paket yapısında görüldüğü gibi hedef ve kaynak adres, protokol bilgileri gibi verinin yolunu bulmasını sağlayan önemli bilgiler vardır. Yönlendirici de paketteki bu önemli bilgileri okuyarak hedef bilgisayarın mantıksal adresini bilir ve kendinde bulunan mantıksal adres tablosuna bakarak en kısa yolu bulup paketi yönlendirir.



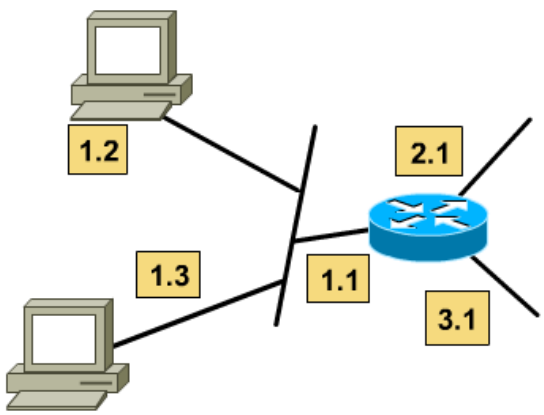
Şekil 1.2: Paket yönlendirmesi

Örneğin Şekil 1.2' de görüldüğü gibi PC 1, PC 2'ye data paketi göndermek istemektedir. PC 1,kendi IP adresi ile hedef bilgisayarın IP adresini karşılaştırır. Eğer hedef başka bir ağda ise en yakın yönlendirici olan R1'e paketi gönderir. Çünkü PC1'de öngörülen

ağ çıkış kapısı olarak R1 konfigüre edilmiştir. R1, bu paketi açar ve hedef bilgisayarın IP adresine bakar. Kendi yönlendirme tablosunu inceleyerek en kısa yolu bulur. Alırken paket üzerinde bulunan Ethernet Data-Link katmanı başlığını çıkartarak Frame Relay başlığı takar ve paketi R2'ye gönderir. R2 aldığı paketin gitmesi gereken adresin kendisine direkt bağlı olan ağ segmenti olduğunu anlayınca, bu segmentin bağlı olduğu arayüzden gönderir. Fakat bu ağ segmenti Token-Ring teknolojisi kullandığı için Token-Ring başlığı takarak paketi gönderir. Böylece PC1 ile PC2 arasındaki data alışverişi tamamlanmış olur.

Yönlendirici paketleri iki temel fonksiyon kullanarak bir data hattından diğer data hattına yani hedefe iletir. Bu fonksiyonlar "**Yol Belirleme"** ve "**Anahtarlama"dır**. Yönlendiriciler yol belirleme ve anahtarlama işlemini yapmak için adresler kullanılır. Bu adreslerin bir network (ağ) bir de host (uç) kısmı vardır. Yönlendiriciler yol belirlerken adresin network kısmını kullanarak, paketi hattın diğer ucundaki yönlendiriciye aktarır.

Network	Host
1	1 2 3
2	1
3	1



Şekil 1.3: Network ve Host tanımı

- **Ağ (Network):** Bir grup bilgisayarı temsil eden ve o grupta bulunan bütün bilgisayarlarda aynı olan bölümdür.

- **Uç (Host):** Ağdaki uç bilgisayarı temsil eden ve o ağda tek olan tekrar etmeyen bölümdür.

Anahtarlama fonksiyonu yönlendiricinin 1 portundan gelen paketi, diğer portuna aktarma işlemdir.

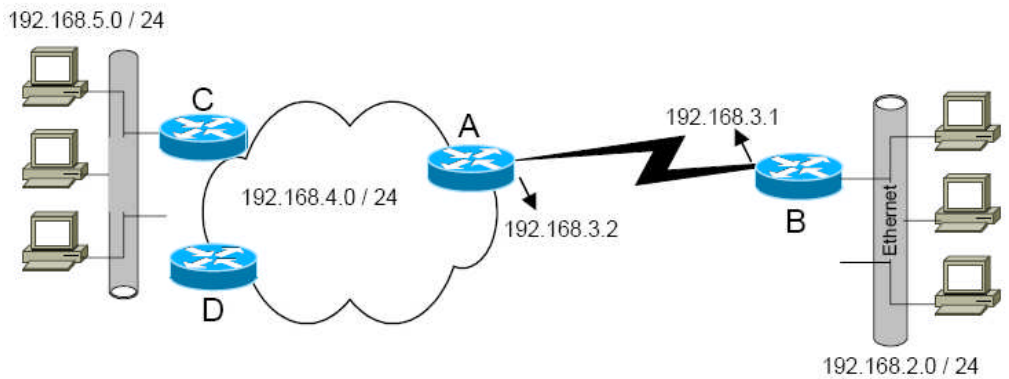
Yol belirleme fonksiyonu da paketin aktarılacağı muhtemel portlar içerisinden en uygununu belirleme işidir.

1.2. Yönlendirme Yolunu İnceleme

Yönlendiricilerin temel işlevi yönlendirme yapmaktır. Kendilerine ulaşan paketleri yönlendiricinin hangi arayüzünden çıkaracaklarını nasıl biliyorlar? Bunun için sabit (statik), değişken (dinamik) veya varsayılan (default) yönlendirmeyi kullanır.

Statik yönlendirmeler sistem yöneticisi tarafından elle girilir ve hedef ağ ile bu paketi hedefine taşıyacak bir sonraki router'ın adresi bilinmelidir. Statik yönlendirme tanımlamak için router'da global konfigürasyon modunda iken "ip route" komutunu kullanmalıyız.

Şekil 1.3'teki ağ küçük olduğu için statik olarak konfigüre edilebilir. A ve B yönlendiricilerde yapılması gereken yapılandırmayı inceleyelim.



Şekil 1.4: Statik yönlendirme

A Yönlendiricisinde,

```
RouterA(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
RouterA(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.2
RouterA(config)#exit
```

B Yönlendiricisinde,

```
RouterB(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
RouterB(config)#ip route 192.168.5.0 255.255.255.0 192.168.3.2
RouterB(config)#exit
```

Ayrıca yönlendiricilerin üzerinde sabit olarak tanımlanan default(varsayılan) yönlendirmeler ise hedef adresi bilinmeyen paketlerin hangi arayüzden çıkarılacağını belirler. Default yönlendirmeyi aşağıdaki örnekte inceleyelim;

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 10.3.10.1
```

Burada yönlendiriciye hedef adresi belli olmayan paketleri 10.3.10.1 adresine sahip arayüzünden çıkarmasını söylüyoruz.

Default yönlendirmenin yönlendiricilerde çalışabilmesi için “ip classless” komutunun girilmesi gerekir. Ayrıca sabit bir kaydı yönlendirme tablosundan silmek için “no ip route” komutunu parametreleriyle birlikte kullanmanız gerekir.

Büyük ağlarda yönetim daha zor olduğu için ağdaki trafik yönlendirmenin daha sağlıklı ve etkin bir biçimde gerçekleşmesi gerekmektedir; bu yüzden de dinamik yönlendirme kullanılır. Dinamik yönlendirme protokolleri, yönlendiricilerin yönlendirme tablolarını oluşturması için gerekli bilgileri birbirlerine mesajla bildirmelerini sağlayacak, bir ağa ulaşım için farklı alternatifler oluşturarak rotaları yedekleyecek, gerektiğinde yük dağılımı yapabilmek için birden fazla rota belirleyebilecek ve ağdaki trafiğin sağlıklı ve etkin bir biçimde akmasını sağlayacak daha birçok özellikleri algoritmalarında içeren yapıya sahiptir.

Dinamik yönlendirmenin iki temel fonksiyonu vardır. Birincisi yönlendirme tablosunu oluşturmak, ikincisi ise oluşturulan bu yönlendirme tablolarının yönlendiriciler arasında paylaşılması yani yönlendiricilerin yönlendirme tablolarındaki güncellemeleri diğer yönlendiricilere haber vermesidir. Dinamik yönlendirme protokolleri hedef ağa ulaşan en iyi yolu belirlemek için metrik değerlerini kullanır. Bir kısım protokol metrik değerini hesaplarken hedef ağa ulaşma sırasında atladığı router sayısını metrik değerine eşit tutar. Bu tür protokoller Uzaklık Vektor protokoller olarak adlandırılır(Distance Vector).Bu protokollere örnek olarak RIP ve IGRP verilebilir.

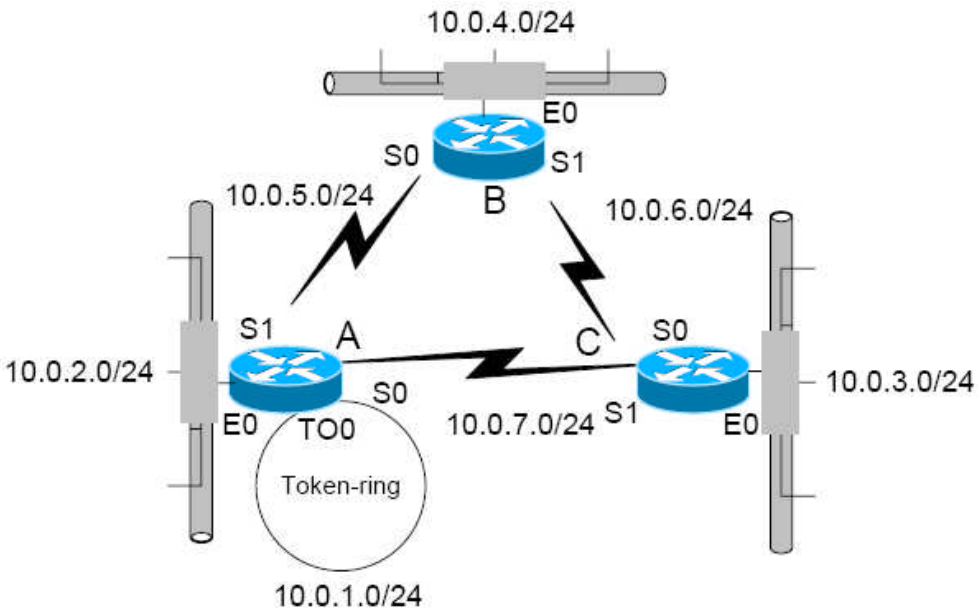
RIP protokolü çalıştıran yönlendiriciler, belli zaman aralıklarıyla yönlendirme tablolarındaki bütün ağ bilgilerini komşuluğunda bulunan bütün yönlendiricilere broadcast yapar. Küçük ağlar için etkili bir biçimde çalışan RIP protokolü bantgenişliğinde ciddi bir trafik oluşturduğundan dolayı büyük ağlar için tercih edilmemektedir. IGRP, küçük ağlarda kullanılabildiği gibi orta ölçekli ağlarda da kullanılabilmektedir. RIP, metrik fonksiyonu olarak bir ağa ulaşabilmek için üzerinden geçilmesi gereken yönlendirici sayısını(hop count) kullanmaktadır. IGRP ise bant genişliği (bandwidth), gecikme (delay), güvenirlik (reliability), yük (load) ve maksimum transmisyon (MTU) biriminden oluşan fonksiyonu metrik olarak kullanılır. IGRP protokolünün metrik fonksiyonunun bantgenişliği, yük ve gecikme gibi ağdaki trafik ile ilgili parametrelerden oluşması RIP’e göre daha etkin rota tespit etmesini sağlamaktadır.

Router rip veya router igrp (proses no) global konfigürasyon komutları ile yönlendiricide RIP ve IGRP protokolleri aktif hale getirilmektedir. RIP ve IGRP protokollerinin konfigürasyonundaki en önemli komut network <ağ numarası> komutudur. Bu komut sayesinde şu fonksiyonlar gerçekleşmektedir:

- Yönlendirme güncellemeleri RIPv1 ise broadcast, RIPv2 ise multicast ile network komutunda belirtilen ağa ait olan arayüzlerden gönderilir.

- Network komutunda belirtilen ağa ait olan arayüzlerden alınan güncellemeler işlenerek yönlendirme tablosuna kaydedilir.

- Yönlendiricinin doğrudan bağlı olduğu alt ağ, network komutunda belirtilen ağa ait ise bu ağ bilgisi komşusu olan diğer yönlendiricilere gönderilir.



Şekil 1.5: Örnek ağ şeması

Şekil 1.5'teki ağ problemsiz çalışıyorken yönlendiricilerdeki yönlendirme tabloları Tablo 1.1, 1.2, 1.3, 1.4, 1.5, 1.6'daki gibi olmaktadır.

Yönlendirme Tabloları

A Yönlendiricisi

Ağ	Arayüz	Metrik
10.0.1.0	TO0	0
10.0.2.0	E0	0
10.0.7.0	S0	0
10.0.5.0	S1	0
10.0.4.0	S1	1
10.0.3.0	S0	1
10.0.6.0	S0	2

B Yönlendiricisi

Ağ	Arayüz	Metrik
10.0.6.0	S1	0
10.0.4.0	E0	0
10.0.5.0	S0	0
10.0.1.0	S0	1
10.0.2.0	S0	1
10.0.3.0	S1	1
10.0.7.0	S1	2

C Yönlendiricisi

Ağ	Arayüz	Metrik
10.0.6.0	S0	0
10.0.3.0	E0	0
10.0.7.0	S1	0
10.0.4.0	S0	1
10.0.2.0	S1	1
10.0.1.0	S1	1
10.0.5.0	S1	2

Tablo1.1: Yönlendirme tabloları

10.0.4.0/24 ağının çalışmadığını varsayalım. Yönlendiriciler belli periyotlarda yönlendirme bilgilerini güncellemektedirler. Güncelleme periyotlarındaki farklılıklardan dolayı ağda döngüler oluşabilecektir. Aşağıdaki tablolar bu döngülerin oluşumunu belirtmektedir. Tablo 1.2, 10.0.4.0/24 ağının çalışmamaya başladıktan hemen sonraki yönlendirme tablosunu göstermektedir.

Yönlendirme Tabloları-1

A Yönlendiricisi			B Yönlendiricisi			C Yönlendiricisi		
Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik
10.0.1.0	TO0	0	10.0.6.0	S1	0	10.0.6.0	S0	0
10.0.2.0	E0	0	10.0.4.0	E0	16	10.0.3.0	E0	0
10.0.7.0	S0	0	10.0.5.0	S0	0	10.0.7.0	S1	0
10.0.5.0	S1	0	10.0.1.0	S0	1	10.0.4.0	S0	1
10.0.4.0	S1	1	10.0.2.0	S0	1	10.0.2.0	S1	1
10.0.3.0	S0	1	10.0.3.0	S1	1	10.0.1.0	S1	1
10.0.6.0	S0	2	10.0.7.0	S1	2	10.0.5.0	S1	2

Tablo1.2

B yönlendiricisi, yönlendirme bilgilerini diğer yönlendiricilere (A ve C) gönderir. A yönlendiricisi de aynı anda 10.0.4.0/24 ağına ait kendi yönlendirme tablosundaki bilgiyi C'ye gönderdiğini varsayalım. B'ye gönderemez çünkü bu ağa ait bilgi, B yönlendiricisinin doğrudan bağlı olduğu arayüzden gelmiştir. C yönlendiricisi, B ve A yönlendiricilerinden aldığı 10.0.4.0/24 ağına ait metrikleri karşılaştıracak ve A yönlendiricisinden aldığı metrik daha küçük olduğu için yönlendirme tablosuna koyacaktır.

Yönlendirme Tabloları-2

A Yönlendiricisi			B Yönlendiricisi			C Yönlendiricisi		
Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik
10.0.1.0	TO0	0	10.0.6.0	S1	0	10.0.6.0	S0	0
10.0.2.0	E0	0	10.0.4.0	E0	16	10.0.3.0	E0	0
10.0.7.0	S0	0	10.0.5.0	S0	0	10.0.7.0	S1	0
10.0.5.0	S1	0	10.0.1.0	S0	1	10.0.4.0	S1	2
10.0.4.0	S1	1	10.0.2.0	S0	1	10.0.2.0	S1	1
10.0.3.0	S0	1	10.0.3.0	S1	1	10.0.1.0	S1	1
10.0.6.0	S0	2	10.0.7.0	S1	2	10.0.5.0	S1	2

Tablo1.3

Bir sonraki güncellemede C yönlendiricisi 10.0.4.0/24 ağına ait bilgiyi A'dan aldığı için B yönlendiricisine gönderecektir. A yönlendiricisi de daha önceden B'den 10.0.4.0/24 ağına ait bilgi aldığı için metriğini sonsuz (yani 16) yaparak değiştirmiştir.

Yönlendirme Tabloları-3

A Yönlendiricisi			B Yönlendiricisi			C Yönlendiricisi		
Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik
10.0.1.0	TO0	0	10.0.6.0	S1	0	10.0.6.0	S0	0
10.0.2.0	E0	0	10.0.4.0	S1	3	10.0.3.0	E0	0
10.0.7.0	S0	0	10.0.5.0	S0	0	10.0.7.0	S1	0
10.0.5.0	S1	0	10.0.1.0	S0	1	10.0.4.0	S1	2
10.0.4.0	S1	16	10.0.2.0	S0	1	10.0.2.0	S1	1
10.0.3.0	S0	1	10.0.3.0	S1	1	10.0.1.0	S1	1
10.0.6.0	S0	2	10.0.7.0	S1	2	10.0.5.0	S1	2

Tablo1.4

B yönlendiricisi, C'den aldığı yeni metrikle yönlendirme tablosunu değiştirdikten sonra bu bilgiyi A'ya aktarır. A yönlendiricisi de 10.0.4.0/24 ağının metriğini değiştirerek bu bilgiyi C'ye aktarır. Böylece ağda döngü oluşmuş ve 10.0.4.0/24 ağına ait metrik bütün yönlendiricilerde sonsuza doğru artmaktadır.

Yönlendirme Tabloları-3								
A Yönlendiricisi			B Yönlendiricisi			C Yönlendiricisi		
Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik
10.0.1.0	TO0	0	10.0.6.0	S1	0	10.0.6.0	S0	0
10.0.2.0	E0	0	10.0.4.0	S1	3	10.0.3.0	E0	0
10.0.7.0	S0	0	10.0.5.0	S0	0	10.0.7.0	S1	0
10.0.5.0	S1	0	10.0.1.0	S0	1	10.0.4.0	S1	2
10.0.4.0	S1	4	10.0.2.0	S0	1	10.0.2.0	S1	1
10.0.3.0	S0	1	10.0.3.0	S1	1	10.0.1.0	S1	1
10.0.6.0	S0	2	10.0.7.0	S1	2	10.0.5.0	S1	2

Tablo1.5

Yönlendirme Tabloları-3								
A Yönlendiricisi			B Yönlendiricisi			C Yönlendiricisi		
Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik	Ağ	Arayüz	Metrik
10.1.1.0	TO0	0	10.1.6.0	S1	0	10.1.6.0	S0	0
10.1.2.0	E0	0	10.1.4.0	S1	6	10.1.3.0	E0	0
10.1.7.0	S0	0	10.1.5.0	S0	0	10.1.7.0	S1	0
10.1.5.0	S1	0	10.1.1.0	S0	1	10.1.4.0	S1	5
10.1.4.0	S1	4	10.1.2.0	S0	1	10.1.2.0	S1	1
10.1.3.0	S0	1	10.1.3.0	S1	1	10.1.1.0	S1	1
10.1.6.0	S0	2	10.1.7.0	S1	2	10.1.5.0	S1	2

Tablo1.6

Oluşan bu döngüyü önlemek için "holddown timer" mekanizması kullanılmaktadır. Örnekte C yönlendiricisi, 10.0.4.0/24 ağına B yönlendiricisi üzerinden S0 arayüzünden ulaşmaktadır. A yönlendiricisi, daha sonra metrik değeri 2 olan 10.0.4.0/24 ağına ait rotayı C'ye göndermesine rağmen rota değiştirilmeyecektir. C yönlendiricisi eski rotayı "holddown timer" süresince koruyacaktır. ("holddown timer" süresi, en az bir kaç güncelleme periyot süresi kadardır.) C yönlendiricisi, B yönlendiricisinden 10.0.4.0/24 ağının çalışmadığını öğrenecek ve yönlendirme tablosunda bu ağa ait olan metriği sonsuz yapacaktır. A yönlendiricisi de aynı şekilde B'den bu bilgiyi alacaktır. Ağdaki bütün yönlendiriciler 10.0.4.0/24 ağına ulaşılamaz olduğunu öğrenmişlerdir. Dolayısıyla ağda döngünün oluşması büyük ölçüde engellenmiştir.

Şekil 1.4' deki örnekte C yönlendiricisinde RIP protokolünü konfigüre edelim.

```
RouterA#configure terminal
RouterA(config)#int E0
RouterA(config-if)#ip address 10.0.2.1 255.255.255.0
RouterA(config-if)#int TO0
RouterA(config-if)#ip address 10.0.1.1 255.255.255.0
RouterA(config-if)#int S0
RouterA(config-if)#ip address 10.0.7.1 255.255.255.0
RouterA(config-if)#int S1
```

```
RouterA(config-if)#ip address 10.0.5.1 255.255.255.0
RouterA(config-if)#exit
RouterA(config)#router rip
RouterA(config-router)#network 10.0.2.0
RouterA(config-router)#network 10.0.5.0
RouterA(config-router)#network 10.0.7.0
RouterA(config-router)#network 10.0.1.0
```

Konfigürasyonda görüldüğü üzere ilk önce RIP protokolü router rip komutuyla aktif edilmiştir. Network komutundan sonra kullanılan ağ numarası A, B ve C sınıfı IP ağ adreslerinden biri olmak zorundadır. Bu komuttan sonra yazılan ağ bilgisi alt ağ veya IP adresi kesinlikle olmayacaktır. Bu komutla elde edilen fonksiyonlar daha önce belirtilmişti. Bu fonksiyonları sırasıyla incelersek;

- Network komutuyla belirtilen 10.0.0.0, 10.0.5.0 ve 10.0.7.0 ağlara ait olan A yönlendiricisinin arayüzlerinde RIP protokolü çalışacaktır. Yani A'nın E0, S0 ve S1 arayüzlerinden ağ bilgileri RIP mesajları ile komşu yönlendiricilere broadcast veya multicast ile gönderilecektir.

- Ayrıca bu arayüzlerden B ve C yönlendiricilerinden alınan RIP mesajları da işlenerek yönlendirme tablosuna kaydedilecektir. Eğer alınan mesajlar RIPv1 ise alt ağ maskeleri olmadığı için yönlendirici alındığı arayüzün alt ağ maskesini uygular ve yönlendirme tablosuna kaydeder. Bu mesajlar RIPv2 ise zaten alt ağ maskeleri beraber alındığı için bu alt ağ maskesi kullanılır.

- A'nın E0, S0 ve S1 arayüzleri network komutuyla belirtilen ağlara ait alt ağlarda oldukları için bu alt ağ bilgileri arayüzlerden diğer yönlendiricilere aktarılır. Fakat A yönlendiricisi 10.0.7.0 ağını C'ye, 10.0.5.0 ağını B'ye ortak alt ağları olduğundan göndermeyecektir.

Şekil 1.5' teki örnekte E0 ve TO0 arayüzleri başka yönlendiricilere bağlı olmadıkları için bu arayüzlerde RIP protokolü çalıştırmak gereksizdir. RIP protokolün bu arayüzlerde çalışması yönlendiriciye gereksiz bir işlemci yükü getirmektedir. Bu arayüzlerde RIP protokolünün sadece RIP güncelleme mesajlarını dinlemesini ve RIP mesajlarını göndermesini durdurmak üzere **passive-interface** komutu kullanılmaktadır.

```
RouterC(config)#router rip
RouterA(config-router)#network 10.0.0.0
RouterA(config-router)#network 10.0.5.0
RouterA(config-router)#network 10.0.7.0
RouterA(config-router)#network 10.0.1.0
RouterC(config-router)#passive-interface E0
RouterC(config-router)#passive-interface TO0
```

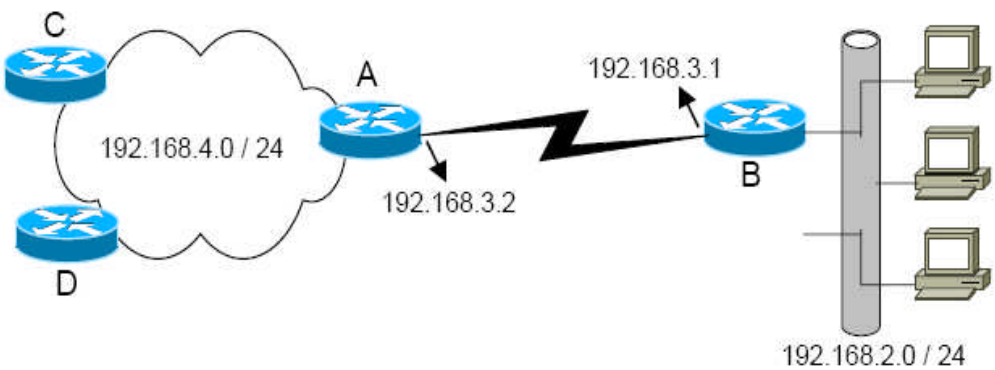
Yönlendiriciler öngörüldüğü şekliyle 4 adet eşit metrik değerine sahip rotayı yönlendirme tablosunda bulundurabilir. Böylece yönlendiriciler, trafiği bu 4 farklı eşit metrikli rotayı kullanarak ve yük dağılımı yaparak yönlendirir. Yönlendirme tablosundaki eşit metrikli rota sayısını **ip maximum-paths (**eşit metrikli rota sayısı**)** komutuyla

değiştirilebilmektedir. RIP protokolünün metrik değerleri üzerinden geçilen yönlendirici sayısı ile belirlendiği için eşit olma olasılığı yüksektir. Fakat IGRP protokolünün metrik değeri bir fonksiyon olduğu için eşit olma olasılığı çok azdır. Yönlendirme tablosunda yük dağılımı yapmak üzere aynı ağa giden birden fazla rotaya ihtiyaç duyulabilmektedir. Bu durumda IGRP rotaların da metrik değerleri birbirine yakın olanları aynı metriğe sahip hale getirmek üzere **variance (**çarpan**)** komutu kullanılmaktadır. Yönlendiriciler bir ağa ait en küçük metrik değerli rotayı aldıktan sonra bu metrik değeri "variance" komutunda belirtilen çarpan ile çarparlar. Çıkan sonuç ile en küçük metrik değer arasındaki bütün metrik değerlerine sahip rotalar bu IGRP yönlendirici için eşit metrikli rotalardır. Yönlendiriciler, **ip maximum-paths** komutuyla belirtilen rota sayısı kadar rotayı yönlendirme tablolarına kaydedebilir; ayrıca yönlendiricilerin eşit metrikli rotalar arasında yük dağılımını nasıl yapacakları **traffic-share (**balanced | min**)** komutuyla belirlenmektedir.

1.3. Ağ Geçidini Belirleme

Birçok ağın birleşmesinden oluşan büyük ağlarda, her bir ağ kendine özgü protokoller ve sistemler kullanmaktadır. Bu ağların birbirleri ile sorunsuz olarak anlaşabilmeleri için geçitler kullanılmaktadır. Geçitler, birbirlerinden tamamıyla farklı ağları birleştirir. Halen pek çok farklı ağ sistemleri kullanılmakta olduğundan geçitlere büyük ihtiyaç duyulmaktadır

Yönlendirici aldığı paketi hedef ağ adresini yönlendirme tablosunda bulamadığı zaman paketi göndermek istediğiniz ağı ip default-network komutu ile belirleyebilirsiniz.



Şekil 1.6: Örnek bir ağ şeması

Şekil1.6'daki örnekte 192.168.4.0 ağında bulunan yönlendiricilerden birine bağlı A, B veya C sınıfı bir ağ adresinin alt ağları bulunduğunu varsayalım. Örneğin 10.0.0.0 ağının alt ağları C yönlendiricisine direkt bağlı olduğunu düşünelim. **ip default-network 10.0.0.0** komutuyla öngörülen rota olarak 10.0.0.0 ağının rotası belirtilmektedir. Yani 10.0.0.0 ağına giden rota ile yönlendirme tablosunda hedef ağın bulunamadığı durumlarda kullanılacak rota aynıdır.

```
RouterA(config)#ip default-network 10.0.0.0
RouterA(config)#exit
RouterA#show ip route
```

```
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is 192.168.3.2 to network 10.0.0.0
C 192.168.5.0 is directly connected, Ethernet0
R 192.168.2.0 [120/1] via 192.168.3.1, 00:00:05, Serial0
C 192.168.4.0 is directly connected, TokenRing0
C 192.168.3.0 is directly connected, Serial0
R* 10.0.0.0/8 [120/1] via 192.168.4.2, 00:00:03, TokenRing0
RouterA#
RouterB#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is 192.168.3.2 to network 0.0.0.0
C 192.168.2.0 is directly connected, Ethernet0
R 192.168.4.0 [120/1] via 192.168.3.2, 00:00:25, Serial0
C 192.168.3.0 is directly connected, Serial0
R 10.0.0.0/8 [120/1] via 192.168.3.2, 00:00:13, Serial0
R* 0.0.0.0/0 [120/1] via 192.168.3.2, 00:00:13, Serial0
RouterB#
```

B yönlendiricisinin yönlendirme tablosunda öngörülen rota olarak 0.0.0.0 ağının gösterilmesi RIP protokolünden dolayıdır. RIP protokolü **ip default-network** komutuyla yazılı olan ağı 0.0.0.0 olarak duyurur. IGRP veya EIGRP kullanılmış olsaydı 10.0.0.0 ağı öngörülen rota olarak duyurulacaktı.

1.4. Yönlendirmeleri Gösterme

KOMUT	AÇIKLAMA
show hosts	Host adlarını ve IP adreslerini listeler.
show interfaces [*tip no*]	Ara yüz istatistiklerini ve IP adreslerini listeler.
show ip interface [*tip no*]	Belirtilen ara yüzün IP adresini ve IP parametrelerini listeler.
show ip interface brief	Bütün ara yüzlerin IP adreslerini kısaca listeler.
show ip route [*subnet*]	Yönlendirme tablosunu listeler.
show ip arp	IP ARP önbelleğini gösterir.
debug ip packet	Her IP paketi bilgilerini tutar.
show ip protocol	Yönlendirme protokol bilgilerini, parametrelerini ve zaman değerlerini görüntüler.
debug ip rip	Komutun uygulandığı sürece alınan ve gönderilen RIP mesajlarının logları görüntülenir.
debug ip igrp transactions	Komutun uygulandığı sürece alınan ve gönderilen IGRP mesajlarının logları görüntülenir.
debug ip igrp events	Komutun uygulandığı sürece alınan ve gönderilen her IGRP paketinin logları görüntülenir.

Tablo 1.7: Yönlendirme komutları

IP yapılandırmasını görüntülemek için Tablo 1.7' deki görülen komutlar kullanılmaktadır.

A Yönlendiricisinde,

```
RouterA(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
RouterA(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.2
RouterA(config)#exit
```

Bu sabit yönlendirmenin yönlendirme tablosunu listelemek için;" show ip route" komutu kullanılır.

```
RouterA#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
```

```
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
162
Gateway of last resort is not set
C 192.168.3.0 is directly connected, Serial0
S 192.168.2.0 [1/0] via 192.168.3.1
S 192.168.5.0 [1/0] via 192.168.4.2
C 192.168.4.0 is directly connected, Serial1
RouterA#
```

B Yönlendiricisinde,

```
RouterB(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
RouterB(config)#ip route 192.168.5.0 255.255.255.0 192.168.3.2
RouterB(config)#exit

RouterB#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
C 192.168.2.0 is directly connected, Ethernet0
S 192.168.4.0 [1/0] via 192.168.3.2
S 192.168.5.0 [1/0] via 192.168.3.2
C 192.168.3.0 is directly connected, Serial0
RouterB#
```

Şekil 1.4’ deki yönlendiricilerin yönlendirme tabloları aşağıdaki gibidir.

```
RouterA#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
10.0.0.0/24 is alt ağted, 7 alt ağs
C 10.0.2.0 is directly connected, Ethernet0
C 10.0.1.0 is directly connected, TokenRing0
C 10.0.5.0 is directly connected, Serial1
```

```
C 10.0.7.0 is directly connected, Serial0
R 10.0.4.0 [120/1] via 10.0.5.2, 00:00:34, Serial1
R 10.0.6.0 [120/1] via 10.0.7.3, 00:00:27, Serial0
[120/1] via 10.0.5.2, 00:00:22, Serial1
R 10.0.3.0 [120/1] via 10.0.7.3, 00:00:27, Serial0
RouterA#

RouterB#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
10.0.0.0/24 is alt ağted, 7 alt ağs
C 10.0.4.0 is directly connected, Ethernet0
C 10.0.5.0 is directly connected, Serial0
C 10.0.6.0 is directly connected, Serial1
R 10.0.1.0 [120/1] via 10.0.5.1, 00:00:36, Serial0
R 10.0.2.0 [120/1] via 10.0.5.1, 00:00:36, Serial0
R 10.0.3.0 [120/1] via 10.0.6.3, 00:00:25, Serial1
R 10.0.7.0 [120/1] via 10.0.6.3, 00:00:25, Serial1
[120/1] via 10.0.5.1, 00:00:23, Serial0
RouterB#

RouterC#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
10.0.0.0/24 is alt ağted, 7 alt ağs
C 10.0.3.0 is directly connected, Ethernet0
C 10.0.6.0 is directly connected, Serial0
C 10.0.7.0 is directly connected, Serial1
R 10.0.1.0 [120/1] via 10.0.7.1, 00:00:32, Serial1
R 10.0.2.0 [120/1] via 10.0.7.1, 00:00:32, Serial1
R 10.0.4.0 [120/1] via 10.0.6.2, 00:00:21, Serial0
R 10.0.5.0 [120/1] via 10.0.6.2, 00:00:21, Serial0
[120/1] via 10.0.7.1, 00:00:25, Serial1
RouterC#
```

Yönlendirme tablolarında da göründüğü gibi 10.0.0.0 ağının bütün alt ağlarının maskesi aynıdır.(255.255.255.0) Dolayısıyla A, B ve C yönlendiricileri bütün alt ağ bilgilerini birbirleriyle paylaşmıştır. Yönlendiricilerin bağlı olduğu alt ağlardan birinin alt ağ

maskesini değiştirdiğinizde bu ağ bilgisi artık yönlendirme mesajları ile gönderilmeyecek ve diğer yönlendiriciler de bu ağa ait bilgiyi yönlendirme tablolarından silecektir. Sadece bu ağa bağlı yönlendiricinin yönlendirme tablosunda bu bilgi bulunacaktır. C yönlendiricisine bağlı10.0.3.0/24 ağının alt ağ maskesini değiştirerek 10.0.3.0/27 ağa dönüştürdüğümüzü düşünelim. C yönlendiricisi hem Serial0 hem de Serial1 portundan bu bilgiyi diğer yönlendiricilere göndermeyecektir. Çünkü bu portların bağlı olduğu alt ağların maskesi /24'tür.Dolayısıyla A ve B yönlendiricilerinde 10.0.3.0 ağına ait kayıt bulunmayacaktır fakat C yönlendiricisinin yönlendirme tablosu şu şekildedir:

```
RouterC#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
10.0.0.0/8 is variably alt ağted, 7 alt ağs, 2 masks
C 10.0.3.0/27 is directly connected, Ethernet0
C 10.0.6.0/24 is directly connected, Serial0
C 10.0.7.0/24 is directly connected, Serial1
R 10.0.1.0/24 [120/1] via 10.0.7.1, 00:00:32, Serial1
R 10.0.2.0/24 [120/1] via 10.0.7.1, 00:00:32, Serial1
R 10.0.4.0/24 [120/1] via 10.0.6.2, 00:00:21, Serial0
R 10.0.5.0/24 [120/1] via 10.0.6.2, 00:00:21, Serial0
[120/1] via 10.0.7.1, 00:00:25, Serial1
RouterC#
```

Show ip route komutu kullanıldığında başındaki açıklayıcı bilgiler, yönlendirme bilgisinin kaynağını belirtmek için kullanılan harf kodlarının ne anlama geldiğini açıklar. Örneğin, C harfi bağlı (connected) yollar, R harfi, RIP, I harfi IGRP için kullanılır. Her A, B ya da C sınıfı ağ ve o ağdaki alt ağ'ler listelenmiştir. O ağ içinde statik bir maske kullanılmış ise, maske yalnızca ağı belirten satırda gösterilmiştir. Ağ, 10.0.0.0 ağı gibi VLSM kullanıyorsa, maske bilgileri bağımsız alt ağları gösteren satırlarda gösterilir.

Her yönlendirme kaydı, alt ağ numarasını ve çıkış arabirimini listeler. Birçok durumda, bir sonraki hop'ta yer alan router'ın IP adresi de listelenir. Çıkış arabiriminin bilinmesi gereklidir; çünkü, router o arabirimden göndereceği paketi enkapsüle etmek için kullanacağı veri bağlantı katmanı başlığını bu bilgiye göre seçecektir. Bir sonraki hop'ta bulunan router'ın IP adresi, router'ın ilgili veri bağlantı adresini bularak yeni oluşturulmuş veri bağlantı başlığı içine yerleştireceği IP adresini bilmesi gereken arabirimlerde kullanılacaktır.

"Show ip route" komutunun çıktısındaki köşeli parantezlerin içindeki sayılar oldukça ilginçtir. Köşeli parantezin içindeki sayılardan ikincisi, yolun metrik değeridir. İlk sayı, yönetimsel uzaklığı (administmtive distance) tanımlar. Yönetimsel uzaklık, yalnızca bir router üzerinde birden fazla yönlendirme protokolü kullanıldığında önemlidir. Bir router'da birden

fazla yönlendirme protokolü kullanıldığında, yönlendirme protokolleri aynı sub-net'lere giden yolları öğrenebilir. Ancak bunların metrik değerleri farklı olacağından, hangi yönlendirme protokolünden öğrenilen yolun daha iyi olduğuna karar vermek mümkün olmayacaktır; bu nedenle, hangi yönlendirme protokolünün öğrendiği yolların daha iyi olduğunu tanımlamak için bir metot kullanılmaktadır. IOS yazılımı, bu kavramı "yönetimsel uzaklık" olarak adlandırılan bir şekilde uygular. Yönetimsel uzaklık, bir tamsayı değeridir ve her yönlendirme bilgisinin kaynağına atanmıştır. Yönetimsel uzaklık değeri daha düşük olan yönlendirme bilgisi kaynağı daha iyi demektir. IGRP'nin varsayılan yönetimsel uzaklığı 100, OSPF'in 110, RIP'in 120 ve EIGRP'nin 90 dır. Köşeli parantezler içindeki 100 değeri, IGRP için kullanılan yönetimsel uzaklık değerinin 100 olduğunu gösterir. Bir başka deyişle, varsayılan değer kullanılmaktadır. Yani, hem RIP hem de IGRP kullanılsaydı ve ikisi de aynı alt ağ'e giden yollar öğrenseydi, bu sub-net'ler için sadece IGRP'nin yönlendirme bilgisi yönlendirme tablosuna eklenecekti. RIP, IGRP'nin bilmediği bir alt ağ öğrenseydi, bu bilgi yönlendirme tablosuna eklenecekti.

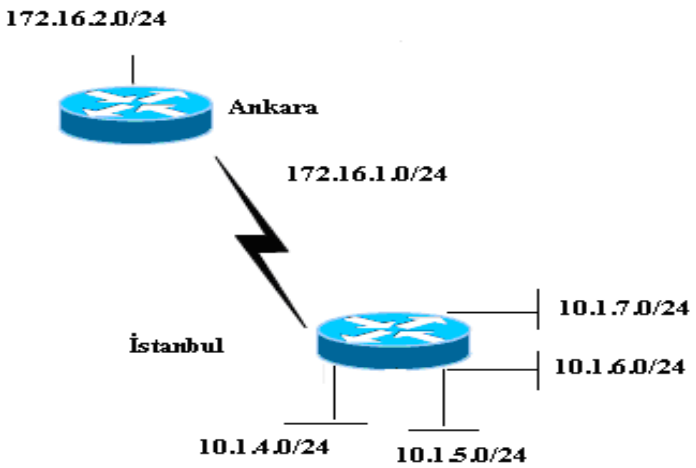
1.5. Otomatik Özetleme ve Yolların Bir Araya Getirilmesi

IOS yazılımı, yönlendirme işlemini mümkün olduğunca hızlı bir şekilde yapmak üzere optimize edilmiştir. Yönlendiricilerin kısa tarihinde, 3 katman yönlendirme performansındaki iyileştirmelerin birçoğu, algoritmalar sayesinde gerçekleştirilmiştir. Birçok seferde de bu algoritmalar donanım üzerinde uygulanmıştır. Yine de herhangi bir algoritmanın, daha kısa bir listeyi daha hızlı bir biçimde araştırabileceğini söylemek yanlış olmayacaktır. Otomatik özetleme ve yolların bir araya getirilmesi, IOS yazılımının IP yönlendirme tablosunun boyutunu küçülten ve bu sayede paketler için gecikme süresini azaltan iki özelliktir. Otomatik özetleme, aşağıdaki kural göre çalışan bir yönlendirme protokolüdür.

IP adresi X ağı içinde yer almayan bir arabirim üzerinden duyurulduklarında, A ağındaki alt ağ'ler hakkındaki yol bilgileri özetlenir ve tek bir yol bilgisi olarak duyurulur. Bu yol bilgisine A, B ya da C sınıfındaki X ağının tümü için varılır.

RIP ve IGRP, otomatik özetlemeyi gerçekleştirir ve bu özelliğin kapatılmasına izin vermezler. Aslında bu, maskeyi ileten yönlendirme protokollerinin bir yan etkisi olmalıdır. RIP-2 ve EIGRP'de otomatik özetleme etkin hale getirilebilir ya da kapatılabilir.

Bir örnek vererek konuyu açıklayalım. Şekil 1.6 10.0.0.0 ve 172.16.0.0 ağlarını göstermektedir. İstanbul, 10.0.0.0 ağının alt ağ'larına bağlı dört yola sahiptir. Aşağıda, Ankara router'ı üzerinde çalıştırılan **show ip route** ve **debug ip rip** komutlarının çıktısını gösterilmektedir.

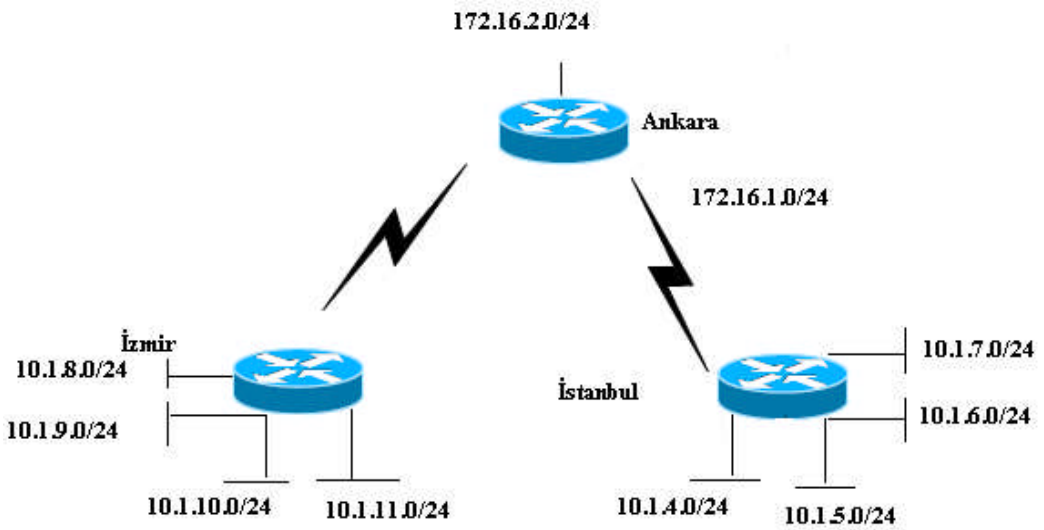


Şekil 1.7: Otomatik özetleme

```
Ankara#debug ip rip
02:20:42: RIP: sending v2 update to 224.0.0.9 via Serial0.2
(172.16.1.251)
02:20:42:              172.16.2.0/24 -> 0.0.0.0, metrik 1, tag 0
02:20:42: RIP: sending v2 update to 224.0.0.9 via EthernetO
(172.16.2.251)
02:20:42:              172.16.1.0/24 -> 0.0.0.0, metrik 1, tag 0
02:20:42:              10.0.0.0/8 -> 0.0.0.0, metrik 2, tag 0
02:20:46: RIP: received v2 update from 172.16.1.253 on Serial0.2
02:20:46:              10.0.0.0/8 -> 0.0.0.0 in 1 hops
Ankara#undebug all
All possible debugging has been turned off

Ankara#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF external
type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll - IS-IS
level-1, L2 - IS-IS level-2, ia - ISIS inter area * - candidate
default, U - per-user static route, o - ODR P - periodic downloaded
static route
Gateway of last resort is not set
172.16.0.0/24 is alt ağted, 2 subuets
C                172.16.1.0 is directly connected, Serial0.2
C                172.16.2.0 is directly connected, EthernetO
R                10.0.0.0/8 fl20/n via 172.16.1.253, 00:00:09,
Serial0.2
```

Yukarıda vurgulandığı gibi, Ankara yönlendiricisi Seri 0.2 arabirimi vasıtasıyla İstanbul yönlendiricisinden gelen bir duyuru alınmıştır. Bu güncelleme, sadece A sınıfı 10.0.0.0/8 ağının tamamını duyurmaktadır. Çünkü İstanbul yönlendiricisi üzerinde otomatik özetleme (varsayılan olarak) etkin durumdadır. IP yönlendirme tablosu 10.0.0.0 ağı için tek

bir yol bilgisini listelemektedir. Şimdi de Şekil1.6'daki ağı ele alalım. Bu ağda, İzmir yönlendiricisi 10.0.0.0 ağının alt ağ'lerine bağlantıları vardır ancak bu alt ağ'ler ile ilgili yol bilgilerini İstanbul'a iletmek için Ankara yönlendiricisini kullanmak zorundadır.



Şekil 1.8

İstanbul yönlendiricisi özetleme yapmadığında Ankara yönlendiricisinin yönlendirme tablosu:

```
Ankara#debug ip rip
RIP protocol debugging is on
Ankara#
02:48:58: RIP: received v2 update from 172.16.1.253 on Serial0.2
02:48:58:              10.1.7.0/24 -> 0.0.0.0 in 1 hops
02:48:58:              10.1.6.0/24 -> 0.0.0.0 in 1 hops
02:48:58:              10.1.5.0/24 -> 0.0.0.0 in 1 hops
02:48:58:              10.1.4.0/24 -> 0.0.0.0 in 1 hops
02:49:14: RIP: received v2 update from 172.16.3.252 on SerialO.l
02:49:14:              10.1.11.0/24 -> 0.0.0.0 in 1 hops
02:49:14:              10.1.10.0/24 -> 0.0.0.0 in 1 hops
02:49:14:              10.1.9.0/24 -> 0.0.0.0 in 1 hops
02:49:14:              10.1.8.0/24 -> 0.0.0.0 in 1 hops
02:49:16: RIP: sending v2 update to 224.0.0.9 via SerialO.l
(172.16.3.251)
02:49:16:              172.16.1.0/24 -> 0.0.0.0, metrik 1, tag 0
02:49:16:              172.16.2.0/24 -> 0.0.0.0, metrik 1, tag 0
02:49:16:              10.0.0.0/8 -> 0.0.0.0, metrik 2, tag 0
02:49:16: RIP: sending v2 update to 224.0.0.9 via Serial0.2
(172.16.1.251)
02:49:16:              172.16.2.0/24 -> 0.0.0.0, metrik 1, tag 0
02:49:16:              172.16.3.0/24 -> 0.0.0.0, metrik 1, tag 0
```

```
02:49:16:             10.0.0,0/8 -> 0.0.0.0, metrik 2, tag 0
02:49:16: RIP: sending v2 update to 224.0.0.9 via Ethernet 0
(172.16.2.251)
02:49:16:             172.16.1.0/24 -> 0.0.0.0, metrik 1, tag 0
02:49:16:             172.16.3.0/24 -> 0.0.0.0, metrik 1, tag 0
02:49:16:             10.0.0.0/8 -> 0.0.0.0, metrik 2, tag 0
Ankara#no debug all
All possible debugging has been turned off
Ankara#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D
- EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP i - ISIS, Ll -
ISIS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic
downloaded static route
Gateway of last resort is not set
172.16.0.0/24 is alt ağted, 3 alt ağs
C                172.16.1.0 is directly connected, Serial0.2
C                172.16.2.0 is directly connected, EthernetO
C                172.16.3.0 is directly connected, SerialO.l
10.0.0.0/24 is alt ağted, 8 alt ağs
R           10.1.11.0 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
R           10.1.10.0 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
R           10.1.9.0 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
R           10.1.8.0 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
R           10.1.7.0 [120/1] via 172.16.1.253, 00:00:03, Serial0.2
R           10.1.6.0 [120/1] via 172.16.1.253, 00:00:03, Serial0.2
R           10.1.5.0 [120/1] via 172.16.1.253, 00:00:03, Serial0.2
R           10.1.4.0 [120/1] via 172.16.1.253, 00:00:03, Serial0.2
Ankara#
```

Yukarıda vurgulandığı gibi, yol güncellemeleri bağımsız **alt ağları** içermektedir. Bu nedenle, Ankara 10 ile başlayan ağın tüm alt ağlarına giden yolları görebilmekte ve paketleri istanbul ve İzmir'e iletebilmektedir. Otomatik özetleme kullanılsaydı, Ankara, İstanbul ve İzmir'in 10.0.0.0 ağına eşit metriğe sahip yollardan ulaşacağını düşünecek ve bu nedenle bazı paketler yanlış iletilecekti.

Yol özetleme (yolların bir araya getirilmesi olarak da adlandırılır), otomatik özetleme gibi çalışır ancak, özetlemenin A, B ya da C sınıfı olarak yapılmasına gerek yoktur. Şekil 1.8' de gösterilen ağı inceleyiniz. Ankara, 10.0.0.0 ağının 8 alt ağı ile ilgili yol bilgilerine sahiptir. Bu yollardan dördü İstanbul yönlendiricisinden öğrenilmiştir. Tablo 1.8'de bu alt ağlardaki atanabilir adresler, broadcast ve alt ağ adresleri gösterilmiştir.

Alt ağ	Broadcast	Maske	Atanabilir Adresler
10.1.4.0	255.255.255.0	10.1.4.255	10.1.4.1 ile 10.1.4.254
10.1.5.0	255.255.255.0	10.1.5.255	10.1.5.1 ile 10.1.5.254
10.1.6.0	255.255.255.0	10.1.6.255	10.1.6.1 ile 10.1.6.254
10.1.7.0	255.255.255.0	10.1.7.255	10.1.7.1 ile 10.1.7.254

Tablo 1.8: Yolların bir araya toplanılması

Şimdi, 255.255.252.0 maskesine sahip 10.1.4.0 alt ağ'ini ele alalım. Bu örnekte, 10.1.4.0/22 (aynı alt ağ farklı bir gösterim kullanılarak yazılmıştır), 10.1.4.1 ile 10.1.7.254 arasında atanabilir adreslere ve 10.1.7.255 broadcast adresine sahiptir. 10.1.4.0/22, orijinal dört alt ağ'teki atanabilir tüm adresleri içerdiğinden, 10.1.4.0/22'ye giden yolun bilinmesi, dört alt ağ için dört yol bilgisinin bilinmesinden daha iyidir. Burada, bir sonraki hop'ta bulunan router'ın dört yol içinde aynı olduğu varsayılmıştır. Yol toplama, yönlendirme protokolüne, bağımsız birçok küçük alt ağ yerine, daha büyük tek bir alt ağ için yol bilgisi duyurmasını söyleyen bir araçtır. Bu örnekte, yönlendirme protokolü, dört bağımsız alt ağ yerine 10.1.4.0/22'yi duyurmaktadır. Ankaranın yönlendirme tablosu bu sayede daha kısa olacaktır. Yolları bir araya toplamayı destekleyen iç IP yönlendirme protokolleri EIGRP ve OSPF protokolleridir. Şekil 1.6'daki ağ kullanılmaya devam etmektedir. Ancak tüm router'lar IGRP'ye terfi ettirilmişlerdir. Aşağıda, Ankara ve İstanbul üzerindeki EIGRP konfigürasyonları ve sonuçta Ankara üzerinde oluşturulan yönlendirme tablosu görülmektedir.

Örnek:
İstanbul Üzerinde:

```
router eigrp 9
Network 10.0.0.0
Network 172.16.0.0
No auto-summary
!
interface serial 0.1 point-to-point
ip address 172.16.1.253 255.255.255.0
frame-relay interface-dlci 901
ip summary-address eigrp 9 10.1.4.0 255.255.252.0
```

Ankara Üzerinde:

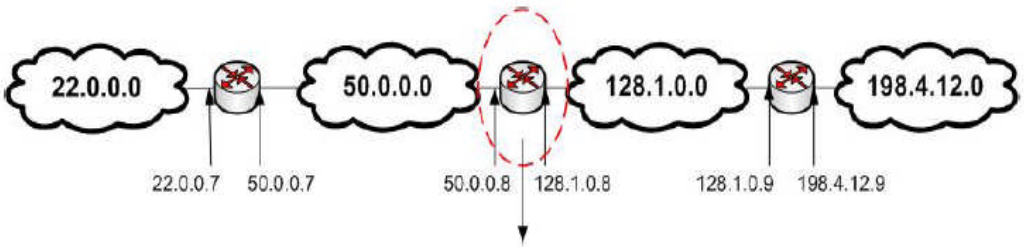
```
router eigrp 9
network 172.16.0.0
no auto-summary
Ankara#show ip route
Codcs:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF external
type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll - IS-IS
level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate
```

```
default, U - per-user static route, o - ODR P - periodic downloaded
static route
Gateway of last resort is not set
172.16.0.0/24 is alt ağted, 3 alt ağs
C                172.16.1.0 is directly connected, Serial0.2
C                172.16.2.0 is directly connected, EthenetO
C                172.16.3.0 is directly connected, SerialO.l
10.0.0.0/8 is variably alt ağted, 5 alt ağs, 2 masks
D     10.1.11.0/24 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
D     10.1.10.0/24 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
D     10.1.9.0/24 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
D     10.1.8.0/24 [120/1] via 172.16.3.252, 00:00:15, SerialO.l
D     10.1.4.0/22 [90/2185984] via 172.16.1.253, 00:00:58, Serial0.2
```

İstanbul'un Seri 0.1 arabirimi üzerinde kullanılan ip summary-address komutu, duyurulacak alt ağların bir supernet'ini tanımlamaktadır. Ankara'nın yönlendirme tablosundaki yol bilgisinin, dört ayrı alt ağ yerine 10.1.4.0/22'yi gösterdiğine dikkat ediniz. Özetleme yapılırken, orijinal alt ağ'lerin superset'i A, B ya da C sınıfı ağdan küçük olabilir, büyük olabilir ya da tam olarak ağ ile eşit olabilir. Örneğin, 192.168.4.0,192.168.5.0, 192.168.6.0 ve 192.168.7.0, dört ardışık C sınıfı ağı temsil eden 192.168.4.0/22 ile özetlenebilir. Özetlenen grup, ağların kümesi olduğunda özetlemeye, *supernetting* dendiği de olur.

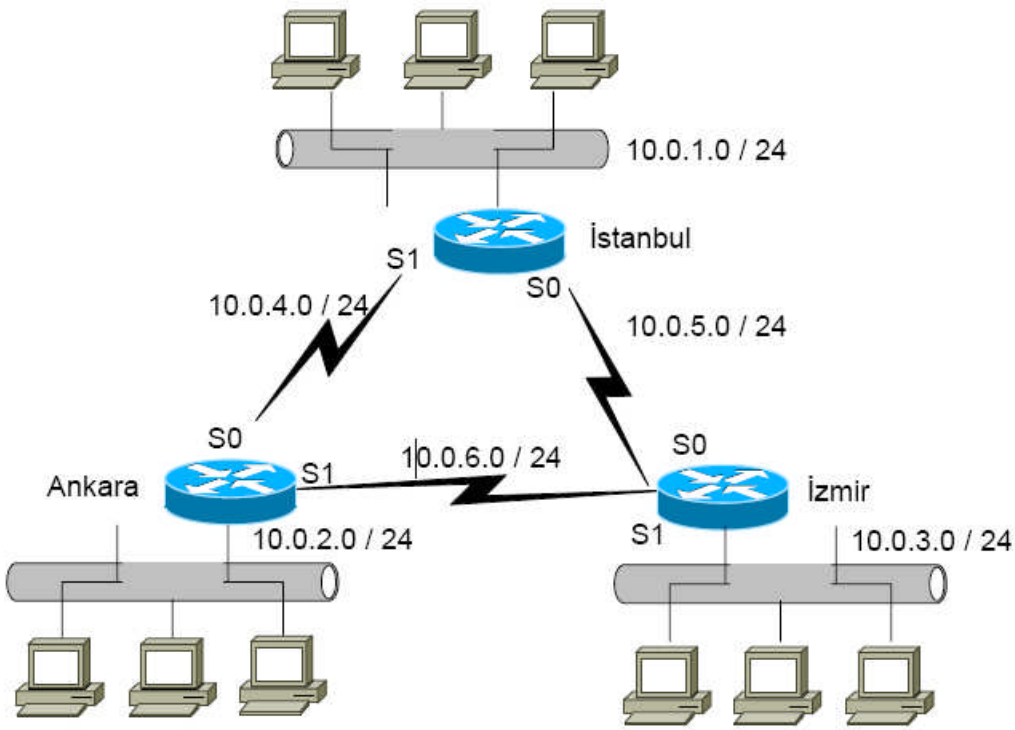
Örnek 1: IP Datagramlarının Yönlendirilmesi

IP datagramları yönlendirilirken sekmede yönlendirme (hop-by-hop routing) tekniği kullanılır. Bir yönlendirici aldığı datagramların varış adreslerine bakar, kendi yönlendirme tablolarındaki maskeleri kullanarak (mantıksal VE işlemi ile) varılmak istenen ağ adresine en çok benzeyen tablo adresini bulur ve paketin aktarılacağı port bilgisine erişir. Paket yönlendiricinin bağlı bulunduğu ağlardan biri üzerindeki düğüme gönderilmişse, doğrudan o düğüme gönderilir. Aksi halde gitmesi gereken yöndeki porttan bir sonraki yönlendiriciye ulaşması için aktarılır. Aşağıdaki şekilde verilen ağda ortadaki yönlendiricinin yönlendirme tablosu gösterilmiştir. 128.1.0.0 adresli ağdaki düğümlerden biri (diyelim ki 128.1.0.7 IP adresine sahip olan), 22.0.0.0 adresli ağdaki düğümlerden birine (diyelim ki 22.0.0.50'ye) bir paket göndersin. Bu paket ortadaki yönlendiriciye ulaşınca tablodan 22.0.0.0 adresli ağa ulaşmak için *Port_sol* üzerinden aktarılır ve soldaki yönlendirici tarafından alınır. Soldaki yönlendirici paketi aldıktan sonra tablosunu kontrol eder ve 22.0.0.0 nolu ağa bağlı olduğu için paketi doğrudan ilgili düğüme iletir.



Varış adresi	Maske	Port	*Bir sonraki düğüm*
22.0.0.0	255.0.0.0	Port_sol	*50.0.0.7*
50.0.0.0	255.0.0.0	Port_sol	*doğrudan iletim*
128.1.0.0	255.255.0.0	Port_sağ	*doğrudan iletim*
198.4.12.0	255.255.255.0	Port_sağ	*128.1.0.9*

Örnek 2



Yukarıdaki şekilde show ip route komutu ile İstanbul yönlendiricisinin yönlendirme tablosundaki rotalar görüntülenmiştir. Bu ağ adresleri daha sonra bahsedileceği üzere network komutu ile konfigüre edilmektedir. Aynı örnekte kullanılan terminal ip netmask-format decimal komutu ile alt ağ maskeleri 10'luk sayı düzeninde görüntülenmektedir.

```
Istanbul#show ip route
```

```
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
10.0.0.0/24 is alt ağted, 3 alt ağs
C 10.0.1.0 is directly connected, Ethernet0
C 10.0.4.0 is directly connected, Serial1
C 10.0.5.0 is directly connected, Serial0
Istanbul#terminal ip netmask-format decimal
Istanbul#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate
default
U – per-user static route, o – ODR
Gateway of last resort is not set
10.0.0.0 255.255.255.0 is alt ağted, 3 alt ağs
C 10.0.1.0 is directly connected, Ethernet0
C 10.0.4.0 is directly connected, Serial1
C 10.0.5.0 is directly connected, Serial0
Istanbul#
```

Yukarıdaki şekilde Ankara yönlendiricisinin ara yüzleri hakkında kısa bilgiyi **show ip interface brief** komutu ile görüntülenmektedir. Ayrıca yönlendiricinin ARP önbelleğinde bulunan adresler **show ip arp** komutu ile görüntülenmektedir.

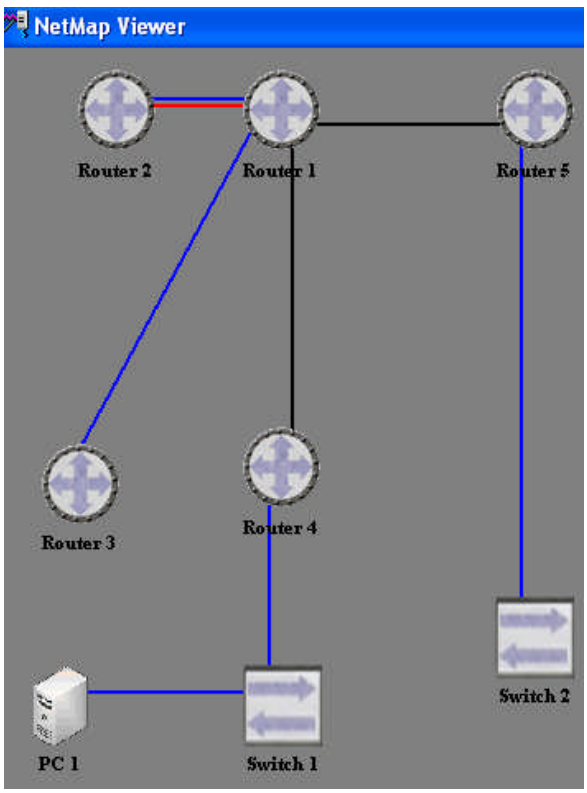
```
Ankara#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Serial0 10.0.4.2 YES manual up up
Serial1 10.0.6.2 YES manual up up
Ethernet0 10.0.2.1 YES manual up up
Ankara#show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.3.10 0 0060.9c65.1321 ARPA Ethernet0
Internet 10.0.3.13 - 0000.0b3d.5653 ARPA Ethernet0
```

Aşağıdaki örnekte iki farklı şekilde ara yüz hakkında bilgi alınabilmektedir. **show ip interface** komutu ile IP konfigürasyonu hakkında daha detaylı bilgi, **show interface** komutu ile ise arayüz hakkında genel bilgiler alınabilmektedir.

```
Izmir#show ip interface serial 1
Serial1 is up, line protocol is up
Internet address is 10.0.6.1/24
```

```
Broadcast address is 255.255.255.255
Address determined by nonvolatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
Web Cache Redirect is disabled
BGP Policy Mapping is disabled
Izmir#show interface serial 0
Serial0 is up, line protocol is up
Internet address is 10.0.5.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:05, output 00:00:04, output hang never
Last clearing of “show interface” counters never
Queuing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
273 packets input, 18621 bytes, 0 no buffer
Received 215 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
309 packets output, 20175 bytes, 0 underruns
0 output errors, 0 collisions, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ IOS yazılımını çalıştırmak için yönlendiriciye bağlı olan bilgisayarın hyper terminallini çalıştırınız ve CLI komut satırı arabirimine geçiniz.	➢ Bu öğrenme faaliyetindeki işlem basamaklarını simulator ya da emulator programları ile de yapabilirsiniz. Boson Netsim simulator programını "Load Simulator with default Labs and Netmap" seçeneği ile açtığınızda netmap olarak karşınıza gelen ağ şeması: 

<table>
<tr>
<td>

- Statik yönlendirme yaparak yönlendirme yollarını belirtiniz ve gösteriniz (Kendi Lab şemanıza göre de yönlendirme yollarını belirtebilirsiniz .).

</td>
<td>

- Yönlendiricilerin arayüzlerinin IP adresleri:

<table>
<tr><th></th><th>eRouter1</th><th>eRouter2</th><th>eRouter4</th></tr>
<tr><td>arayüz Ethernet 0</td><td>10.1.1.1
255.255.255.0</td><td>10.1.1.2
255.255.255.0</td><td></td></tr>
<tr><td>arayüz Seri 0</td><td>12.5.10.1
255.255.255.0</td><td></td><td>12.5.10.2
255.255.255.0</td></tr>
</table>

- Yönlendiricilerin arayüzlerini yukarıda değerlerlere göre yapılandırınız.

eRouter1 yönlendiricisi eRouter2 ve eRouter4 yönlendiricisine direkt bağlıdır. Bu yüzden statik yönlendirme yapılmasına gerek yoktur.

eRouter1 10.1.1.0 ağına bağlıysa, eRouter4 yönlendiricisini bu ağa bağlamak için statik yol belirtilmesi şu şekilde olur.

```
eRouter4(config)#ip route 10.1.1.0 255.255.255.0 12.5.10.1
```

12.5.10.0 ağına eRouter2 yönlendiricisini bağlamak için statik yol belirtilmesi şu şekilde olur.

```
eRouter2(config)#ip route 12.5.10.0 255.255.255.0 10.1.1.1
```

</td>
</tr>
<tr>
<td>

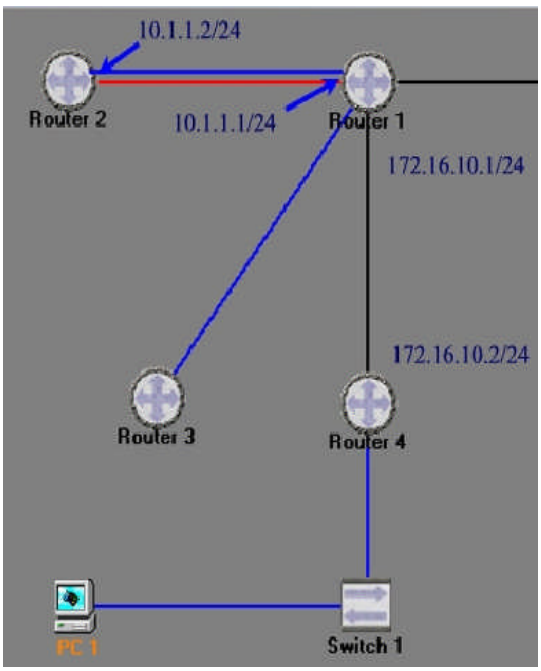
- RIP yönlendirme protokolü ile yönlendirme yollarını gösteriniz.

</td>
<td>

Yönlendiricilerin arayüzlerinin ip adresleri:

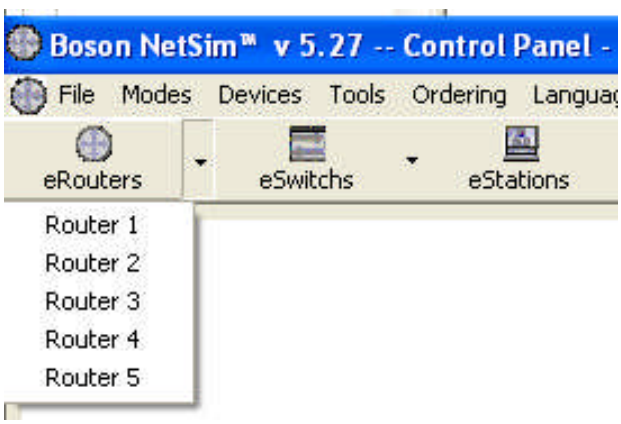
<table>
<tr><th></th><th>eRouter1</th><th>eRouter2</th><th>eRouter4</th></tr>
<tr><td>Arayüz Ethernet 0</td><td>10.1.1.1
255.255.255.0</td><td>10.1.1.2
255.255.255.0</td><td></td></tr>
<tr><td>Arayüz Serial 0</td><td>172.16.10.1
255.255.0.0</td><td></td><td>172.16.10.2
255.255.0.0</td></tr>
</table>

</td>
</tr>
</table>



- Yönlendiricilerin arayüzlerini yukarıda değerlerlere göre yapılandırınız.

- Hangi yönlendiricide yönlendirme yapılacaksa onu sırayla seçiniz.




```
eRouter1#config Terminal
eRouter1(config)#router rip
eRouter1(config-router)#
```

	eRouter1(config-router)#network 10.0.0.0 eRouter1(config-router)#network 172.16.0.0 eRouter2#config Terminal eRouter2(config)#router rip eRouter2(config-router)# eRouter2(config-router)#network 10.0.0.0 eRouter4#config Terminal eRouter4(config)# eRouter1(config-router)#network 172.16.0.0
➢ Ağ geçidini belirtiniz.	eRouter5 yönlendiricisine bağlı 10.0.0.0 ağı bulunduğunu düşünelim. "ip default-network 10.0.0.0" komutuyla öngörülen rota olarak 10.0.0.0 ağının rotası belirtilmektedir. Yani 10.0.0.0 ağına giden rota ile yönlendirme tablosunda hedef ağın bulunamadığı durumlarda kullanılacak rota aynıdır. eRouter4(config)#ip default-network 10.0.0.0
➢ Yönlendirmeleri gösteriniz.	➢ "Show ip route" komutu ile her yönlendiricinin yönlendirme tablosunu görüntüleyip inceleyebilirsiniz. ➢ "Show ip interface brief" komutu ile arayüzlerinip adreslerini listeleyebilirsiniz. ➢ ➢ "Debug ip packet" komutu ile IP paket bilgilerini tutabilirsiniz. ➢ "show interfaces" komutu ile arayüzler hakkında genel bilgiye sahip olabilirsiniz.
➢ Hedefe giden yolları inceleyiniz.	➢ Yönlendiricilerin yönlendirme tablolarına bakarak hedefe giden yolları inceleyiniz. Tabloda bulunan harflerin anlamlarını iyice kavrayınız. ➢ Geçityolu (gateway) adreslerini inceleyiniz.

Komutları yazarken hangi modda olduğunuza dikkat ediniz!

ÖLÇME VE DEĞERLENDİRME

Bu faaliyet sonunda hangi bilgileri kazandığınızı, aşağıdaki soruları yanıtlayarak belirleyiniz.

ÖLÇME SORULARI

Aşağıdaki sorulardan; sonunda parantez olanlar doğru yanlış sorularıdır. Verilen ifadeye göre parantez içine doğru ise "D", yanlış ise "Y" yazınız. Şıklı sorularda doğru şıkkı işaretleyiniz.

1. Paket yapısı içerisinde aşağıdakilerden hangisi bulunmaz?

A) Protokol
B) Kaynak IP adres
C) MAC Adres
D) Versiyon

2. Yönlendirme tablosunu görüntülemek için aşağıdaki komutlardan hangisi kullanılır?

A) show ip arp
B) show ip route
C) show host
D) show ip interface brief

3. Yönlendirici ara yüzleri hakkında kısa bilgiyi görüntülemek için aşağıdaki komutlardan hangisi kullanılır?

A) show ip arp
B) show ip route
C) show host
D) show ip interface brief

4. Ping komutu kullanıldığında bilinmeyen bir paket alınmışsa aşağıdaki işaretlerden hangisi ekrana çıkar?

A) !
B) M
C) P
D) ?

5. Dinamik yönlendirmeler sistem yöneticisi tarafından elle girilir ve hedef ağ ile bu paketi hedefine taşıyacak bir sonraki yönlendiricinin adresi bilinmelidir.( )

6. Yönlendirici aldığı paketi hedef ağ adresini yönlendirme tablosunda bulamadığı zaman paketi göndermek istediğiniz ağı ip default-network komutu ile belirleyebilirsiniz. ( )

7. IP paketi bilgilerini tutan "debug ip packet" komutudur. ( )

8. Ping komutu herhangi bir mantıksal adrese sahip bir bilgisayar ile bağlantının varlığını belirlemek için kullanılmaktadır. ( )

9. Yönlendirme tablosundaki eşit metrikli rota sayısını ip maximum-paths komutuyla değiştirilebilmektedir.( )

10. Bir grup bilgisayarı temsil eden ve o grupta bulunan bütün bilgisayarlarda aynı olan bölüme uç (host) denir. ( )

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz.

Bu öğrenme faaliyetini tam anlamıyla anladığınızı düşündüğünüzde Öğrenme Faaliyeti -2' ye geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Komutları kullanarak katmanları ve ağı test edebileceksiniz.

ARAŞTIRMA

- Ağ testi için kullanılan komutları araştırınız.
- Ağda sık karşılaşılan donanım sorunlarını araştırınız.

2. AĞ TESTİ

Bazen her şeyi düzgün yüklediğiniz halde sistem çalışmayabilir. Bilgisayar zaten yeterince karmaşık bir yapıyken, bunları birbirine bağlamak ve ortak çalışmalarını sağlamaya çalışmak doğal olarak dikkat edilmesi gereken bileşen sayısını artırır. Network sistemlerinde çalışmama veya kilitlenme problemleri çok sık karşılaşılan problemlerdir. Böyle bir durumda adım adım ilerleyerek problemin nerden kaynaklandığını tespit etmek gerekir.

Problem yazılım veya donanım kaynaklı olabilir. Donanımı, kablolar, routerlar, hublar ve ethernetler olarak tanımlayabiliriz. Yazılım problemleri eksik veya yanlış yüklenme, ayarlarda eksiklik veya uyumsuzluk olarak sıralanabilir.

2.1. OSI Katman Hataları

- Katman Hataları

  - Kablo kırılmaları
  - Kablo bağlantı kesikleri
  - Kabloların yanlış portlara takılması
  - Ara kablo bağlantı hataları
  - Yanlış kablo seçimi
  - Alıcı-verici problemleri
  - DCE kablo problemleri.
  - DTE kablo problemleri
  - Cihazların kapalı olması

- Katman Hataları

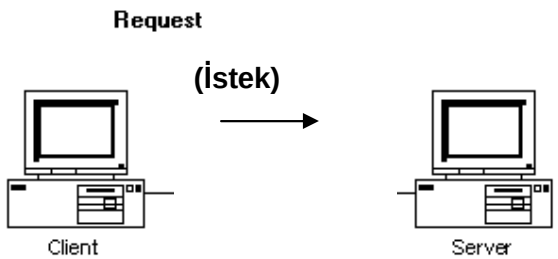
  - Uygunsuz seri arayüz yapılandırılması
  - Uygunsuz Ethernet arayüz yapılandırılması
  - Datanın uygunsuz zarflanması
  - Seri arayüzde uygunsuz saat ayarı yapılması.

- Katman Hataları

  - Yanlış yönlendirme protokollünün kullanılması
  - Yanlış IP adres
  - Yanlış Alt ağ Mask
  - IP bağlantılarında yanlış DNS

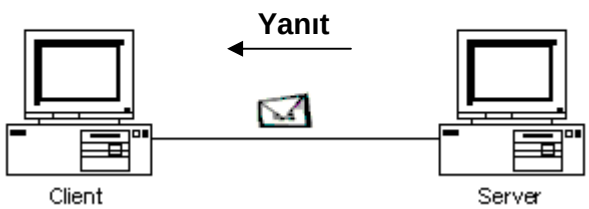
2.2. Ağ testine Giriş

Sağlıklı basit bir ağın çalışması, aşağıdaki şekilde görüldüğü gibi özetlenebilir.



İstemci (client) bir istekte bulunur (bir dizinin listelenmesi,bir dosyanın açılması,bir dosyanın okunup yazılması,yazıcı çıkışı gibi).

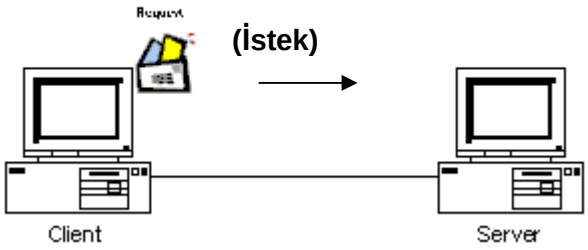
Bu istek bir Network-Veri paketi haline getirilir. Sunucu (server) veri paketini alır. Daha sonra gelen isteği işler, cevap olacak veri paketlerini hazırlar. Cevap tekrar bir veri paketi haline getirilir. Cevabı içeren veri paketi istemciye gönderilir.

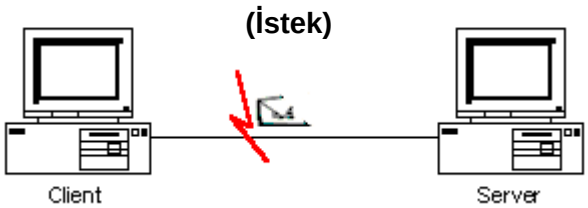


İstemci veri paketini alarak gereken işlemi yapar.

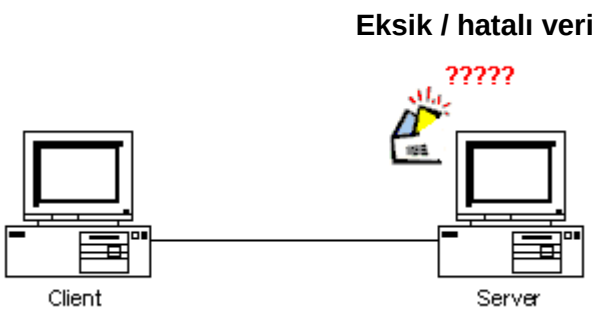
Eğer kablolamada bir problem var ise:

İstemci bir istekte bulunur (bir dizinin listelenmesi, bir dosyanın açılması,bir dosyanın okunup yazılması,yazıcı çıkışı gibi). Bu istek bir Network-Veri paketi haline getirilir.





Bu "paket" bir elektrik sinyali olarak, ethernet kartından çıkar, kablolardan geçerek "server" isimli makineye gönderilir. Fakat kablodaki bir problem nedeniyle yerine tam ve hasarsız ulaşamaz.



Sunucu veri paketini alır. Ancak paket yolda bozulduğu için bunun ne olduğunu anlamaz. Dolayısıyla da bir cevap üretemez.

Sonuçta (bir süre beklendikten sonra) Client gönderdiği veri paketinin yolda kaybolduğunu kabul eder (time out).

Bundan sonra istemci isteğini yineler.

Sonuçta bu beklemeler, tekrar-tekrar gönderimler ağ performansını düşürür.
Böyle durumlarda; sonraki konularda anlatılacak olan NET DIAG / STATUS komutu çalıştırarak ve ağ istatistiklerinizden yararlanarak problem çözülmeye çalışılabilir.

Ethernet paketleri (veri paketleri) genellikle aşağıdaki nedenlerden dolayı bozulmaya uğrarlar:

- Bozuk ağ kartları
- Yanlış bağlanmış terminatörler, bozuk terminatörler ve hub portları
- Kablo çok uzunsa
- Bozuk T konnektörleri
- Cat5 kablo kullanıp sonra Cat3 jak, priz vs. kullanmak
- Kablonun geçtiği bölgelerdeki manyetik alanlar (motorlar, floresan lambalar, mıknatıslar, elektrik kabloları vb.)

Bazen yukarıdaki sebeplerden bir tanesine sahip bir terminal bile ağa sürekli bozuk veri paketleri göndermek suretiyle, tüm sistemi işlemez hale getirebilir.

Hub üzerindeki ışıklardan takip edildiğinde üzerinden veri transferi olmadığı halde bir terminalin ışığı sürekli yanıyorsa (veri iletimi durumunu gösteren ışık) orada bir problem var demektir. Hub'ın ışığının yanması her zaman o bağlantının sağlıklı olduğu anlamına gelmez.

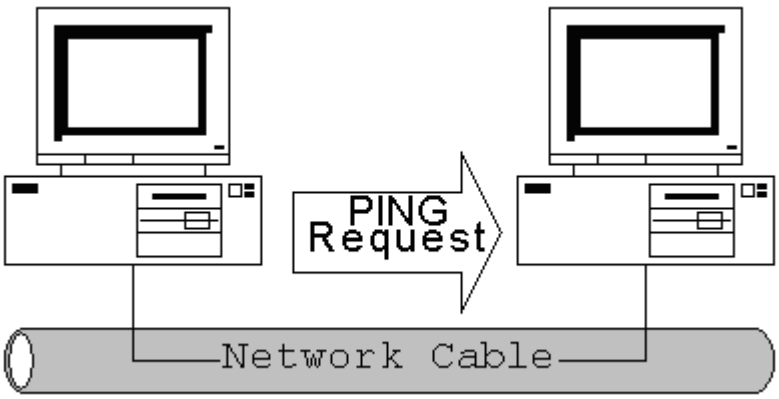
2.3. OSI Katman Sorunlarını Tespit Etme

OSI katman modelinde sorunların tespiti için bazı komutlar kullanılmaktadır. Bunların en başında ping komutu gelmektedir. Ping komutu fiziksel katmanla, ağ katmanını test etmek için kullanılır. Diğer komutlar tracert, netstat, ipconfig, route'dır. Ayrıca ağı kontrol etmek için NetDıag komutu kullanılır. Uygulama katmanında ağı test etmek için telnet kullanılmaktadır.

2.3.1. Ping Komutu

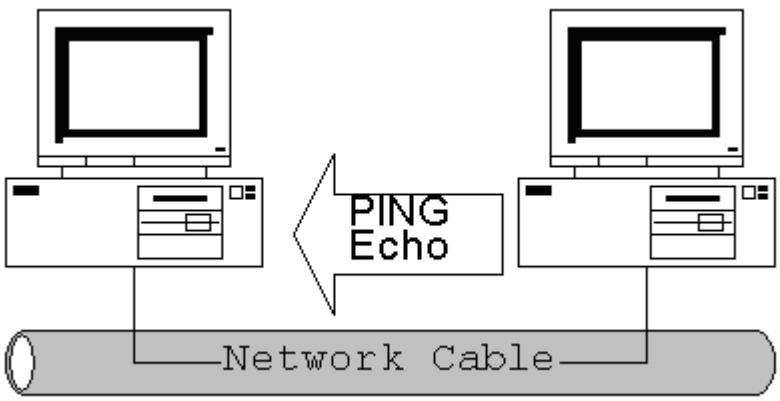
Ağda herhangi bir problem olup olmadığının testi ping (packet internet grapher) komutu ile kolayca yapılabilir. Ping, ağ üzerinde bulunan bilgisayarların ulaşılabilirliğini test etmek için ICMP (Internet Control Message Protocol) protokolünü kullanan bir uygulamadır.

Denizaltıların birbirlerini bulmak için yolladıkları sesleri ping sinyaline benzetebiliriz. Gönderilen bir sinyale diğer denizaltıdan cevap gelecektir. Bu örnek ping'in yaptığına tam uymaktadır:



PING Request : PING isteği **Network Cable: Ağ kablosu**

Şekil 2.1 Ping isteğinin gönderilmesi



PING Echo: PING yankısı

Şekil2.2 Ping isteğinin alınması

Ping komutu TCP/IP nin bir parçasıdır ve işletim sisteminden bağımsız çalışır. Bir ping sinyali alındığında, sinyali gönderene geri yollanır (Yani bir Windows makinesinden bir UNIX makinesine ping atabilirsiniz, makinelar üzerinde yüklü işletim sistemi önemsizdir, yeter ki TCP/IP yüklü ve ayarlanmış olsun.)

Kablonun iletiminde bir problem olmadığını ve makinenin ağ açısından çalışır durumda olup olmadığını anlamak için ping komutunu kullanılır.

Ping komutunun bazı kullanım şekilleri vardır:

```
C:\Documents and Settings\      >ping/?

Kullanımı: ping [-t] [-a] [-n sayım] [-l boyut] [-f] [-i TTL] [-v TOS]
               [-r sayım] [-s sayım] [[-j anabilgisayarlistesi] |
               [-k   anabilgisayarlistesi]]
               [-w zamanaşımı] hedef_adı

Seçenekler:
    -t             Belirtilen ana bilgisayar durana kadar ping komutunu
                   kullanın.
                   İstatistikleri görmek ve devam etmek için - Control-Break
                   yazın;
                   Durdurmak için - Control-C yazın.
    -a             Adresleri ana bilgisayar adlarına çözün.
    -n sayım       Gönderilecek yankı isteklerin sayısı.
    -l boyut       Arabellek boyutunu gönderin.
    -f             Pakette Parçalara Ayırma bayrağını ayarlayın.
    -i TTL         Yaşam Süresi.
    -v TOS         Hizmet Türü.
    -r sayım       Sayım durakları için kayıt yolu.
    -s sayım       Sayım durakları için zaman damgası.
    -j ana bilgisayar-listesi
                        Ana bilgisayar-listesi boyunca belirsiz kaynak yolu.
    -k ana bilgisayar-listesi
                        Ana bilgisayar-listesi boyunca kesin kaynak yolu.
    -w zamanaşımı  Her yanıt için milisaniye cinsinden beklenecek süre.


C:\Documents and Settings\      >_
```

ping -a 192.168.0.2 ===> IP deki diğer bilgisayara ufak veri paketleri gönderip, alarak baglantıyı test eder. "-a" parametresi ile IP deki bilgisayarın adresi görüntülenir.

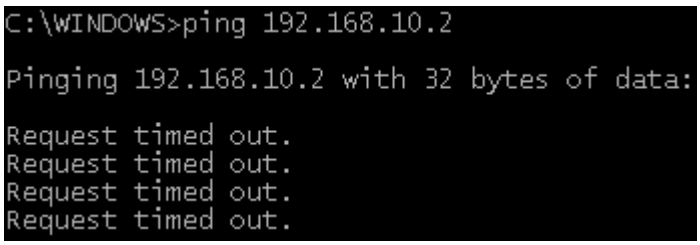
ping -a -n 20 192.168.0.2 ===> -n parametresinin yanındaki değer kadar veri paketleri gönderilerek test edilir.

```
C:\>ping 192.168.0.10

32 bayt veri ile 192.168.0.10 'ping' ediliyor:

192.168.0.10 cevabı: bayt=32 süre<1ms TTL=128
192.168.0.10 cevabı: bayt=32 süre<1ms TTL=128
192.168.0.10 cevabı: bayt=32 süre<1ms TTL=128
192.168.0.10 cevabı: bayt=32 süre<1ms TTL=128

192.168.0.10 için Ping istatistiği:
    Paket: Giden = 4, Gelen = 4, Kaybolan = 0 (0% kayıp),
Mili saniye türünden yaklaşık tur süreleri:
    En Az = 0ms, En Çok = 0ms, Ortalama = 0ms

C:\>
```

Eğer paketler geri gelirse Ethernet kartının ve kablolamanın çalıştığından emin olunabilir. Eğer bağlantı sorunu buna rağmen devam ediyorsa, bir yazılım sorunu var

demektir. Bunun için, protokol ayarlarına bakılmalıdır. IPX – SPX kullanılıyorsa ağ üzerinde paylaşımlar, kullanıcı hakları ve çalışma grupları kontrol edilmelidir.

Ancak paketler geri gelmiyorsa;



Eğer 'ping' geri gelen cevabı alamıyorsa (' Request timed out'-'İstek zaman aşımına uğradı'), donanımsal bir problem var demektir. Kablolar, hublar, jak ve T konnektörler ölçü aleti ile kontrol edilmelidir! Gözle görülemeyen temassızlık veya arızalar olabilir.

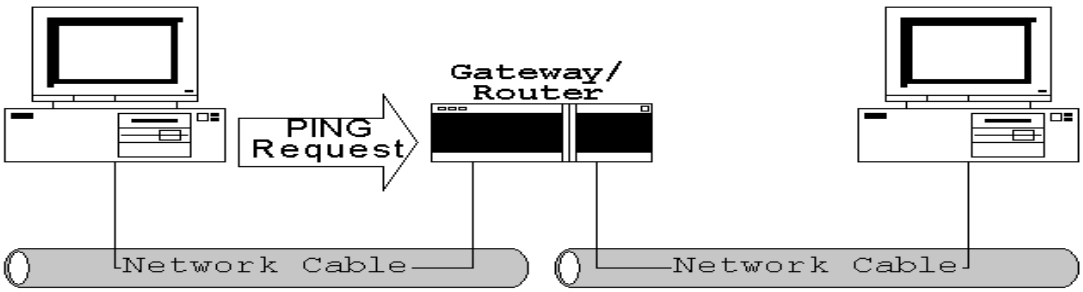
Ağların kurulumunda "Ethernet kablo test edicileri" kullanılır. Bu cihaz size kablonun sağlam olup olmadığını bildirir.

Bazen de ping tek yönlü çalışır. Eğer ping her iki yönde de çalışmıyorsa, büyük ihtimalle donanımsal bir problem var demektir. Ağ kartı, hub (eğer 10 Mbit ise), veya T konnektörler (eğer koaksiyel kullanılırsa) problemli olabilir. Bazen bu T konnektörler üzerinde (veya RJ-45 jaklarda) gözle görülemeyen mikro çatlaklar oluşabilir.

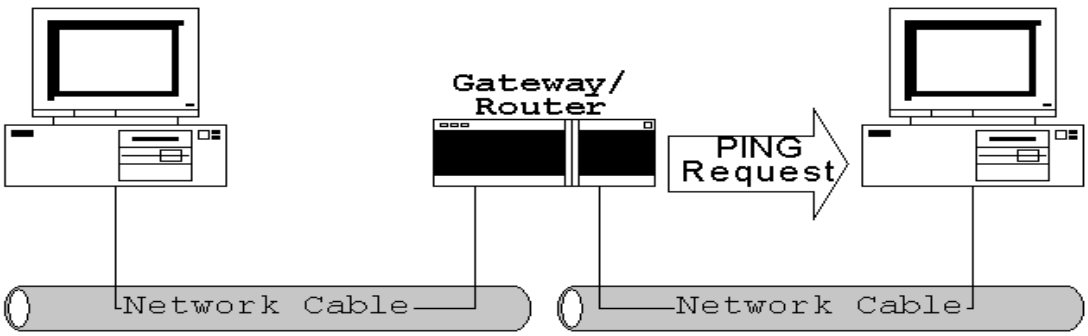
Yukarıdaki hata mesajı, ping atılan makine aynı alt ağda değilse (bu şekilde doğrudan bağlantı mümkün değildir) ve gerekli geçityolu (gateway) adresi doğru girilmemişse alınır. Bunu düzeltmek için geçerli bir geçityolu adresi girmek gerekir.

Bağlantı, geçityolu/Router(yönlendirici) üzerinden kontrol edilirken izlenmesi gereken işlem adımları aşağıdadır:

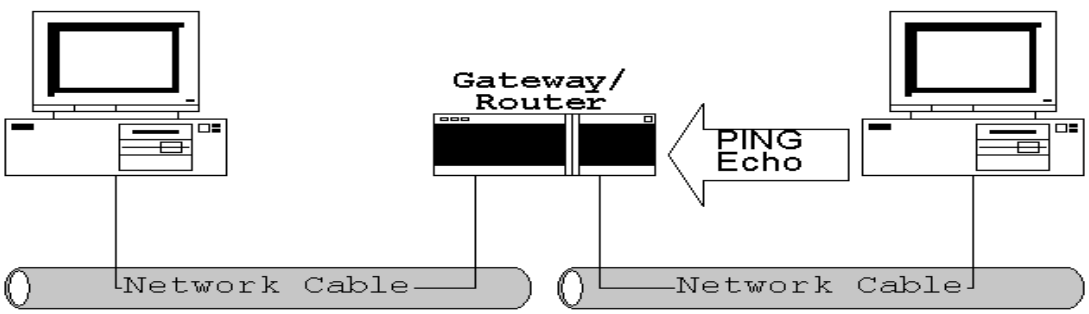
- PING sinyali Gateway/Router'a yolanır.



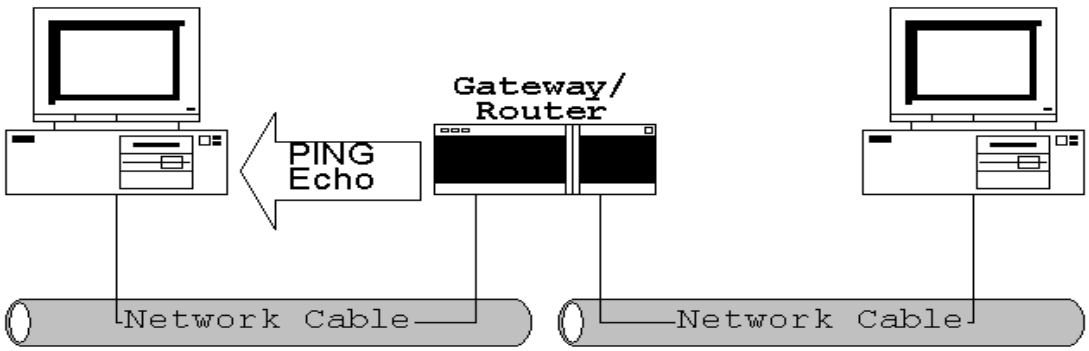
- Gateway PING sinyalini hedef sisteme geçirir.(veya hedef bilgisayarın olduğu sub-nete bağlı diğer bir Gateway'e iletir.)



- Hedef makine PING ECHO yu oluşturur (sinyali geri yollar).(ancak hedef makineda da gateway/router ayarları yapılmışsa bu gerçekleşebilir!)



- Gateway/Router PING Echo'yu alır ve kaynak sisteme yollar.



Gateways/Router, kurulumunda tüm sistemlerde gerekli ayarlar yapılmalıdır, sinyal kaynaktan hedefe ve geriye doğru dolaşabilmelidir.

Eğer problem yaşanırsa ping komutu her iki sistemde de çalıştırılır. Bu şekilde problemi tespit etmeyi kolaylaştıracak hata mesajları alınır ("missing Gateway definition" mesajı gibi mesela).

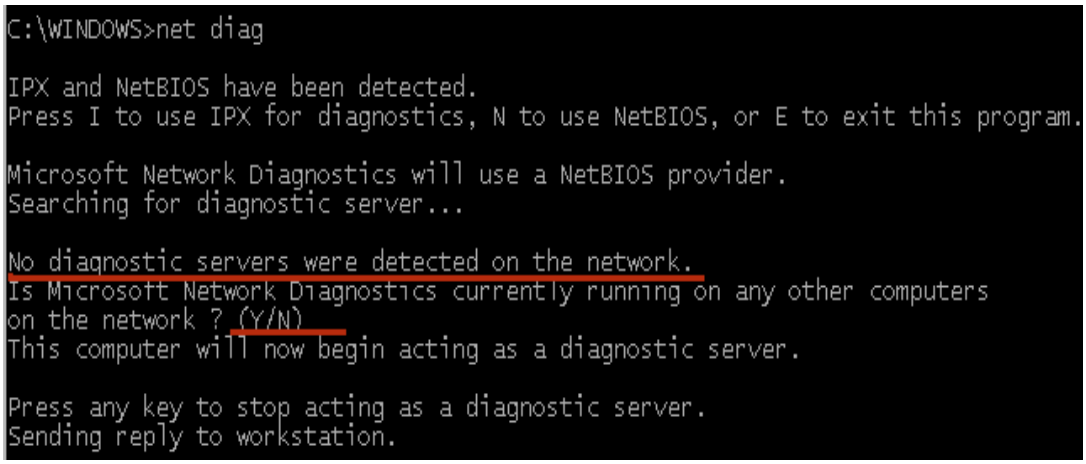
Ping komutu bir IP adresiyle kullanıldığında doğru yanıtı veriyor fakat bir ana bilgisayar veya NetBIOS adıyla kullanıldığında hatalı bir yanıt veriyor ise ad çözümleme sorunu vardır. Ping komutu gibi TCP/IP araçları kullanıldığında ad çözümlemesi için Hosts dosyası veya bir DNS sunucusu kullanılır. Hosts dosyası systemroot\System32\Drivers\Etc klasöründe bulunur. Bu dosya dinamik değildir; girdileri el ile eklemek gerekir. DNS sunucusu ana bilgisayar adı çözümlemesi için doğru DNS sunucularının doğru sırade ve şekilde yapılandırıkdıkları doğrulanmalıdır. Geçerli TCP/IP yapılandırmasını **ipconfig /all** komutuyla ve DNS sunucularınızla bağlanırlığı ping komutuyla denetlenebilir.

2.3.2. NET DIAG ile Ağ Kontrolü

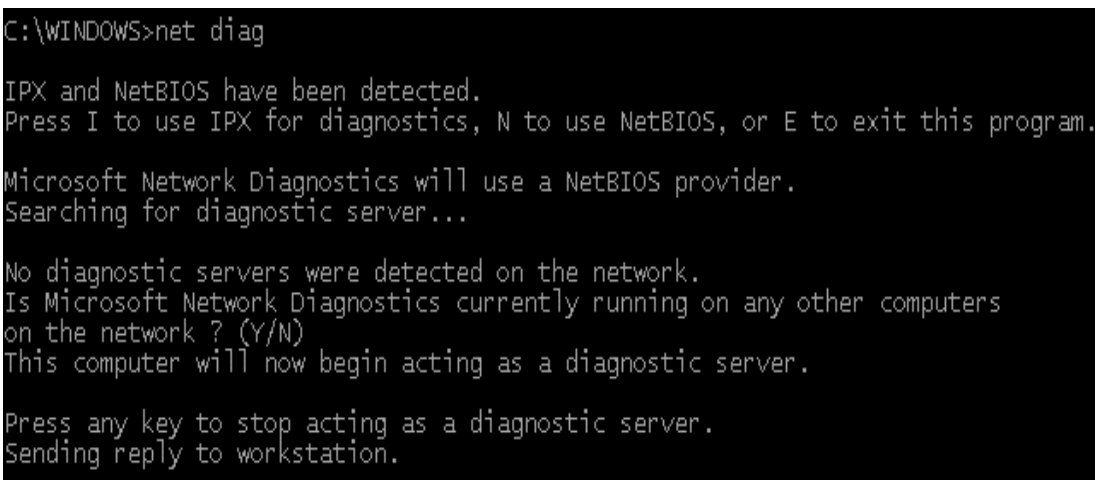
Bir ağ çalışmadığında donanım problemi ile mi yazılım problemi ile mi karşı karşıya olduğunuzu ayırt etmemiz gereklidir. Windows'a ağ eklentileri yüklendiğinde bazı DOS modunda çalışan programcıklar yüklenir (ping,ftp gibi). Ancak "net.exe" programı bunlar içinde en fazla parametreye sahip olanıdır. Net programcığının en önemli özelliklerinden biri "diag" parametresidir, bu parametre ile çalıştırıldığında güçlü bir kontrol programı haline gelir.

Net Diag ile protokolden bağımsız bir test yapılabilir. Yani bu aracın kullanılması için TCP/IP veya diğer bir protokolün özellikle yüklenmesi gerekmez.

Birinci makinede MS-DOS komut isteminde: net diag yazıp **enter** tuşuna basılır.



Eğer birden fazla protokol yüklü ise testte kullanılmak üzere birisi seçilir.Öncelikle ağdaki diğer bir makine üzerinde halen çalışır halde bir net diag olup olmadığını sorulur, eğer N denilirse makineyı bir 'Diagnostic Server' haline getirir.Diğer terminallerde de aynen net diag komutu çalıştırılır.



Eğer sorulursa protokol seçilir.

Eğer ağ donanımı düzgün çalışıyorsa şimdi bu makine üzerindeki net diag, az önce diğer makine üzerinde çalıştırıp bıraktığımız 'Diagnostic Server' ı bulmalı, ancak bulamazsa (No diagnostic servers were detected on the network-Ağ üzerinde herhangi bir Diagnostic sunucu bulunamadıI) mesajı verecektir. Bu durumda donanımsal bir problem var demektir.

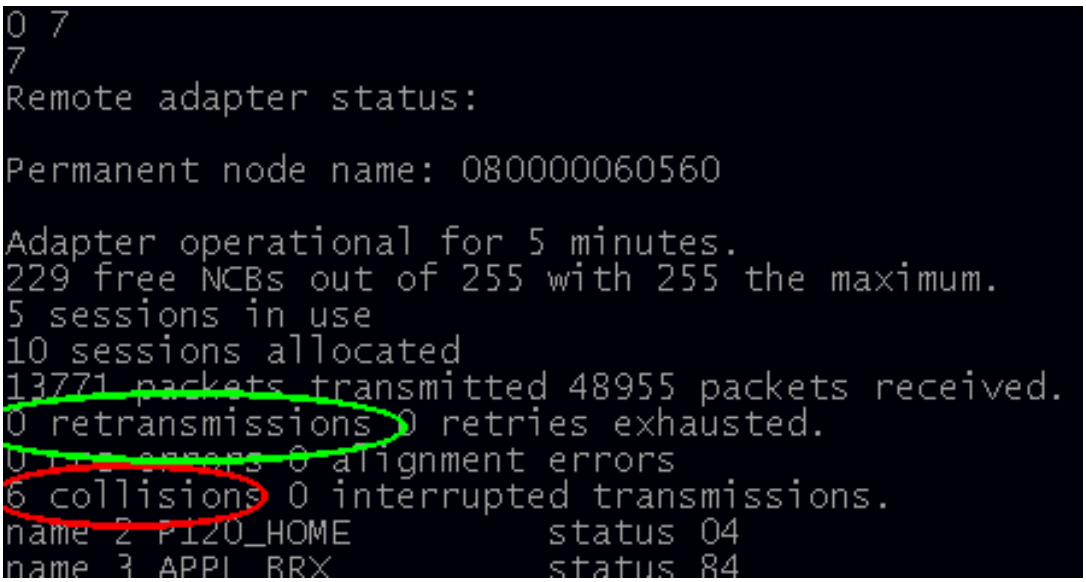
Özetleyecek olursak, bir makinede "net diag" komutu çalıştırılır ve N tuşuna basıp onu sürekli olarak ağa "ben diagnostik sunucuyum, yok mu bana kontrol sinyali yollayıp, bağlantısını kontrol edecek terminal !" şeklinde mesaj yayar, daha sonra diğer terminale gidilir, "net diag" çalıştırılarak ağdaki diag sunucu bulunarak bağlantı kurulması beklenir. Eğer diag sunucu bulunamıyor ise, donanımsal olarak bir problem var demektir. Ağ kartı, kablo ve konnektörleri kontrol etmek gerekir.

2.3.2.1. NET DIAG /STATUS

Windows komut isteminde çalıştırılan Net komutu network hakkında birçok önemli bilgi verebilir.

Ağ istatistiklerini analiz etmek için, NET DIAG /STATUS komutu kullanılır.

Komut kullanıldığında bilgisayar ismi sorulur, kendi sisteminiz için boş bir enter yapılabilir. Eğer sistemde birden fazla ağ kartı takılı ise birini seçmek gereklidir (dial-up adapter burada bir network kartı olarak sayılmaz). Örneğin konfigurasyonda Dial-up adapter 0 numara ile, Ne2000 Ethernet kartı ise 7 numarası ile belirlidir.



Bu rapor şunları gösterir:

- Ağ kartının kullanım süresi (5 dakika)
- Alınmış ve gönderilmiş ağ paketleri
- Tekrar gönderimler
- Collision'lar (çakışmalar)
- **Çakışmalar (Collisions)**

Ethernet bir CSMA/CD (Carrier Sence - Multipe Access /Collision Detection) network'dür.

Bağlı tüm istasyonlar network kablosunu geçerli bir taşıyıcı sinyal varlığını dinler.

Eğer o anda aktif bir iletişim yoksa (yani kablo üzerinde bir veri paketi yoksa), istasyon iletişime geçer(veri paketlerini kabloya koyar).Ancak eğer aynı anda birden fazla istasyon veri paketlerini yollarsa, sinyal çarpışması durumu oluşur. Bu tespit edildiğinde her iki istasyonda rastgele bir süre bekler ve tekrar veri paketlerini göndermeye çalışır. Bir ethernet ağında her zaman bu tip çakışmalar (collision) olur. Çünkü daima aynı anda iletişime geçmek isteyen birden fazla terminal bulunacaktır. Ancak eğer çakışma ortalaması gönderilen paketlerin %10'unu geçmeye başlamışsa, ağ kablosu üzerinde fazla yük vardır ve kablo fazla meşgul demektir. Bu durumda ağı farklı segmentlere bölmelisiniz. Bunu server'a ek ağ kartları takıp veya köprüler (bridge) kullanarak yapabilirsiniz.

- **Tekrar Gönderimler (Retransmittions)**

Bu değer çok düşük olmalıdır. Çünkü tekrar gönderimler ağdaki ciddi bir problemi gösterir. Veri paketleri aktarım esnasında bozulmaktadır ve bekleme periyodundan sonra tekrar gönderilmektedir. Bu performansın düşmesine sebep olur.

2.3.3. Ipconfig Komutu

Ipconfig bilgisayarın ağdaki IP adresini gösterir. Bu komut, bilgisayar tarafından kullanılan IP yapılandırması ayrıntılarını görüntülemek ve değiştirmek için kullanılır. DNS istemcilerinin sorunlarının giderilmesine ve desteklenmelerine yardımcı olmak üzere, bu yardımcı programa ek komut satırı seçenekleri eklenmiştir.

```
C:\>ipconfig

Windows IP Yapılandırması


Ethernet bağdaştırıcı Wireless Network Connection:

        Bağlantıya özgü DNS Soneki .  . . :
        IP Adres. . . . . . . . . . . . . : 192.168.2.2
        Alt Ağ Maskesi. . . . . . . . . . : 255.255.255.0
        Varsayılan Ağ Geçidi. . . . . . . : 192.168.2.1

Ethernet bağdaştırıcı Local Area Connection 2:

        Ortam Durumu  . . . . . . . . : Ortam Bağlantısı kesildi

Ethernet bağdaştırıcı Local Area Connection:

        Bağlantıya özgü DNS Soneki .  . . :
        IP Adres. . . . . . . . . . . . . : 192.168.50.1
        Alt Ağ Maskesi. . . . . . . . . . : 255.255.255.0
        Varsayılan Ağ Geçidi. . . . . . . :

C:\>_
```

ipconfig /all ===> bilgisayarın agdaki ip adresini ve birçok ayrıntıyı gösterir.

ipconfig /all >egemen.txt ===> dökülen tüm bilgiyi egemen.txt dosyası içine atar.

ipconfig /release ===> bilgisayarın ağdaki IP sini bırakır.

ipconfig /renew ===> bilgisayarın ağdaki IPsini yeniler. Yenileme işlemi sırasında ilk önce "release" , sonra "renew" işlemi uygulanır.

ipconfig /registerdns ===> bilgisayarı adını ve IPsini DNS e kaydetmek için kullanılır.

ipconfig /flushdns ===> DNS istemcilerin önbelleklerinde tuttukları isim ve IP adres eşleşmelerine ait bilgileri siler, önbelleği boşaltır.

ipconfig /displaydns ===> Eğer kullandığınız bilgisayar aynı zamanda bir DNS istemcisi ise, DNS Cache belleğinde bulunan IP adresleri ve onlara ait olan DNS isimlerinin gösterilmesini sağlar.

```
KULLANIM:
    ipconfig [/? | /all | /renew [bağdaşdırıcı] | /release [bağdaşdırıcı] |
             /flushdns | /displaydns | /registerdns |
             /showclassid adapter |
             /setclassid adapter [sınıfid] ]

yer
    adapter         bağlantı adı
                   (joker karakter * ile ? kullanılır; bkz. örnekler)

    Seçenekler:
       /?           Bu yardım iletisini görüntüler
       /all         Tüm yapılandırma bilgisini görüntüler.
       /release     Belirtilen bağdaştırıcı için IP adresini serbest bırakır.
       /renew       Belirtilen bağdaştırıcı için IP adresini yeniler.
       /flushdns    DNS Çözücü önbelleğini temizler.
       /registerdns Tüm DHCP kiralarını yeniler ve DNS adlarını yeniden
                    kaydettirir
       /displaydns  DNS Çözücü önbelleğinin içeriğini gösterir.
       /showclassid Bağdaştırıcıda izin verilen tüm dhcp sınıf kimliklerini
                    gösterir.
       /setclassid  DHCP sınıf kimliğini değiştirir.

Varsayılan, TCP/IP\'ye bağlı tüm bağdaştırıcılar için, IP adresi,
alt ağ maskesi ve varsayılan ağ geçidinin görüntülenmesidir.

Bırakma ve Yenileme için bağdaştırıcı adı belirtilmezse, TCP/IP'ye bağlı
tüm bağdaştırıcıların IP adres kiraları serbest bırakılıp yenilenir.

SetClassID için ClassId belirtilmezse, ClassId kaldırılır.

örnekler:
    > ipconfig                    ... Bilgi gösterir.
    > ipconfig /all               ... Ayrıntılı bilgi gösterir
    > ipconfig /renew             ... tüm bağdaştırıcıları yeniler
    > ipconfig /renew EL*         ... adı EL ile başlayan başlayan
                                      bağlantıları yeniler
    > ipconfig /release *Con*     ... eşleşen tüm bağdaştırıcıları serbest
                                      bırak,
                                      örn. "Yerel Ağ Bağlantısı 1" ya da
                                           "Yerel Ağ Bağlantısı 2"
```

2.3.4.Route Komutu

Yerel IP yönlendirme tablosundaki girdileri görüntüler ve değiştirir. **route**, parametreler olmadan kullanıldığında yardımı görüntüler.

Route add ===> Bir yol ekler.

Route change ===> Var olan bir yolu değiştirir.

Route delete ===> Var olan bir yolu ya da yolları siler.

Route print ===> Var olan bir yolu ya da yolları yazdırır.

Komut **print** veya **delete** ise, *Ağgeçidi* parametresi atlanabilir ve hedef ve ağ geçidi için joker karakterler kullanılabilir. *Hedef* değer, yıldız işareti (*) ile belirtilen bir joker karakter değeri olabilir. Belirtilen hedef, bir yıldız işareti (*) veya soru işareti (?) içeriyorsa, joker karakter olarak işlem görür ve yalnızca eşleşen hedef yollar yazdırılır veya silinir. Yıldız işareti herhangi bir dizeyle eşleşirken, soru işareti kullanıldığında tek bir karakterle eşleşme sağlanır. Örneğin, 10.*.1, 192.168.*, 127.* ve *224*, yıldız işareti joker karakterinin geçerli kullanımlarıdır. Hedef ve alt ağ maskesinin (ağ maskesi) değerinin geçersiz bir birleşimi kullanıldığında, "Yol: hatalı ağ geçidi adresi ağ maskesi" hata iletisi görüntülenir. Hedef, ona karşılık gelen alt ağ maskesi bitinin 0'a ayarlanacağı yerde 1'e ayarlanan bir veya daha çok bit içerdiğinde bu hata iletisi görünür. Bu durumu sınamak için, hedef ve alt ağ maskesi ikili yazım kullanarak ifade edilmelidir. İkili yazımda alt ağ maskesi, hedefin ağ adresi kısmını temsil eden bir dizi 1 bit ve hedefin ana bilgisayar adresi kısmını temsil eden bir dizi 0 bitten oluşur. Hedefte, hedefin ana bilgisayar adresi (alt ağ maskesiyle tanımlandığı gibi) olan kısmı için 1'e ayarlanan bitler olup olmadığını belirlemek için denetlenmelidir. **-p** parametresi yalnızca Windows NT 4.0, Windows 2000, Windows ME, Windows XP ve Windows Server 2003 ailesinin route komutunda desteklenir. Bu parametre, Windows 95 veya Windows 98 için **route** komutu ile desteklenmez. Bu komut, yalnızca **Internet Protokolü (TCP/IP)**, Ağ Bağlantıları'ndaki bir ağ bağdaştırıcısının özelliklerinde bir bileşen olarak yüklenirse kullanılabilir.

Örnekler:

route print ===> IP yönlendirme tablosunun tüm içeriğini görüntüler.

route print 10.* ===> IP yönlendirme tablosunda *10.* ile başlayan yolları görüntüler

route add 0.0.0.0 mask 0.0.0.0 192.168.12.1 ===>Varsayılan ağ geçidi adresi 192.168.12.1 olan varsayılan bir yol ekler.

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 ===> Hedef 10.41.0.0'a, alt ağ maskesi 255.255.0.0 ve bir sonraki atlama adresi 10.27.0.1 olan bir yol ekler.

route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1 ===> Hedef 10.41,0.0'a, alt ağ maskesi 255.255.0.0 ve bir sonraki atlama adresi 10.27.0.1 olan kalıcı bir yol ekler.

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metrik 7 ===> Hedef 10.41.0.0'a, alt ağ maskesi 255.255.0.0, bir sonraki atlama adresi 10.27.0.1 ve maliyet ölçümü 7 olan bir yol ekler.

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 if 0x3 ===> Hedef 10.41.0.0'a, alt ağ maskesi 255.255.0.0, bir sonraki atlama adresi 10.27.0.1 olan ve arabirim dizini 0x3

kullanan bir yol ekler.

route delete 10.41.0.0 mask 255.255.0.0 ===> Hedef 10.41.0.0'a giden, alt ağ maskesi 255.255.0.0 olan yolu siler.

route delete 10.* ===> IP yönlendirme tablosunda *10.* ile başlayan tüm yolları siler.

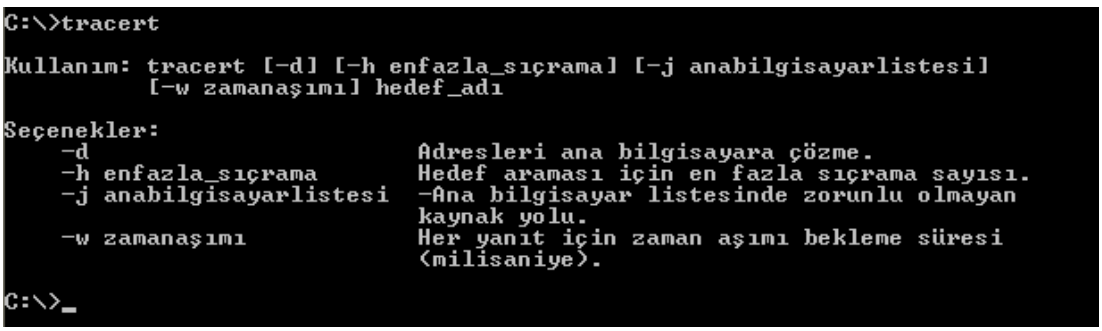
route change 10.41.0.0 mask 255.255.0.0 10.27.0.25 ===> Hedefi 10.41.0.0 ve alt ağ maskesi 255.255.0.0 olan yolun bir sonraki atlama adresini 10.27.00.1'den 10.27.0.25'e değiştirir.

```
C:\>route

Ağ yönlendirici tablolarını kullanır.

ROUTE [-f] [-p] [komut [hedef]
                [MASK ağmaskesi]  [ağgeçidi] [METRIC metrik]  [IF arabirim]

  -f            Tüm ağ geçidi girdilerinin yönlendirici tablolarını temizler.
                Komutlardan biriyle kullanıldığında, tablolar komut
                yürütülmeden önce temizlenir.
  -p            ADD komutuyla birlikte kullanıldığında, sistemin önyüklemeleri
                boyunca yolun kalıcı olmasını sağlar. Varsayılan olarak,
                sistem yeniden başlatıldığında yol korunmaz. Çoğunlukla uygun
                kalıcı yolları etkileyen diğer komutlarda yoksayılır. B
                seçenek Windows 95'te desteklenmez.
  komut         Şunlardan biri:
                  PRINT     Yolu yazdırır
                  ADD       Yol ekler
                  DELETE    Yolu siler
                  CHANGE    Varolan yolu değiştirir
  hedef           Ana bilgisayarı belirtir.
  MASK          Bir sonraki parametrenin 'ağmaskesi' değeri olduğunu belirtir.
  ağmaskesi     Bu yol girdisi için al ağ maskesi değerini belirtir.
                Belirtilmezse, varsayılan değer olarak 255.255.255.255
                kullanılır.
  ağgeçidi      Ağ geçidini belirtir.
  arabirim      belirtilen yolun arabirim numarası.
  METRIC        ölçümü belirtir; örn. hedefin maliyeti.

Hedef için kullanılan tüm simgesel adlar, NETWORKS veritabanı dosyasında
aranır. Ağ geçidinin simgesel adları, HOSTS ana bilgisayar adları veritabanı
dosyasında aranır.

PRINT veya DELETE komutu söz konusu olduğunda, hedef veya ağ geçidi için
joker kullanılabilir (joker karakter olarak yıldız  '*' belirtilir) veya ağ
geçidi bağımsız değişkeni yoksayılabilir. Hedef * veya ? içeriyorsa, kabuk
desen olarak kabul edilir ve yalnızca eşleşen hedef yolları yazdırılır.
'*' bir dizenin yerine,  '?' ise tek, bir karakter yerine kullanılır.
Örnekler: 157.*.1, 157.*, 127.*, *224*.
Tanılama Notları:
    (DEST ve MASK) != DEST olduğunda geçersiz MASK hata oluşturuyor.
    Örnek> yol ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
              Yol eklemesi başarısız oldu: Belirtilen maske parametresi geçersiz.

(Hedef && Maske) != Hedef.

Örnekler:

    > yol PRINT
    > yol ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              hedef^      ^maske      ^ağ geçidi     ölçüm^    ^
                                                        Arabirim^
      IF değeri verilmezse, verili ağ geçidi için en iyi arabirimi bulmaya
      çalışır.
    > route PRINT
    > route PRINT 157*            .... Yalnızca 157* ile eşleşenler yazdırılır
    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE geçit ve/veya yalnızca metrik değişimi için kullanılır.
    > route PRINT
    > route DELETE 157.0.0.0
```

2.3.5. Tracert Komutu

Bağlantı sorunları olduğunda ulaşılmak istenen hedef IP adresinin yolunu denetlemek için "tracert" komutu kullanılır.

Tracert komutu, paketleri bilgisayardan hedefe göndermede kullanılan IP yönlendiricileri serisini ve her atlamada bunun için geçen süreyi görüntüler. Paketler hedefe gönderilemiyorsa tacert komutu ile paketleri başarıyla ileten son yönlendirici görüntülenir.



Yol üzerindeki her yönlendirici, IP paketindeki TTL değerini iletmeden önce en az 1 azaltmak zorundadır. TTL (time to live – yaşam süresi), en çok bağlantı sayacıdır. Bir paket üzerindeki TTL 0'a ulaştığında, yönlendiricinin bir ICMP Zaman Aşıldı iletisini kaynak bilgisayara geri döndürmesi beklenir. En çok atlama sayısı varsayılan olarak 30'dur ve -h parametresi kullanılarak belirlenebilir. Yol, ara yönlendiriciler tarafından döndürülen ICMP Zaman Aşımı iletileri ve hedefin döndürdüğü Yankı Yanıtla iletisi incelenerek belirlenir. Ancak, bazı yönlendiriciler TTL değeri bitmiş paketler için Zaman Aşımı iletisi göndermezler ve tracert tarafından görülemezler. Bu durumda bu atlama için bir sıra yıldız (*) görüntülenir. Bir yolu izlemek ve yol üzerindeki her yönlendirici ve bağlantı için ağ gecikmesi ve paket kaybı bilgilerini sağlamak için, pathping komutunu kullanabiliriz. Bu komut, yalnızca Internet Protokolü (TCP/IP), Ağ Bağlantıları'ndaki bir ağ bağdaştırıcısının özelliklerinde bir bileşen olarak yüklenirse kullanılabilir.

Örnekler:

tracert kurum7.meb.gov.tr ===> Adı kurum7.meb.gov.tr olan ana bilgisayarın yolunu izler.

tracert -d kurum7.meb.gov.tr ===> Adı kurum7. meb.gov.tr olan ana bilgisayarın yolunu izlemek ve IP adreslerinin adlarını çözümler.

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 kurum7. meb.gov.tr ===> Adı kurum7. meb.gov.tr olan ana bilgisayarın yolunu izler ve 10.12.0.1-10.29.3.1-10.1.44.1 boştaki kaynak yönünü kullanır.

Örnek Ağ:

Hedef Network	Maske	Ağ geçidi	Arayüz
212.45.64.226	255.255.255.255	127.0.0.1*	Loopback
212.45.64.224	255.255.255.224	212.45.64.226	Ethernet0
0.0.0.0	0.0.0.0	212.45.64.225	Ethernet0

212.45.64.226 IP numarasına ve 255.255.255.224 alt ağ maskına sahip bir bilgisayar için ağ geçidinin 212.45.64.225 olarak tanımlandığını düşünelim. Bu durumda bilgisayar ait olduğu networkü 212.45.64.224 olarak hesaplayacaktır, oluşturduğu yönlendirme tablosu ise şu şekilde ifade edilebilir. Öncelikle kendi IP numarasına giden paketleri kendi kendine gönderir. 212.45.64.224 ağında olan tüm paketleri 212.45.64.226 IP numarasını kullanarak gönder, bu ağın dışındaki adreslere gidecek paketleri ise 212.45.64.225 IP numarası üzerinden yönlendir. Tablo olarak ifade edecek olursak,

* 127.0.0.1 (Loopback) bilgisayarın kendisini ifade eder, 255.255.255.255 ise tek bilgisayarı tanımlayan alt ağ maskesidir.

sonucunu elde edebiliriz. Burada belirtilen arayüz bilgisayarın bu IP numarasına ulaşmak için kullandığı arayüzdür, bu arayüzün tanımı ve gösterimi çeşitli işletim sistemleri arasında farklı olabilmektedir, unix türevi sistemlerde ethernet için eth0, le0, hme0 gibi isimler kullanılırken (burada 0 kaçıncı arayüz olduğunu gösterir, örneğin bir bilgisayarda iki ethernet kartı varsa bunlar eth0 ve eth1 ya da hme0 ve hme1 olarak tanımlanırlar), Windows tabanlı sistemlerde ise bundan farklı olarak arayüzler sahip oldukları birincil IP ile tanımlanırlar, örneğin örneğimizdeki arayüz, arayüzün birincil IP numarası olan 212.45.64.226 ile tanımlanacaktır.Bu tanımlamaların yapılmış olduğu bir bilgisayarın IP yönlendirme tablosu incelenecek olursa

C:\>route print

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
0.0.0.0	0.0.0.0	212.45.64.225	212.45.64.226	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
212.45.64.224	255.255.255.224	212.45.64.226	212.45.64.226	1
212.45.64.226	255.255.255.255	127.0.0.1	127.0.0.1	1
212.45.64.255	255.255.255.255	212.45.64.226	212.45.64.226	1
224.0.0.0	224.0.0.0	212.45.64.226	212.45.64.226	1
255.255.255.255	255.255.255.255	212.45.64.226	212.45.64.226	1

*N*OT: 0.0.0.0/0.0.0.0 tanımlanabilecek en genel ağdır. Bütün IP numaralarını kapsar.

Yukarıdaki tabloda birinci, üçüncü ve dördüncü satırların bizim oluşturduğumuz tabloda yer aldığı diğerlerinin ise yer almadığı hemen dikkati çekecektir. Burada ikinci satır 127 ile başlayan tüm adreslerin loopback arayüzüne yönlendirilmesi gerektiğini

belirtmektedir. Bu da 127 ile başlayan tüm adreslerin aslında kendi kullandığımız bilgisayarı tanımladığı anlamına gelir. Beşinci, altıncı ve yedinci satırlar ise broadcast ve multicast tanımlamalarıdır, broadcast yönlendirmeler belli bir IP numarasına değil tüm networke ulaşılmaya çalışıldığında kullanılırlar. Ancak yönlendirme tablosunun bu tanımları sistem tarafından otomatik olarak yapılmaktadır, kullanıcının bunları değiştirmesine, silmesine ya da eklemesine gerek duyulmamaktadır. Bizim oluşturduğumuz tabloda bulunmayan "metrik" hanesi ise eşdeğer yönlendirmeler arasında hangisinin önce kullanılacağını belirtir.

Bir IP yönlendirme tablosu incelenirken yada oluşturulurken dikkat edilmesi gereken en önemli noktalardan biri yönlendirme tablosunun en özelden en genele doğru taranacağıdır, örneğin 212.45.64.226 numaralı IP'ye ulaşmaya çalışırken bu IP numarasının hem 212.45.64.226/255.255.255.255 hem 212.45.64.224/255.255.255.224 hem de 0.0.0.0/0.0.0.0 networklerinin içinde kaldığı görülür ama bunların arasında en özel olan kullanılacaktır, bu da 212.45.64.226/255.255.255.255'tir.

212.45.64.226/27 IP numaralı bilgisayarımızın 212.45.64.231 IP numaralı bilgisayara ulaşmak istediğini düşünelim. Öncelikle kendi yönlendirme tablosunda bulunan ağ adresleri ile alt ağ maskelerini kullanarak bu IP'nin yönlendirme tablosundaki ağlardan herhangi birinin dahilinde olup olmadığını hesaplayacaktır. Hem birinci (0.0.0.0/0) hem de üçüncü satırların (212.45.64.224/27) bu IP'yi kapsadığı bu hesaplama sonucu ortaya çıkacaktır, 212.45.64.224/27 diğerinden daha özel bir tanımlama olduğu için bunu kullanacak ve paketi kendi IP numarası üzerinden LAN'e gönderecektir. Bunu komut satırında inceleyecek olursak.

C:\>tracert 212.45.64.231
Tracing route to aboneservisi.marketweb.net.tr [212.45.64.231]
over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms aboneservisi.marketweb.net.tr [212.45.64.231]
Trace complete.

Buradan da görüldüğü gibi 212.45.64.226 ve 212.45.64.226 bilgisayarları aynı ağda bulundukları için hiçbir ağ geçididen geçmeksizin haberleşebilmektedirler.

Bu kez aynı bilgisayarı kullanarak 212.45.64.20 IP numarasına sahip bilgisayara ulaşmaya çalıştığımızı düşünelim. Bilgisayarımız yine yönlendirme tablosunu kullanarak bu IP'nin hangi networkler tarafından kapsandığını bulmaya çalışacaktır. Bulacağı networkün ise yalnızca 0.0.0.0/0 olduğu görülecektir. (Daha önce de söylendiği gibi 0.0.0.0/0 tüm ağları kapsamaktadır, bu yüzden "sabit yol" -default route- adı verilmiştir). Bu durumda paketler, ağ geçidi olarak tanımlanan 212.45.64.225 IP numaralı cihaza yönlendirilecektir yani bir anlamda "top 212.45.64.225'e atılmıştır". 212.45.64.225 IP numaralı cihaz 212.45.64.20 IP numarasına nasıl ulaşacaktır. Bir cihazın ağ geçidi görevini görebilmesi için en az iki farklı ağda arayüzünün bulunması gerekmektedir. Örneğin bir ağ geçidi x.y.z.0/24 ağındaki bilgisayarların a.b.c.0/24 networkündeki bilgisayarlara ulaşması için kurulmuşsa, bir arayüzünün (örneğin ethernet) x.y.z.0/24 ağına bağlı, başka bir arayüzünün (ethernet, seri/dialup arabirim vs) a.b.c.0/24 ağına bağlı olması gerekmektedir.

212.45.64.20 IP numaralı bilgisayar ağ yönlendiricisine 1 numaralı ethernet

arayüzünden, 212.45.64.226 IP numaralı bilgisayar ise ağ yönlendiricisine 2 numaralı ethernet arayüzünden bağlı olduğunu düşünebiliriz.

Traceroute sonucunu incelersek

C:\>tracert 212.45.64.20
Tracing route to kheops.marketweb.net.tr [212.45.64.20]
over a maximum of 30 hops:
1 10 ms <10 ms 10 ms grf.marketweb.net.tr [212.45.64.225]
2 <10 ms 10 ms 10 ms kheops.marketweb.net.tr [212.45.64.20]
Trace complete.

Görüldüğü gibi 212.45.64.20 IP numaralı bilgisayara 212.45.64.225 numaralı cihaz üzerinden ulaşılmıştır. Buradan çıkan sonuç 212.45.64.225 IP numaralı cihazın en az iki arayüzü/IP adresinin olduğu ve bu arayüzlerden biri 212.45.64.224 ağında iken diğerinin 212.45.64.0 ağında olduğudur. 212.45.64.225 IP numaralı cihazın yönlendirme tablosu hakkında basit bir yorum yaparsak şöyle bir sonuç elde edebiliriz.

Network Address	***Netmask***	***Gateway Address***	***Interface***
212.45.64.0	*255.255.255.128**	*212.45.64.1***	*Ethernet0*
212.45.64.224	*255.255.255.224*	*212.45.64.225*	*Ethernet1*

* Buradaki traceroute sonucu ile netmaskı öğrenmek mümkün değildir, burada verileni bir önbilgi kabul edebilirsiniz.

** Burada belirtilen 212.45.64.0/25 segmentinde herhangi bir IP olabilir. Bu yönlendiricinin 212.45.64.0/25 segmentindeki IP numarasıdır. Aynı şekilde arayüzler de (ethernet0, ethernet1) önbilgi olarak yazılmıştır, arayüzlerin ne olduğu eldeki verilerle tesbit edilemez.

Görüldüğü gibi 212.45.64.225 adresine yönlendirilen paketler bu cihazın yönlendirme tablosunda taranarak ilgili arayüzlerden hedeflerine ulaştırılmışlardır. Aynı şekilde 212.45.64.20/25 IP numaralı bilgisayardan 212.45.64.226 adresine çekilen "traceroute" sonucu da

>traceroute 212.45.64.226
traceroute to 212.45.64.226 (212.45.64.226), 30 hops max, 40 byte packets
1 212.45.64.1 (212.45.64.1) 3 ms 3 ms 1 ms
2 taurus.marketweb.net.tr (212.45.64.226) 5 ms 5 ms 6 ms
şeklindedir. Bu da ağ geçidimizin hem 212.45.64.1 hem de 212.45.64.225 IP numaralarına sahip olduğunu göstermektedir.

2.3.6. Pathping Komutu

Bir kaynak ve hedef arasındaki ara atlamalarda ağ gecikmesi ve ağ kaybı konularına ilişkin bilgi verir. Pathping komutu, bir kaynak ve hedef arasındaki her yönlendiriciye belirli bir süre içinde Yankı İsteği iletileri gönderir ve her yönlendiriciden dönen paketlere dayalı olarak sonuçları hesaplar. Pathping verilen yönlendirici veya bağlantılarda paket kayıp derecesini gösterdiğinden, hangi yönlendirici veya alt ağlarda ağ sorunu bulunduğunu belirleyebilirsiniz. Pathping komutu, yol üzerinde hangi yönlendiricilerin olduğunu belirleme konusunda tracert komutu ile aynı biçimde çalışır. Belirli bir süre boyunca, tüm yönlendiricilere düzenli olarak ping isteği gönderir ve her birinden dönenlerin sayısına bağlı olarak istatistikleri hesaplar. Pathping parametresiz kullanıldığında yardımı görüntüler.

```
C:\>pathping

Kullanım: pathping [-g ana makine liste] [-h en çok sıçrama] [-i adres] [-n]
                [-p süre] [-q sorgu sayısı] [-w zaman aşımı] [-P] [-R] [-T]
                [-4] [-6] hedef adı

Seçenekler:
    -g ana makine listesi   Ana makine listesi boyunca kaynak yolunu çöz.
    -h en fazla atlama      Hedefi ararken yapılacak en fazla atlama.
    -i address              Belirtilen kaynak adresini kullan.
    -n                      Adresleri ana makine adları olarak çözümleme.
    -p süre                 Ping'ler arasında msaniye olarak bekleme süresi.
    -q sorgu sayısı         Atlama başına sorgu sayısı.
    -w zaman aşımı          Her yanıt için msaniye olarak bekleme zaman aşımı.
    -P                      RSVP PATH bağlanılabilirliğini sına.
    -R                      Her atlamanın RSVP etkin olup olmadığını sına.
    -T                      Her sıçramanın bağlanılabilirliğini
                            Tabaka 2 öncelikli etiketlerle sına.
    -4                      IPv4 kullanmaya zorla.
    -6                      IPv6 kullanmaya zorla.

C:\>_
```

Pathping parametreleri büyük/küçük harf duyarlıdır.

Ağda yığılmayı engellemek için, pingler yeterli yavaşlıkta bir hızla gönderilmelidir. Veri bloğu kayıplarının etkilerini en aza indirmek için, pingler çok sık aralıklarla gönderilmemelidir.

-p parametresini kullanırken, pingler her ara atlamaya ayrı ayrı gönderilir. Bu nedenle, aynı atlamaya gönderilen iki ping arasındaki aralık, süre'nin atlama sayısı ile çarpımı sonucu elde edilen sayıdır.

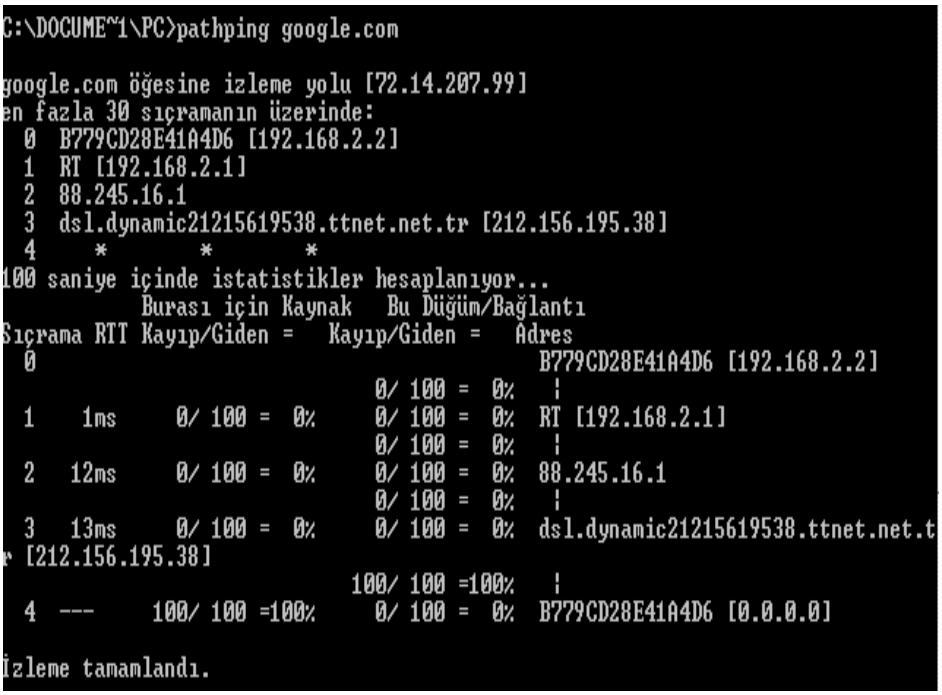
-w parametresini kullanırken, birden fazla ping paralel olarak gönderilebilir. Bu nedenle, "zaman aşımı" parametresinde belirtilen süre, iki ping arasındaki bekleme için gereken süre parametresinde belirtilen süre ile sınırlı değildir.

Bu komut, yalnızca Internet Protokolü (TCP/IP), Ağ Bağlantıları'ndaki bir ağ bağdaştırıcısının özelliklerinde bir bileşen olarak yüklenirse kullanılabilir.

Aşağıdaki örnekte **pathping** komutu çıkışı gösterilmektedir:

D:\>pathping -n corp

corp1 [10.54.1.196] öğesini izleme yolu; en fazla 30 sıçramanın üzerinde: 0 172.16.87.35 1 172.16.87.218 2 192.168.52.1 3 192.168.80.1 4 10.54.247.14 5 10.54.1.196



125 saniye içinde istatistikler hesaplanıyor...

Sıçrama	RTT			
0		172.16.87.35 0/ 100 = 0% |		
1	41ms	0/ 100 = 0%	0/ 100 = 0%	172.16.87.218 13/ 100 = 13%
2	22ms	16/ 100 = 16%	3/ 100 = 3%	192.168.52.1 0/ 100 = 0%
3	24ms	13/ 100 = 13%	0/ 100 = 0%	192.168.80.1 0/ 100 = 0%
4	21ms	14/ 100 = 14%	1/ 100 = 1%	10.54.247.14 0/ 100 = 0%
5	24ms	13/ 100 = 13%	0/ 100 = 0%	10.54.1.196

İzleme tamamlandı.

Pathping çalıştığında, ilk sonuçlar yolu listeler. Bu, **tracert** komutu kullanılarak gösterilen yolla aynı yoldur. Sonra, yaklaşık 90 saniye boyunca (bu süre atlama sayısına göre değişebilir) bir meşgul iletisi görüntülenir. Bu süre içinde, önceden listelenmiş tüm yönlendiricilerden ve aralarındaki bağlantılardan bilgi toplanır. Süre sonunda sınama sonuçları görüntülenir.

Yukarıdaki örnek raporda, **Bu Düğüm/Bağlantı**, **Kayıp/Giden = %** ve **Adres** sütunları, 172.16.87.218 ve 192.168.52.1 arasındaki bağlantının paketlerin % 13'ünü bıraktığını göstermektedir. 2 ve 4. atlamalardaki yönlendiriciler de kendilerine gönderilen paketleri bırakmakta, ancak bu kayıp kendilerine yönlendirilmeyen akışı iletmelerini etkilememektedir.

Bu bağlantıların, **Adres** sütununda dikey çubuk (|) olarak tanımlanan kayıp oranları, yol boyunca iletilen paketlerin kaybına yol açan bağlantı yığılmasını belirtir. IP adresleri ile gösterilen yönlendiriciler için görüntülenen kayıp oranları, bu yönlendiricilerin aşırı yüklenmiş olabileceğini belirtir.

2.3.7. Netstat

Etkin TCP bağlantılarını, bilgisayarın bağlı olduğu bağlantı noktalarını, Ethernet istatistiklerini, IP yönlendirme tablosunu, IP, ICMP, TCP ve UDP iletişim kuralları için IPv4 istatistikleri ile IPv6, ICMPv6, IPv6 üzerinden TCP ve IPv6 iletişim kuralları üzerinden UDP için IPv6 istatistiklerini görüntüler. Parametreler olmadan kullanılan **netstat** etkin TCP bağlantılarını görüntüler.

Bu komutla birlikte kullanılan parametrelerden önce, eğik çizgi (/) değil, bir tire işareti (-) eklenmelidir.

Netstat komutu aşağıdaki öğelerin istatistiklerini verir:

İletişim kuralının (TCP veya UDP) adı

Yerel Adres

Yerel bilgisayarın IP adresi ve kullandığı bağlantı noktasının numarası, yerel bilgisayarın IP adresine karşılık gelen adı ile bağlantı noktasının adı, ancak **-n** parametresi belirtilmediğinde görüntülenir. Bağlantı noktası henüz kurulmadıysa, bağlantı noktası numarası bir yıldız işareti (*) olarak gösterilir.

Yabancı Adres

Uzak bilgisayarın IP adresi ve bağlantı noktası numarası, IP adresine ve bağlantı noktasına karşılık gelen adlar, ancak **-n** parametresi belirtilmediğinde görüntülenir. Bağlantı noktası henüz kurulmadıysa, bağlantı noktası numarası bir yıldız işareti (*) olarak gösterilir.

Bir TCP bağlantısının durumunu gösterir. Olası durumlar şunlardır:

CLOSE_WAIT
CLOSED
ESTABLISHED
FIN_WAIT_1
FIN_WAIT_2

LAST_ACK
LISTEN
SYN_RECEIVED
SYN_SEND
TIMED_WAIT

Bu komut, yalnızca **Internet İletişim Kuralları (TCP/IP)**, Ağ Bağlantıları'nda bağlantı öğeleri altında bir bileşen olarak yüklenirse kullanılabilir.

```
C:\>netstat ?

Geçerli TCP/IP ağ bağlantılarını ve iletişim kuralı istatistiklerini gösterir.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [aralık]

  -a            Tüm bağlantıları ve dinleme bağlantı noktalarını gösterir.
  -b            Her bağlantı veya dinleme bağlantı noktası oluşumu ile ilişkili
                çalıştırılabilir dosyayı gösterir. Bazı durumlarda iyi bilinen ç
alıştırılabilir dosyalar
                birden çok bağımsız bileşeni üzerinde bulundurur ve bazı durumla
rda
                bağlantı veya dinleme bağlantı noktası oluşumu ile ilişkili
                bileşenlerin sırası gösterir. Bu durumda çalıştırılabilir dosyan
ın
                adı en altta [] içindedir, TCP/IP'ye ulaşılıncaya
                kadar üstünde çağırdığı bileşen bulunmaktadır. Dikkat edin, bu s
eçenek
                uzun sürebilir; yeterli izinleriniz yoksa başarısız
                olabilir.
  -e            Ethernet istatistiklerini gösterir. Bu, -s
                seçenek ile birleştirilebilir.
  -n            Adresleri ve bağlantı noktaları numaralarını sayısal biçimde gös
terir.
  -o            Her bağlantıyla ilişkili sahip işlem kimliğini gösterir.
  -p proto      İletişim bölümünde belirtilen iletişim kuralının
                bağlantılarını gösterir. proto
                bunlardan birisi olabilir: TCP, UDP, TCPv6 veya UDPv6.  Her ilet
işim kuralları için -s
                istatistikleri gösteren seçenekle kullanıldığında; proto bunlard
an birisi olabilir:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP veya UDPv6.
  -r            Yönlendirme tablosunu gösterir.
  -s            Her iletişim kuralları için istatistikleri gösterir.  İstatistik
ler, varsayılan olarak
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ve UDPv6 için gösterilir
;
                -p seçeneği, varsayılanın alt kümesini belirtmek için kullanılab
ilir.
  -v            -b ile birlikte kullanılırsa; tüm çalıştırılabilir dosyalar
                için bağlantı ve bağlantı noktası oluşumu ile ilgili
                bileşenlerin sırasını gösterir.
  aralık      Her görüntü arasında aralık saniyesi kadar duraklayarak
                seçili istatistikleri yeniden gösterir.  Yeniden gösterimi durdu
rmak için
                CTRL+C tuşlarına basın.  Atlanırsa, netstat, geçerli yapılandırm
a
                bilgisini bir kez yazdırır.
```

Örnekler:

netstat -e –s ===> Hem Ethernet istatistiklerini, hem de tüm protokollerin istatistiklerini görüntüler.

netstat -s -p tcp udp ===> Yalnızca TCP ve UDP protokollerinin istatistiklerini görüntüler.

nbtstat -o 5 ===> Etkin TCP bağlantılarını ve işlem kimliklerini her 5 saniyede bir görüntüler.

nbtstat -n –o ===> Etkin TCP bağlantılarını ve işlem kimliklerini sayısal formda görüntüler.

Bir ana bilgisayarla kurulan TCP/IP bağlantısı durmuş gibi görünüyorsa, veriler TCP ve UDP sıralarında engellenmiştir veya ağ ya da kullanıcı düzeyinde yazılım gecikme sorunları vardır.

Bunu çözümü "netstat –a" komutunu kullanarak yerel bilgisayarın TCP ve UDP bağlantı noktalarındaki tüm etkinliklerin durumunu görüntülemektir.

İyi bir TCP bağlantısının durumu genelde gönderme ve alma sıralarında 0 bayt ile kurulur. Veriler sıraların birinde engellenirse veya durumu düzensizleşirse, büyük bir olasılıkla bağlantıyla ilgili bir sorun vardır yoksa olasılıkla bir ağ veya uygulama düzeyinde yazılım gecikmesi söz konusudur.

2.3.8. Telnet Kullanarak Ağı Test Etmek

Telnet, herhangi bir şekilde ulaşılabilen (Internet veya özel bir ağ ile) bir makineye bağlanmayı, o makine tarafından sunulmuş kaynaklardan yararlanmayı sağlayan bir protokoldür. Telnet kullanıldığında, uzaktaki makineye oturum açılır, Terminal emülasyonu sayesinde, sanki o makinenin başında çalışılıyormuş gibi işlemler yapılabilir. Telnet ile makineye bağlanıldığında, sunucunun sahip olduğu ortamın bir kopyası kullanıcıya sunulur. Dolayısıyla hangi işletim sisteminin kullanıldığı, istekler sonucunda nasıl bir ekranın oluşturulduğu aynen kullanıcı ekranına yansır. Örneğin, Windows NT kullanılan bir makineden, Unix işletim sistemi kurulu bir makineye Telnet yapıldığında, yerel makinede Windows NT yüklü olmasına rağmen Telnet yapılan makinede Unix koştuğundan, işlemleri UNIX komutlarıyla yapmak gerekmektedir.

Kısacası Telnet yapıldığında, bağlanılan makinenin bir kopyası Telnet penceresi vasıtasıyla yerel makineye getirilmekte, dolayısıyla uzaktaki makinenin başındaymış gibi çalışmalar yapılabilmektedir. Bu sayede uygulama katmanının yazılımının doğru çalışıp çalışmadığı da test edilmiş olunur. Telnet test için geçerli bir mekanizmadır.

Bir kullanıcının Telnet yazılımından yararlanabilmesi için, dolayısıyla da Telnet protokolünü kullanabilmesi için, kendisine Internet servisi sağlayıcısının imkân vermesi gerekir. Günümüzde servis sağlayıcılarının büyük bir kısmı Telnet imkânı veriyorken, bu

hizmeti vermeyenler de vardır.

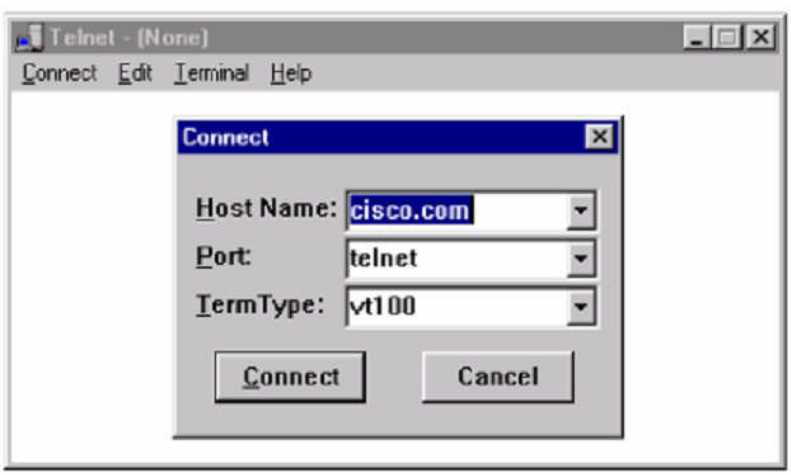
- Telnet gerçekleştirebilmek için sahip olunması gereken bilgiler:
- Bağlanılmak istenen konak (host) makinenin IP adresi veya adı,
- Buraya bağlanmakta kullanıla kullanıcı kodu.
- Kullanıcı şifresi,
- Bütün bilgiler mevcutsa, iligili makineye Telnet yapılabilir.

Windows ortamından Telnet yapmanın üç yolu vardır. Bunlardan biri MS_DOS komut satırında doğrudan komutu yazmaktır.

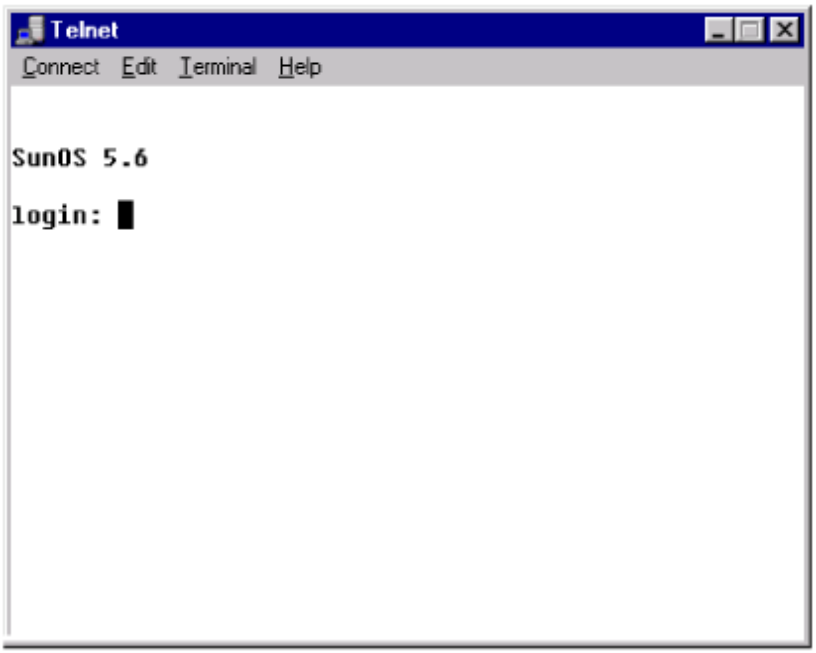
Böyle bir durumda komut ile birlikte Telnet yapılmak istenen makinenin IP numarası veya adı yazılmalıdır. Eğer makine DNS (Domain Name Service)'e kayıtlı değilse, IP numarasını yazmak gerekecektir.

Windows NT ortamından Telnet gerçekleştirmenin bir başka yolu, NT Explorer' dan yararlanıp programı tıklayarak çalıştırmaktır. Yani, Windows NT Explorer çalıştırılıp, "telnet.exe" programının bulunduğu katalog açılacak, burada da Telnet programı tıklanarak çalıştırılacaktır. Telnet programına \winnt\system32\telnet dosya yolundan erişilebilir.

Üçüncü ve son yöntemde de yine Telnet uygulaması tıklanacaktır. Ancak bu sefer Windows' un sunduğu menü sisteminden yararlanılacaktır. Son iki yöntemde, hangi makineye bağlanılmak istendiği belirtilmemişti. Dolayısıyla bir ekran vasıtasıyla bu bilgilerin alınması gerekmektedir. Telnet yapılmak istenen yeri belirtmek için menü çubuğundaki 'Connect' tıklanıp buradan da Remote System seçilmelidir. Bu durumda gelecek ekranda yapılması gereken, "Host Name" alanına, bağlanılmak istenen makinenin adının veya IP adresinin yazılmasıdır. Port alanında yazılı olan 'telnet', Telnet için ayrılmış olan portun kullanılmak istendiğini göstermektedir. Standart olarak 23 numaralı port bu işlem için kullanılır. Telnet ile diğer servislere ulaşmak isteniyorsa, bunlara ilişkin port numarası yazılmalıdır. TermType alanındaki 'vt100' de, emülasyonu yapılmak istenen terminal tipini göstermektedir. Resimde "Host Name" alanına cisco.com yazılmıştır.



Telnet oturumunun başlatılabilmesi için önce kullanıcı kodunun, sonra da şifrenin girilmesi gerekmektedir. Bu işlemler de tamamlandıktan sonra artık uzaktaki makineye oturum açılmıştır.



Bir bilgisayara aynı anda en fazla 5 telnet bağlantısı yapılabilmektedir.

Bağlanılan makine üzerinde istenen işlemler yapıldıktan sonra oturumun kapatılması gerekecektir. Bunun yapılması, bağlanılan makineye oturum açmış bir terminalin çıkması için yapılması gerekenler ile aynı olacaktır. Genellikle komut satırında yazılacak 'exit' komutu bu işlemi yerine getirecektir.

Telnet, TCP/IP protokol ailesinin bir üyesidir ve istemci/sunucu mantığına dayanır. Programın bir istemci tarafı bir de sunucu tarafı vardır. Kullanıcının bağlantıyı gerçekleştirdiği yerel makine üzerinde oturumu başlatacak, istekte bulunacak, gelecek cevapları ekranda gösterecek istemci Telnet Yazılımı' nın bulunması gerekir. Bağlanılan ve konak bilgisayar olarak adlandırılan uzaktaki makine üzerinde ise, istemci taleplerine cevap verecek bir Sunucu Telnet Programı' na ihtiyaç vardır. Protokol yalnızca alfa sayısal terminalleri destekler; diğer bir deyişle fare ve diğer işaret aygıtlarını veya grafik kullanıcı arabirimlerini desteklemez. Bu nedenle, tüm komutlar komut satırından girilmelidir.

2.3.8.1. Telnet Sunucusu

Telnet sunucusu'nu kullanarak, Telnet istemci yazılımı kullanıcılarının bilgisayarınıza bağlanabilmelerine ve komut modu uygulamalarını çalıştırabilmelerine izin verebilirsiniz.

Telnet Sunucusu, Telnet istemcileri için bir ağ geçididir. Bir bilgisayarda Telnet

Sunucusu çalışırken, kullanıcılar uzak bilgisayarlardan bu bilgisayara bağlanmak için Telnet istemcilerini kullanabilir. Telnet istemcisi, Telnet sunucusu çalıştıran bir bilgisayara bağlandığında, uzak kullanıcının bir kullanıcı adı ve parola girmesi istenir. Varsayılan değer olarak, bu sunucuya oturum açmak için yalnızca yerel sunucuda geçerli olan kullanıcı adı ve parola bileşimleri kullanılabilir.

Oturum açıldığında, kullanıcıya yerel olarak bir komut penceresinde açılmış gibi bir komut istemi verilir. Ancak varsayılan değer olarak, kullanıcı, masaüstüyle etkileşimli çalışan uygulamaları kullanamaz.

Administrators grubunun üyeleri Telnet Sunucusu'nda oturum açabilir. Diğer kullanıcıların erişimi, TelnetClients grubuna üyelikle denetlenir. Varsayılan olarak, bu grup hiçbir giriş içermez. Administrators grubunun üyesi olmayan kullanıcıların Telnet Sunucusu'nda oturum açabilmelerine izin vermek için, TelnetClients grubuna uygun kullanıcı ve grupları eklenmelidir.

Telnet Sunucusu çalıştıran bir bilgisayara erişim izni vermek için;

- Denetim Masası / Yönetimsel Araçlar / Bilgisayar Yönetimi'ni açınız.
- Konsol ağacında, Yerel Kullanıcılar ve Gruplar'ı genişletiniz ve Gruplar'ı tıklatınız.
- TelnetClients grubunu çift tıklatınız.
- Ekle seçeneğini tıklatınız.
- 5.TelnetClients grubuna kullanıcı eklemek için Kullanıcıları Seç kutusundaki yönergeleri izleyiniz ve Tamam'ı tıklatınız.

Kimlik doğrulaması, kullanıcı kimliğinin tanımlandığı ve izin verildiği bir yöntemdir. Telnet Sunucusu iki kimlik doğrulama yöntemini destekler: NTLM (NT LAN Manager – NT Yerel Ağ Yöneticis) ve düz metin

NTLM kimlik doğrulamasını kullanıyorsanız, Windows tabanlı istemciler kimlik doğrulaması için Windows güvenlik içeriğini kullanır ve kullanıcının ad ve parolasını girmesi istenmez. Kullanıcı adı ve parolası şifrelenir. Şifreleme kullanmayan oturumlar, şifresiz metin (düz metin olarak da bilinir) kullanır ve bunlar ağ içinde görünür.

NTLM kimlik doğrulamayı kullanmazsanız, kullanıcı adı ve parolası Telnet Sunucusu'nu çalıştıran bilgisayara düz metin olarak gönderilir. Kimlik doğrulama işleminin paketlerini yakalayan herhangi biri, parolayı kolaylıkla okuyabilir ve bu parolayı kullanarak intranetinize yetkisiz erişimde bulunabilir; bu nedenle düz metin kimlik doğrulaması önerilmez.

Kullanıcı için "Kullanıcı Bir Sonraki Oturum Açışında Parolayı Değiştirmeli" ayarlıysa, Telnet Sunucusu'nu çalıştıran bilgisayarda oturum açma girişimi başarısız olur. Kullanıcı sunucuya doğrudan girmeli ve parolayı değiştirmeli, daha sonra Telnet'in içinden oturumu açmalıdır.

NTLM kimlik doğrulaması kullanarak Telnet Sunucusu çalıştıran bir bilgisayara bağlanırsanız, NTLM kimlik doğrulamasının getirdiği sınırlamalardan dolayı bazı ağ kaynaklarına erişemezsiniz. Ağ kaynaklarına bir Telnet oturumundan erişmek için, kullanıcı adınız ile parolanızı yeniden vererek ağ sürücülerine erişmeniz gerekir.

NTLM, seçilen istemci kimlik doğrulaması modu olmayabilir. Bu durum, aşağıdaki istemcilerden birine sahip olduğunuzda ortaya çıkar: NTLM kullanma seçeneği olmayan, Windows tabanlı bir istemci, UNIX Telnet istemcisi.

Bu senaryoda, Telnet Sunucusu'nu çalıştıran bilgisayarın desteklediği tek farklı kimlik doğrulama yöntemi, kullanıcı adı/parola yöntemidir. Bu yöntemde, kullanıcı adı ve parola, sunucu tarafından kimlik doğrulaması için düz metin olarak gönderilir.

tlntadmn komutunu kullanarak, Telnet Sunucusu'nu çalıştıran bir yerel veya uzak bilgisayar yönetilebilir.

```
C:\>tlntadmn


localhost öğesine ait ayarlar aşağıdadır

Alt Tuşu 'CTRL+A' olarak eşlendi          :     YES
Boş oturum zaman aşımı                    :     1 hours
En Çok Bağlantı Sayısı                    :     2
Telnet bağlantı noktası                   :     23
En fazla başarısız oturum açma denemesi   :     3
Bağlantı kesildiğinde görevleri sonlandır :     YES
İşlem Modu                                :     Console
Doğrulama Düzenekleri                     :     NTLM, Password
Varsayılan Etki Alanı                     :     B779CD28E41A4D6
Bölge                                     :     Stopped

C:\>_
```

- **Telnet Sunucu çalıştıran bir bilgisayarı yönetme**

Sözdizimi

tlntadmn [\\UzakSunucu] [start] [stop] [pause] [continue] [-u KullanıcıAdı-p Parola]

Parametreler

\\ UzakSunucu

Yönetmek istediğiniz uzak sunucunun adını belirtir. Sunucu adı belirtmezseniz, yerel sunucu olduğu varsayılır.

start

Telnet Sunucu'yu başlatır.

stop

Telnet Sunucu'yu durdurur.

pause

Telnet Sunucu'yu keser.

continue

Telnet Sunucu'yu devam ettirir.

-u KullanıcıAdı -p Parola

Yönetmek istediğiniz uzak sunucunun yönetici kimlik bilgilerini belirtir. Yönetici kimlik bilgileriyle oturum açmadığınız bir uzak sunucuyu yönetmek isterseniz, bu parametre gereklidir.

/?

Komut isteminde yardımı görüntüler.

Telnet oturumlarını yönetme

Sözdizimi
tlntadmn [\\UzakSunucu] [-s] [-k{OturumNo | all}] [-m {OturumNo | all} "İleti"]

Parametreler

\\ UzakSunucu
Yönetmek istediğiniz uzak sunucunun adını belirtir. Sunucu adı belirtmezseniz, yerel sunucu olduğu varsayılır.
-s
Etkin Telnet oturumlarını görüntüler.

-k{OturumNo | all}
Oturumları bitirir. Belli bir oturumu bitirmek için oturum numarasını yazınız veya bütün oturumları bitirmek için all yazınız.

-m {OturumNo | all} "İleti"
Bir veya daha fazla oturuma ileti gönderir. Belli bir oturuma ileti göndermek için oturum numarasını yazınız veya bütün oturumlara ileti göndermek için all yazınız. Göndermek istediğiniz iletiyi tırnak işareti içine alarak ("İleti" şeklinde) yazınız.

/?
Komut isteminde yardımı görüntüler.

Yönettiğiniz ve tlntadmn komutunu kullandığınız bilgisayarların Windows NT, Windows 2000, Windows XP veya Windows Server 2003 ailesinden bir işletim sistemini çalıştırıyor olması gerekir. Bilgisayarlardan biri Windows NT veya Windows 2000 çalıştırıyorsa, aynı zamanda Windows Services for UNIX 2.0'ı da çalıştırmalıdır.

Tlntadmn komutunu kullanmak için yerel bilgisayara yönetici kimlik bilgileriyle oturum açmalısınız. Uzak bir bilgisayarı yönetmek için uzak bilgisayara ilişkin yönetici kimlik bilgilerini de sağlamalısınız. Bunu, hem yerel hem de uzak bilgisayara ilişkin yönetici kimlik bilgileri olan bir yerel bilgisayara oturum açarak yapabilirsiniz. Bu yöntemi kullanamazsanız, uzak bilgisayara yönetici kimlik bilgilerini sağlamak için -u ve -p parametrelerini kullanabilirsiniz.

2.3.8.2. Telnet İstemcisi

Telnet İstemcisi'ni kullanarak Telnet sunucu yazılımını çalıştıran uzak bir bilgisayara bağlanabilir ve konsol penceresini kullanarak o bilgisayarla etkileşime girebilirsiniz.

Telnet protokolü çok az güvenlik sağlar. NTLM kimlik doğrulamasının kullanılmadığı bir Telnet oturumunda, parolaları da içeren tüm veriler, istemciyle sunucu arasında düz metin olarak aktarılır. Telnet oturum trafiği güvenli olmadığı için, Telnet oturumu sırasında hiçbir hassas verinin gönderilmediğinden emin olmanız gerekir.

Telnet İstemcisi'nde iki işlem modu vardır: Telnet komut modu ve Telnet oturum modu. Telnet komut modu, Telnet terminalinin uzaktaki bir ana bilgisayarla bağlantı kurmasını, uzaktaki bir ana bilgisayarla bağlantısını kapatmasını, işletim parametrelerini görüntülemesini, terminal seçeneklerini belirlemesini, durumu yazdırmasını ve programdan çıkmasını sağlar.

Uzaktaki bir ana bilgisayara bağlandığında, Telnet İstemcisi Telnet oturum modundadır. Bu, en yaygın moddur. Oturum açtıktan sonra kullanıcılara bir Komut İstemi penceresi verilir. Kullanıcılar daha sonra, herhangi bir uzak Telnet sunusundaki karakter tabanlı uygulamaları, sisteme doğrudan bağlanmış gibi kullanabilir.

Bir ana bilgisayara bağlandıktan sonra, terminal ayarlarını değiştirmek için oturum modundan komut moduna dönebilirsiniz. CTRL +] tuşlarına basarak Telnet oturum modundan Telnet komut moduna geçebilir ve ENTER tuşuna basarak tekrar Telnet oturum moduna geçebilirsiniz.

Telnet Sunucusu'nu çalıştıran bilgisayara erişim sağlamak için, yerel Windows kullanıcı adınızı ve parolanızı veya etki alanı hesap bilginizi kullanabilirsiniz.

Kimlik doğrulaması için NTLM seçeneğini kullanmazsanız, kullanıcı adı ve parolası Telnet sunucusuna düz metin olarak gönderilir.

NTLM kimlik doğrulamasını kullanıyorsanız, Telnet İstemcisi, kimlik doğrulaması için Windows güvenlik içeriğini kullanır ve kullanıcının adını ve parolasını girmesi

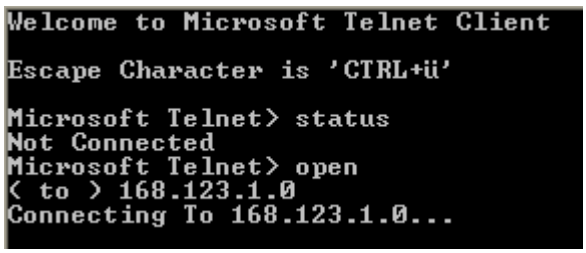
istenmez. Kullanıcı adı ve parolası şifrelenir.

Parola seçeneği için kullanıcının bir sonraki oturum açışında parolasını değiştirmesi gerekir değeri belirlenirse, NTLM kimlik doğrulama kullanılarak Telnet sunucusuna oturum açma girişimleri başarısız olur. Başarılı bir şekilde oturum açmak için doğrudan sunucuda oturum açmalı, parolanızı değiştirmeli ve daha sonra Telnet İstemcisi aracılığıyla açmalısınız.

NTLM kimlik doğrulaması kullanarak bir Telnet sunucusuna bağlanırsanız, NTLM kimlik doğrulamasının getirdiği sınırlamalardan dolayı bazı ağ kaynaklarına erişemezsiniz. Ağ kaynaklarına bir Telnet oturumundan erişmek için, kullanıcı adınız ile parolanızı yeniden vererek ağ sürücülerine erişmeniz gerekir.

Telnet komutları, Telnet protokolünü kullanan bir uzak bilgisayarla iletişim kurmanıza olanak verir. Telnet komut istemi (**Microsoft Telnet>**) tarafından belirtilen Telnet içeriğini girmek için, Telnet'i parametreler olmadan çalıştırabilirsiniz. Telnet komut isteminden aşağıdaki komutları kullanarak, Telnet İstemcisi'ni çalıştıran bir bilgisayarı yönetebilirsiniz.

Telnet İstemcisi komut istemi, aşağıdaki komutları kabul eder:

Komut	Açıklama
open	Ana bilgisayar ile bir Telnet bağlantısı kurmak için, **open** *ana bilgisayar adı* komutu kullanılır. 
close	Varolan bir Telnet bağlantısını kapatmak için **close** komutu kullanılır.
display	Telnet İstemcisi için geçerli ayarları görüntülemek için **display** komutu kullanılır.
gönderme	Telnet sunucusuna komut göndermek için **send** komutu kullanılır. Aşağıdaki komutlar desteklenir: **ao** Çıktı komutunu durdurur. **ayt** "Orada mısın?" komutu. **esc** Geçerli çıkış karakterini ayarlar. **ip** İşlem komutunu keser. **synch** Telnet synch (eşitleme) işlemini gerçekleştirir. **brk** Kesme sinyali gönderir. Yukarıda listelenen komutlar dışındaki her şey, Telnet sunucusuna bir dize olarak gönderilir. Örneğin, **send abcd** komutu, Telnet sunucusuna **abcd** dizesini gönderir, sunucu da bu dizeyi Telnet oturum penceresine yansıtır.
quit	Telnet İstemcisi'ni kapatmak için **quit** komutu kullanılır.
set	Telnet İstemcisi'ni geçerli oturum için yapılandırmak üzere, **set** komutunu aşağıdaki değişkenlerden biriyle kullanınız. **bsasdel** Geri tuşu, sil olarak gönderilir.

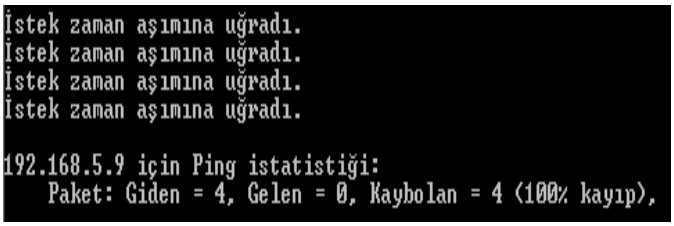
	codeset seçeneği Aynı kod kümesinin uzak bilgisayarda da ayarlanması gerekir. Varsayılan olarak, Telnet İstemcisi tarama yazı tipi kullanır. Bu kod kümelerinden birini kullanarak uzak bilgisayara erişmeden önce, karakterlerin düzgün şekilde görüntülenebilmeleri için, Telnet İstemcisi'ni bir TrueType yazı tipi kullanacak şekilde yapılandırmanız gerekir. **crlf** Yeni satır modu; RETURN tuşunun 0x0D, 0x0A göndermesine neden olur. **delasbs** Sil, geri tuşu olarak gönderilir. **Escape** *karakter* Telnet oturum modundan, Telnet komut moduna geçiş yapar. Telnet komut modundayken Telnet oturum moduna dönmek için, "Enter" tuşuna basınız. **localecho** Localecho'yu açar. **Logfile** *ad* Bu oturum için Telnet günlüğünün yazılacağı dosyanın adını belirtir. Dosyanın yolunu belirtmezseniz, dosya geçerli dizinde oluşturulur. Günlük dosyasının belirtilmesi, günlüğe kaydetmeyi de etkinleştirir. **mode** {**console** | **stream**} İşlem modu. **ntlm** NTLM kimlik doğrulamasını etkinleştirir. **term** {**ansi** | **vt100** | **vt52** | **vtnt**} Telnet İstemcisi'nin benzetim yapmasını istediğiniz terminal türü. **?** **set** için Yardım bilgileri görüntüler.
unset	Daha önce **set** komutu kullanılarak ayarlanan bir seçeneği kapatmak için **unset** komutu kullanılır.
status	Telnet İstemcisi'ni çalıştıran bilgisayarın bağlı olup olmadığını belirlemek için **status** konutu kullanılır.
?/help	Yardım bilgilerini görüntüler.

UYGULAMA FAALİYETİ

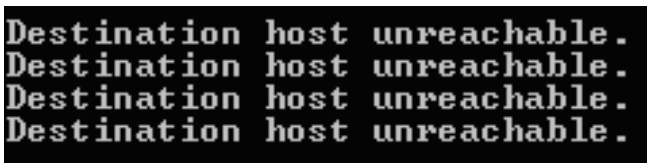
İşlem Basamakları	Öneriler
➢ Ağınızda bulunan kablo bağlantılarıyla, ağınızda bulunan araç gereçlerinin bağlantılarını kontrol ediniz.	➢ Ağınızda bozuk network kartları, yanlış bağlanmış portlar, uzun kablolar yüzünden yaşanan kırılmalar, bozuk T konnektörleri, sonradan kablo değişimi yapılarken yanlış kablo seçimi, kablonun manyetik alanlara maruz kalması, data prizlerinin çalışmaması gibi birçok sorun olabilir. Ağınızda bir problem var ise bu hataların alabileceğini var sayarak bunları kontrol ediniz. ➢ Ayrıca ağınızda bulunan yönlendiricinin doğru bağlı olup olmadığını, sisteme elektrik gelip gelmediğini, portlaın durumunu kontrol ediniz. 

➢ Test komutlarını kullanarak ağı test ediniz.	➢ Ping komutunu kullanarak kabloya kadar makinenin ağ açısından çalışır durumda olup olmadığını anlayabilirsiniz.
	➢ Ping komutunu kallandıktan sonra gelen cevapları dikkatlice inceleyiniz.
	`192.168.0.10 için Ping istatistiği:`
	`Paket: Giden = 4, Gelen = 4, Kaybolan = 0 (0% kayıp),`
	`Mili saniye türünden yaklaşık tur süreleri:`
	`En Az = 0ms, En Çok = 0ms, Ortalama = 0ms`

Yukarıdaki gibi bir mesaj alırsanız, paketler geri geliyor makine kablolama açısından çalışır durumdadır.



Yukarıdaki gibi bir mesaj alırsanız donanımsal bir problem var demektir. Kablolar, hublar, jak ve T konnektörler ölçü aleti ile kontrol edilmelidir.



Yukarıdaki gibi bir mesaj alırsanız gerekli gateway adresi düzgün girilmemiştir.

- Net Diag ile ağınızı kontrol ediniz. Net Diag ile protokolden bağımsız bir test yapılabilir.

Makinede ms-dos komut isteminde: net diag yazıp entera basılır.

Birden fazla protokol yüklü ise test için biri seçilir. Ağda halen çalışır halde bir net diag olup olmadığını sorulur, eğer N denilirse makineyı bir 'Diagnostic Server' haline getirir. Diğer makinelerde de komut çalıştırılır. Diğer sistem(ler)de de aynen net diag komutunu çalıştırılır.

Eğer network donanımı düzgün çalışıyorsa şimdi bu makine üzerindeki net diag, az önce diğer makine üzerinde çalıştırıp bıraktığımız 'Diagnostic Server' ı bulmalı, ancak bulamazsa (No diagnostic servers were detected on the network-yukarıdaki resim de bu mesajı bulun) yukarıdaki gibi mesaj verecektir. Bu durumda donanımsal bir problem var demektir.

- MS-DOS komut isteminde Ipconfig komutunu yazınız.

```
Bağlantıya özgü DNS Soneki .  . . :
IP Adres. . . . . . . . . . . . . : 192.168.2.2
Alt Ağ Maskesi. . . . . . . . . . : 255.255.255.0
Varsayılan Ağ Geçidi. . . . . . . : 192.168.2.1
```

Bilgisayar tarafından kullanılan IP yapılandırmasının ayrıntılarını görüntülemek ve değiştirmek için kullanabilirsiniz.

- Route komutunu kullanınız. Bu komut yerel IP yönlendirme tablosundaki girdileri görüntüler ve değiştirir. route, parametreler olmadan kullanıldığında yardımı görüntüler.

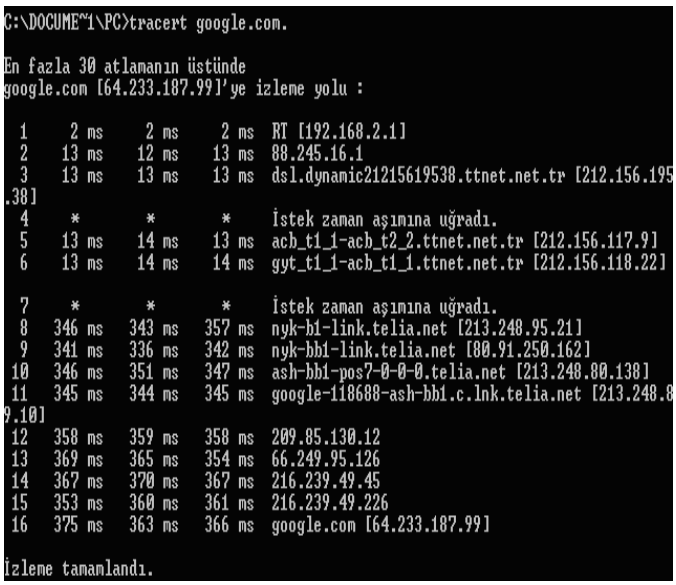
Route add ===> Bir yol ekler.
Route change ===> Var olan bir yolu değiştirir.
Route delete ===> Var olan bir yolu ya da yolları siler.
Route print ===> Var olan bir yolu ya da yolları yazdırır.

```
C:\DOCUME~1\PC>route print
===========================================================================
Arabirim Listesi
0x1 ........................... MS TCP Loopback interface
0x2 ...00 13 ce ba 09 3a ...... Intel(R) PRO/Wireless 2200BG Network Connection
 - Packet Scheduler Miniport
0x3 ...00 90 f5 44 cd 8d ...... Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Con
troller - Packet Scheduler Miniport
0x4 ...00 0d f0 1f 3b 12 ...... Bluetooth PAN Network Adapter - Packet Scheduler
 Miniport
===========================================================================
===========================================================================
Etkin Yollar:
       Ağ Hedefi      Ağ Maskesi      Ağ Geçidi       Arabirim   Ölçüt
         0.0.0.0          0.0.0.0    192.168.2.1    192.168.2.2      25
       127.0.0.0        255.0.0.0      127.0.0.1      127.0.0.1       1
     192.168.2.0    255.255.255.0    192.168.2.2    192.168.2.2      25
     192.168.2.2  255.255.255.255      127.0.0.1      127.0.0.1      25
   192.168.2.255  255.255.255.255    192.168.2.2    192.168.2.2      25
    192.168.50.0    255.255.255.0    192.168.50.1   192.168.50.1      30
    192.168.50.1  255.255.255.255      127.0.0.1      127.0.0.1      30
  192.168.50.255  255.255.255.255    192.168.50.1   192.168.50.1      30
       224.0.0.0        240.0.0.0    192.168.2.2    192.168.2.2      25
       224.0.0.0        240.0.0.0    192.168.50.1   192.168.50.1      30
 255.255.255.255  255.255.255.255    192.168.2.2    192.168.2.2      1
 255.255.255.255  255.255.255.255    192.168.50.1             3      1
 255.255.255.255  255.255.255.255    192.168.50.1   192.168.50.1      1
Varsayılan
Ağ Geçidi:           192.168.2.1
===========================================================================
```

- Tracert komutunu kullanınız.

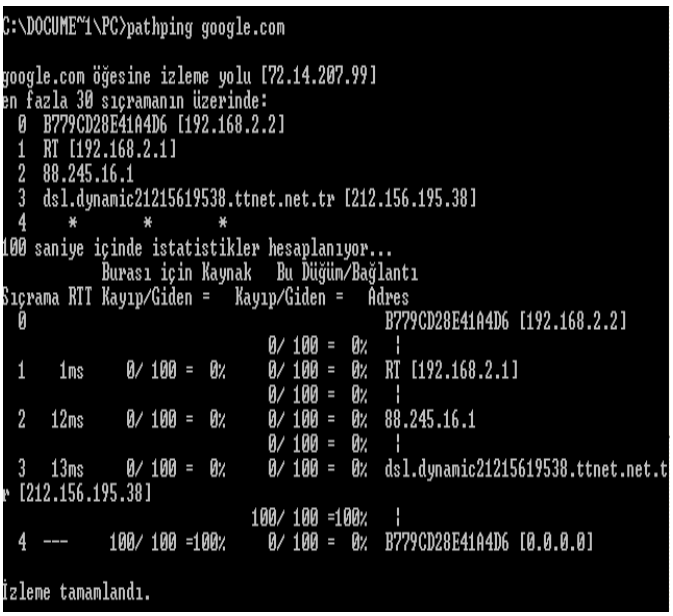
Bu komut sayesinde, farklı TTL süreleri kullanılarak aynı hedefe ICMP paketleri gönderilir. Bu sayede, bilgisayarınızdan bir başka hedef noktaya ulaşırken, paketlerimizin hangi yolları takip ettiği kontrol edilir. Bu komut ile hedef bilgisayar ve sizin aranızdaki en yakın ve en kısa yolu belirleyen router ların bir listesi gösterilmiş olur.

Örneğin;



- Pathping komutunu kullanınız.

Bu komut sayesinde yönlendiriciler üzeriden geçen verinin kayba uğrayıp uğramadığı kontrol edilir.

	Örneğin; 
➢ Telneti kullanrak ağı test ediniz.	Telnet yapıldığında, bağlanılan makinenin bir kopyası Telnet penceresi vasıtasıyla yerel makineye getirilmekte, dolayısıyla uzaktaki makinenin başındaymış gibi çalışmalar yapılabilmektedir. Bu sayede uygulama katmanının yazılımının doğru çalışıp çalışmadığı da testmiş olursunuz. Telnet test için geçerli bir mekanizmadır. Telnet gerçekleştirebilmek için sahip olunması gereken bilgiler: ➢ Bağlanılmak istenen konak (host) makinenin IP adresi veya adı, ➢ Buraya bağlanmakta kullanıla kullanıcı kodu, ➢ Kullanıcı şifresi,

ÖLÇME VE DEĞERLENDİRME

Bu faaliyet sonunda hangi bilgileri kazandığınızı, aşağıdaki soruları yanıtlayarak belirleyiniz.

ÖLÇME SORULARI

Aşağıdaki sorulardan; sonunda parantez olanlar doğru yanlış sorularıdır. Verilen ifadeye göre parantez içine doğru ise "D" , yanlış ise "Y" yazınız. Çoktan seçmeli sorularda ise doğru şıkkı işaretleyiniz.

1. Ping, Internet Control Message Protocol protokolünü kullanan bir uygulamadır. ( )

2. Uygunsuz seri arayüz yapılandırması 3. katmanın hatasıdır. ( )

3. Yönlendirme protokollerinin yanlış kullanılması 2. katman hatasıdır. ( )

4. Bir Windows makinesinden bir UNIX makinesına ping atılamaz. ( )

5. Net Diag ileTCP/IP protokolden bağımsız bir test yapılabilir. ( )

6. Telnet, ağ üzerindeki bir makineya uzaktan bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel addır. ( )

7. IP yönlendirme tablosunda *10.* ile başlayan yolları görüntülemek için aşağıdaki komutlardan hangisi kullanılır?

   A) route print
   B) route print 10.*
   C) route print 10*
   D) route 10.*

8. Yol üzerinde hangi yönlendiricilerin olduğunu belirleme konusunda tracert komutu ile aynı biçimde çalışan komut aşağıdakilerden hangisidir?

   A) netstat
   B) route
   C) ipconfig
   D) pathping

9. Bağlantı sorunları olduğunda ulaşılmak istenen hedef IP adresinin yolunu denetlemek için kullanılan komut aşağıdakilerden hangisidir?

A) route
B) tracert
C) ipconfig
D) netstat

10. Ana bilgisayar ile bir Telnet bağlantısı kurmak için, aşağıdaki komutlardan hangisi kullanılır?

A) start
B) tlntadmn
C) telnet
D) open

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz.

Bu öğrenme faaliyetini tam anlamıyla anladığınızı düşündüğünüzde Öğrenme Faaliyeti- 3'e geçiniz.

ÖĞRENME FAALİYETİ–3

AMAÇ

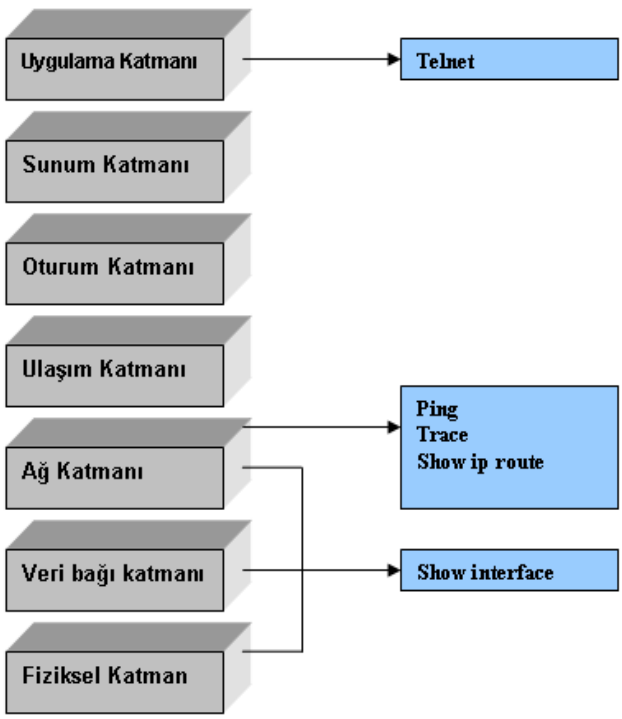
Yönlendirici komutları kullanarak sorun giderme işlemini yapabileceksiniz

ARAŞTIRMA

- Yönlendirici sorunlarını tespit etmek için kullanılan komutları araştırınız.
- Yönlendirici yapılanlandırma komutlarını gözden geçiriniz.

3. YÖNLENDİRİCİ SORUNLARINI TESPİT ETME

3.1. Yönlendirici Komutları ile Sorunları Test Etme



Şekil 3.1: Test komutları

Ağlarda meydana gelen en genel problem, adresleme problemidir. Bu yüzden adresi test etmek önemlidir.

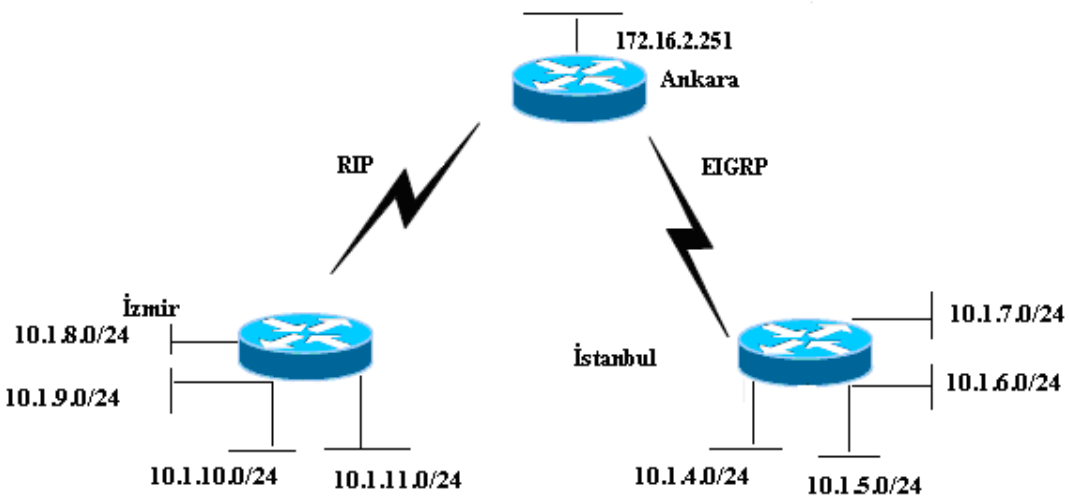
OSI modelinde ağ testi art arda ilerlemektedir. Her katmanda kullanılan test komutları vardır.

Telnet, ping, trace, show interface, show ip route ve debug ağı test etmeye izin veren komutlardır.

3.1.1. Yönlendirme Sorunlarını Tespit Etme

show ip route komutu, geniş bir ağdaki sorunları gidermeye çalıştığınızda, yardımcı olacak sayısız seçenek sunacaktır. Aynı bağlamda, **show ip protocol** komutu da, oldukça yardımcı olacaktır. Küçük bir ağ üzerinde çalışıyorsanız, **show ip route** komutunun birçok seçeneği işinize yaramayacaktır ancak, seçenekleri bilmek, ileride yardımcı olabilir.

Bu komutu bir örnekle açıklayalım:
Şekil 3.2'de örnek ağ gösterilmiştir. Bu örnekte, **İstanbul** ile **Ankara** arasında EIGRP ve **Ankara** ile **İzmir** arasında RIP-2 kullanılmıştır. Show ip route seçeneklerinin kullanılabilmesi için bu şekilde bulunan yönlendiricileri yapılandırmak gerekmektedir.



Şekil 3.2: show ip route komutunun seçeneklerinin kullanılabileceği örnek ağ

"show ip route" seçeneklerinin kullanılabilmesi için Ankara üzerinde yapılan konfigürasyon:

```
Ankara#show running-config
Current configuration : 964 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-ençryption
!
hostname Ankara
!
enable secret 5 $l$J3Fz$QaEYNIiI2aMu.3Ar.qOXm.
enable password friend
!
ip alt ağ-zero
no ip domain-lookup
!
interface SerialO
   no ip address
   no ip directed-broadcast
   encapsulation frame-relay IETF
   clockrate 56000
   frame-relay Imi-type cisco
!
interface SerialO.1 point-to-point
   ip address 172.16.3.251 255.255.255.0
   no ip directed-broadcast
   frame-relay interface-dlci 902
!
interface SerialO.2 point-to-point
   ip address 172.16.1.251 255.255.255.0
   no ip directed-broadcast
frame-relay interface-dlci 903
!
interface Seriall
   no ip address
   no ip directed-broadcast
   shutdown
!
interface EthernetO
   ip address 172.16.2.251 255.255.255.0
   no ip directed-broadcast
!
router eigrp 9
   passive-interface SerialO. 1
   network 172.16.0.0 no auto-summary
!
router rip
   version 2
   passive-interface SerialO.2
   network 172.16.0.0
   no auto-summary
!
ip classless
no ip http server
!
access-list 1 permit 10.0.0.0 0.255.255.255
```

"show ip route" seçeneklerinin kullanılabilmesi için İzmir üzerinde yapılan

konfigürasyon:

```
Izmir#show running-config
Currentconfiguration : 968 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Izmir
!
enable secret 5 $l$J3Fz$QaEYNIiI2aMu.3Ar.qOXm.
!
ip alt ağ-zero
no ip domain-lookup
!
interface SerialO
  no ipaddress
  no ip directed-broadcast
  encapsulation frame-relay IETF
  no fair-queue
  frame-relay Imi-type cisco
!
interface SerialO.1 point-to-point
  ipaddress 172.16.3.252 255.255.255.0
  no ip directed-broadcast
  frame-relay interface -d Ici 901
!
interface Seriall
no ip address
no ip directed-broadcast
shutdown
!
interface EthernetO
ip address 10.1.8.253 255.255.255.0
!
interface Ethernetl
ip address 10.1.9.253 255.255.255.0
!
interface Ethernet2
ip address 10.1.10.253 255.255.255.0
!
interface Ethernet3
ip address 10.1.11.253 255.255.255.0
!
router rip
  version 2
  network 10.0.0.0
  network 172.16.0.0
  no auto-summary
!
```

```
ip classless
no in http server
```

"show ip route" seçeneklerinin kullanılabilmesi için İstanbul üzerinde yapılan konfigürasyon:

```
Istanbul#show running-config
Current configuration : 960 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname İstanbul
!
enable secret 5 $i$33Fz$QaEYNIiI2aMu.3Ar.qOXm.
!
ip alt ağ-zero
no ip domain-lookup
!
interface SerialO
  no ip address
  no ip directed-broadcast
  encapsulation frame-relay IETF
  no fair-queue
  frame-relay Imi-type cisco
!
interface SerialO.l multipoint
  ip address 172.16.1.253 255.255.255.0
  no ip directed-broadcast
  ip summary-address eigrp 9 10.1.4.0 255.255.252.0
  frame-relay interface-dlci 901
!
interface Seriall
  no ip address
  no ip directed-broadcast
  shutdown
!
interface EthernetO
ip address 10.1.4.253 255.255.255.0
!
interface Ethernetl
ip address 10.1.5.253 255.255.255.0
!
interface Ethernet2
ip address 10.1.6.253 255.255.255.0
!
interface Ethernet3
ip address 10.1.7.253 255.255.255.0
!
router eigrp 9
```

```
  network 10.0.0.0
  network 172.16.0.0
  no auto-summary
!
ip classless
no ip http server
```

"show ip route" seçeneklerinin kullanılabilmesi için Ankara üzerinde yapılan konfigürasyon:

```
Ankara#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl -
OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll -
IS-IS level-1, L2 - IS-IS leveI-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic
downloaded static route

Gateway of last resort is not set

             172.16.0.0/24 is alt ağted, 3 alt ağs
C       172.16.1.0 is directiy connected, Serial0.2
C       172.16.2.0 is directiy connected, EthernetO
C       172.16.3.0 is directiy connected, SerialO.l
             10.0.0.0/8 is variably alt ağted, 5 alt ağs, 2 masks
R       10.1.11.0/24 [120/1] via 172.16.3.252, 00:00:17, SerialO.l
R       10.1.10.0/24 [120/1] via 172.16.3.252, 00:00:17, SerialO.l
R       10.1.9.0/24 [120/1] via 172.16.3.252, 00:00:17, SerialO.l
R       10.1.8.0/24 [120/1] via 172.16.3.252, 00:00:17, SerialO.l
D    10.1.4.0/22 [90/2185984] via 172.16.1.253, 00:28:01,Serial0.2

Ankara#show ip route ıgrp

Ankara#show ip route eigrp
10.0.0.0/8 is variably alt ağted, 5 alt ağs, 2 masks
D 10.1.4.0/22 {90/2185984J via 172.16.1.253, 00:29:42, Serial0.2

Ankara#show ip route connected
 172.16.0.0/24 is alt ağted, 3 alt ağs
C 172.16.1.0 is directly connected, Serial0.2
C 172.16.2.0 is directly connected, EthernetO
C 172.16.3.0 is directly connected, SerialO.l

Ankara#show ip route summarv

Route Source      Networks    Alt ağs     Overhead    Memory (bytes)
connected            0           3          156          420
static               0           0          0            0
rip                  0           4          208          560
eigrp 9              0           1          52           140
```

```
internal              2                                  2320
Total                 2           8          416         3440

Ankara#show ip route supernet
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EİGRP erternal, O - OSPF, IA - OSPF inter area
Nl - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
El - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, Ll - IS-IS level-1, L2 - IS-IS level-2,
* - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
```

"Show ip route" komutu hakkında yardım almak için aşağıdaki komut kullanılabilir.

```
Ankara#show ip route ?
Hostname or A.B.C.D Network to display information about orhostname
Bgp                 Border Gateway Protocol (BGP)
Connected           Connected
Egp                 Exterior Gateway Protocol (EGP)
Eigrp               Enhanced Interior Gateway Routing Protocol (EIGRP)
İgrp                Interior Gateway Routing Protocol (IGRP)
İsis                ISO IS-IS
List                IP Access list
Mobile      Mobile routes
Odr                 On Demand stub Routes
Ospf                Open Shortest Path First (OSPF)
Profile     IP routing table profile
Rip                 Routing information Protocol (RIP)
Static      Static routes
Summary             Summary of ali routes
supernets-only      Show supernet entries only
vrf                 Display routes from a VPN Routing/Forwarding
instance
I                       Output modifiers
```

"Show ip route ?" komutu kullanılarak seçeneklerin listelendiğini görüyorsunuz. Bu seçeneklerden bazılarının kullanımına örnekler verilmiştir. Show ip route komutunun çıktısını sınırlandırarak sadece belli bir protokol tarafından öğrenilen yol bilgilerinin listelenmesini sağlayabilirsiniz. Benzer şekilde, çıktıyı sadece yeni bağlanan yollan gösterecek şekilde kısıtlamak da mümkündür.

```
Ankara#show ip route 10.1.5.8
Routing entry for 10.1.4.0/22
Knoyvn via "eigrp 9", distance 90, metrik 2185984, type internal
Redistributing via eigrp 9
Last update from 172.16.1.253 on Serial0.2, 00:28:36 ago
 Routing Descriptor Blocks:
* 172.16.1.253, from 172.16.1.253, 00:28:36 ago, via Serial0.2
Route metrik is 2185984, traffic share count is 1
```

```
Total delay is 20630 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes Loading 1/255, Hops 1

Ankara#show ip route rip
10.0.0.0/8 is variably alt ağted, 5 alt ağs, 2 masks
R 10.1.11.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
R 10.1.10.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
R 10.1.9.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
R 10.1.8.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
```

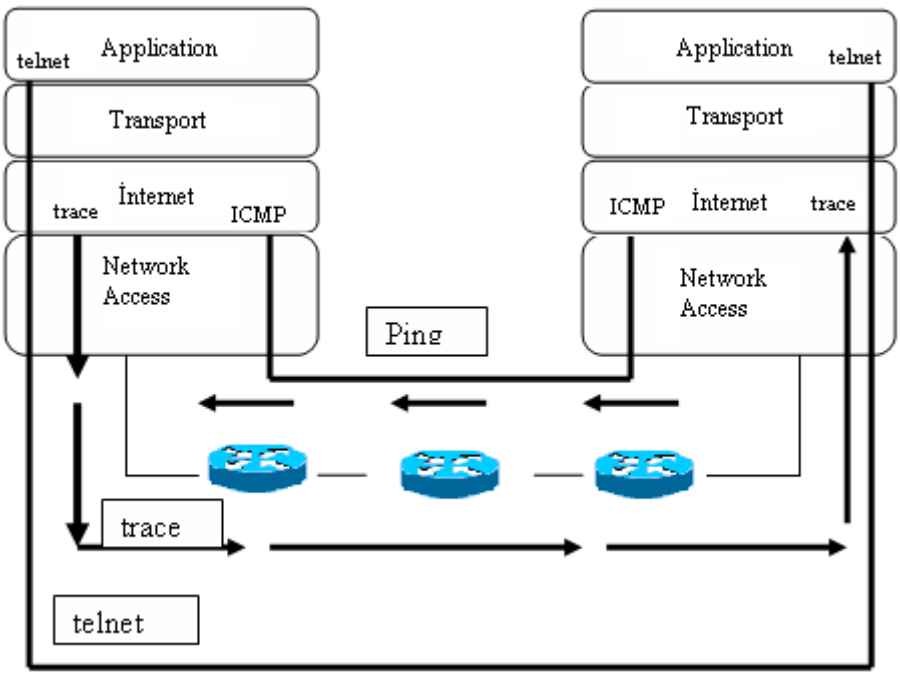
"Show ip route" komutu ile ilgili seçeneklerin en önemlileri arasında, son parametre olarak bir IP adresinin geçirilmesi vardır. Bu sayede router'a, belirtilen adrese gidecek bir paket için yapacağına benzer bir yönlendirme tablosu incelemesi yaptırılır. **Show ip route 10.1.5.8** komutu bir takım mesajlar üretir. Bunlardan ilki, yönlendirme tablosunda eşleşen yol bilgisinin 10.1.4.0/22 olduğunu belirtir. Eşleşen yolun listelenmesi sayesinde, router'ın özel bir IP adresine hangi yolu kullanarak erişeceğini öğrenmiş olursunuz.

```
Ankara#show ip route list 1
10.0.0.0/8 is variably alt ağted, 5 alt ağs, 2 masks
R 10.1.11.0/24 [120/1] via 172.16-3.252, 00:00:22, SerialO.l
R 10.1.10.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
R 10.1.9.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
R 10.1.8.0/24 [120/1] via 172.16.3.252, 00:00:22, SerialO.l
D 10.1.4.0/22 [90/2185984] via 172.16.1.253, 00:29:58, Serial0.2
```

Son olarak, büyük ağlarda oldukça kullanışlı olan bir diğer özellik gösterilmiştir. Bu özellik, komutun çıktısının bir izin listesine bağlı olarak filtrelendirilmesini sağlar. Verilen kodalar arasında "**show ip route list 1"** komutuna dikkat edin. İzin listesi 1, sadece 10.0.0.0 ağı ile ilgili yol bilgilerinin eşlenmesini sağlayacak şekilde konfigüre edilmiştir. Diğerleri, görmezden gelinecektir. İzin listesi referans olarak kullanılarak, show ip route komutunun çıktısı filtrelenir ve yollardan sadece bir kısmı görüntülenmiş olur. Bu özellik, yönlendirme tablosunda birçok kayıt bulunduğu zamanlarda olukça kullanışlıdır.

3.1.2. Katman Bağlantılarını Test Etmek

Bağlantı kontrolü için kullanılan komutlar, ping, telnet, trace'dir.



Şekil 3.3: Bağlantı kontrolü İçin kullanılan komutlar

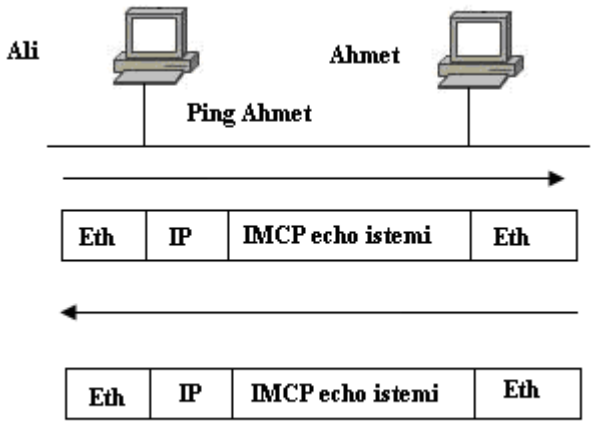
3.1.2.1. Ping Komutu

Ping komutu ağ bağlantısını test eder. Uçtan uca bağlantı olup olmadığını kontrol eder. Ping *(Packet INternet Gropher),* ICMP echo request (ICMP yankı istemi) adı verilen bir mesajı bir başka IP adresine gönderen, ICMP (Internet Control Message Protocol) protokolünü kullanır. Echo request'i içindeki IP adresine sahip olan bilgisayar, geriye bir ICMP echo yanıtı göndermelidir.

ICMP echo request mesajlarının, sesin yankılanmasına benzediğini düşünebilirsiniz. Bu mesajlar ağ üzerinde dolaşır ve taşımakta olduğu IP adresi ile eşleşen bir makineye ulaştığında, geriye dönerek aranan IP'ye ulaşıldığını belirtir.

Komut çalıştırıldığında aldığınız yanıt olumlu ise, problem büyük bir ihtimalle uygulama ile ilgilidir. ICMP, hiçbir uygulamaya bağımlı olmadan, IP üzerinden bağlanılabirliği yani, OSI modelinin 1, 2 ve 3. katmanlarını test eder.

Şekil 3.4 Temel süreci göstermektedir.



Şekil 3.4: Örnek ağ, ping komutu

Ping komutu uygulandığında bazı işaretler ekranda görüntülenecektir. Bu işaretlerin belli anlamları bulunmaktadır:

İşaret	Açıklama
!	ICMP yankı cevabı alındı.
.	Hiçbir şey alınmadı.
?	Bilinmeyen bir paket alındı.
M	Parçalanamaz ICMP mesajı alındı.
Q	Kaynağın data gönderme hızını yavaşlatması için ICMP mesajı alındı. (Source Quench)
N	Hedef ağa ulaşılamıyor ICMP mesajı alındı.
U	Hedef bilgisayara ulaşılamıyor mesajı alındı.
P	Hedef bilgisayarın portuna ulaşılamıyor mesajı alındı.

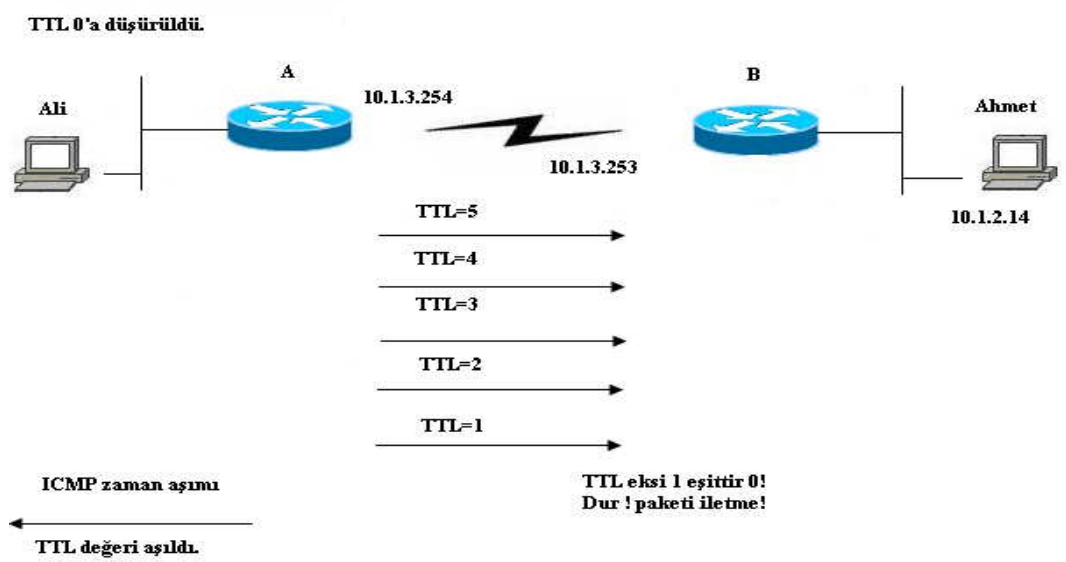
Tablo3.1: Ping işaretleri

```
Router> ping 172.16.101.1 –ip adresi bilinmiyorsa DNS ismi yazılmalıdır.
Type escape sequence to abort
Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:
 Rastgele üretilmiş 100 bytelık 5 paket          cevap zamanı. 2 saniye içinde cevap gelmese ağa
                                                 ulaşılamıyor anlamındadır.
!!!!! – Burada 1 tane '!'görsek bile yeterli ama bu networkün yoğun olduğunu gösterir.

Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms
                %80 başarılı                     paketlerin gidiş süreleri
Router>
```

3.1.2.2. Trace Komutu

Ağın üzerinde bir uçtan diğer uca varana kadar her noktayı kontrol eder. Aşamalı kontroldür yani basamak basamak kontrol yapar bu da en fazla 15 basamak olur. ICMP protokolü içerisinde kullanılan bir komuttur.

ICMP Zaman Aşımı mesajı, makineye göndermiş olduğu paketin zaman aşımı nedeniyle hedefine ulaştırılamadığını bildirmek için kullanılır. Aslında paketler için zaman tutulmaz ancak paketlerin router'lar arasında sonsuz döngüye girmelerini engellemek için her IP başlığı bir TTL (Time to Live) alanı kullanır. Router'lar TTL alanındaki değeri bir paketi ilettiklerinde azaltırlar. Router'lardan herhangi biri bu alandaki değeri 1 eksilttiğinde değer 0 olursa, paketi düşürür (iletmez). Bu, paketlerin router'lar arasında sonsuza kadar dolaşmasını engeller. Şekil 3.5 bu süreci göstermektedir.

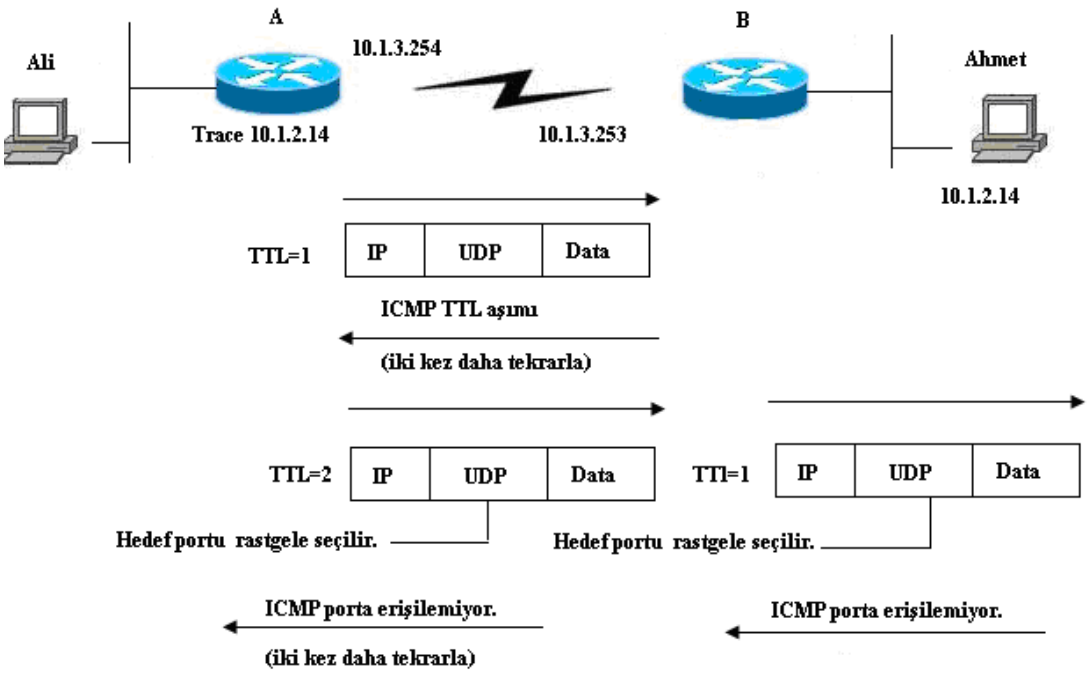


Şekil 3.5:TTL sıfır olacak şekilde azaltılır.

Şekilde gördüğünüz gibi, router paketi düşürür (atar) ve "zaman aşımı" kodu ile bir ICMP Zaman Aşımı mesajı gönderir. Bu sayede gönderici, paketin iletilemediğini öğrenir. Bir zaman aşımı mesajı almanız, ağdaki sorunların çözümünde size yardımcı olabilir. Bu mesajlar ile çok sık karşılaşmanız, yönlendirme problemleri yaşadığınız anlamına gelir.

IOS trace komutu, Zaman Aşımı mesajını ve IP TTL alanını kendi amaçları için kullanır. TTL alanı 1 yapılmış bir IP paketi gönderilerek (UDP İletim katmanı ile birlikte), yol üzerindeki ilk router'ın bir ICMP Zaman Aşımı mesajı göndermesi sağlanır. Router TTL değerini bir azalttığında, değer sıfır olacağından bir zaman aşımı mesajı gönderecektir. Trace komutu, router'dan gelen zaman aşımı mesajını inceleyerek, mesajı gönderen router'ın IP adresini öğrenir, (trace komutu genellikle TTL=1 olan üç paket gönderir) bunun ardından, trace komutu tarafından TTL=2 olan üç IP paketi daha gönderilir. Bu mesajlar, yol üzerindeki ilk router tarafından iletilecek ancak ikinci

router'a gelindiğinde TTL değeri 0 olacağından, ikinci router bir zaman aşımı mesajı gönderecektir. Aynı süreç izlenerek yol üzerindeki router'ların IP adresleri öğrenilecektir, trace komutu tarafından gönderilen orijinal paketler, kullanılma ihtimali oldukça düşük olan bir hedef port numarası kullanır. Bu sayede, hedef makine "Porta Erişilemiyor" mesajı döndürür. ICMP Porta erişilemiyor mesajı, paketlerin doğru hedefe zaman aşımı olmadan ulaştığını belirtir. Bu sayede "trace" komutu paketlerin doğru noktaya iletildiğini bilir. Şekil 3.6 süreci özetlemektedir. Bu şekilde Router A, trace komutunu kullanarak Ahmet'te giden bir yol bulmaya çalışmaktadır. Örnekte, Router A üzerindeki bu trace komutunu ve Router B'deki Zaman Aşımı mesajlarını göstermektedir.



Şekil 3.6:Cisco IOS yazılımı trace komutu

Router A'da "trace" komutu çalıştırıldığında Router B'de ICMP derleme sonuçları:

```
RouterA#trace 10.1.2.14
Type escape sequence to abort. Tracing the route to 10.1.2.14
1 10.1.3.253 8 msec 4 msec 4 msec -1. basamak
2 10.1.2.14 12 msec 8 msec 4 msec -2. basamak
RouterA#
```

Router B de ICM derleme sonuçları

```
RouterB#
ICMP:time exceeded(time to live)sent to 10.1.3.251 (dest was 10.1.2.14)
ICMP:time exceedecl(time to live)sent to 10.1.3.251 (dest was 10.1.2.14)
ICMP:time exceeded(time to live)sent to 10.1.3.251 (dest was 10.1.2.14)
```

Trace komutu uygulandığında bazı hata mesajları ekrana gelebilmektedir.

İşaret	Açıklama
*	zaman aşımı (süre içinde cevap gelmediyse)
!H	Paket karşı taraftan alındı fakat geri bildirim gelmedi.
N	Ağa ulaşılamadı.
U	Porta Ulaşılamadı.
P	Protokole Ulaşılamadı.

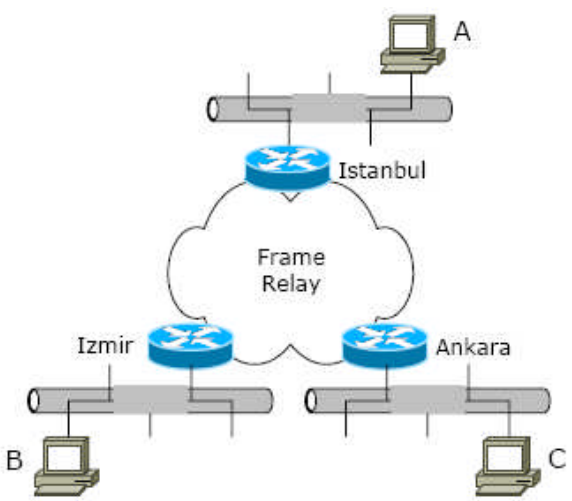
Tablo 3.2 :Hata mesajları

3.1.2.3. Telnet

Ağınızda birden fazla anahtar ve yönlendirici bulunuyorsa bütün bu ağ cihazlarının yönetimi için telnet uygulaması kullanılmaktadır. IOS telnet sunucuyu çalıştırmaktadır. Eğer bilgisayarınızdan yönlendirici ve anahtarlara telnet ile bağlanacaksanız aynı anda birden fazla pencere açıp bu cihazlara bağlanıp konfigürasyon yapabilirsiniz.

Şekil 3.7'de görüldüğü gibi önce C bilgisayarından Ankara yönlendiricisine telnet bağlantı kuralım. Ankara yönlendiricisine telnet ile bağlı bulunduğumuz halde İstanbul yönlendiricisine telnet ile bağlanalım. Daha sonra İstanbul yönlendiricisine yapmış olduğumuz bağlantıyı askıya alarak İzmir yönlendiricisine telnet ile bağlanalım. Telnet bağlantılarını CTRL+SHIFT+6 ve X tuşlarını hep birlikte kullanarak askıya alabilirsiniz. Bir telnet oturumu askıya alındıktan sonra, enter'a basıldığında en son askıya alınmış telnet bağlantısı devam etmektedir.

Telnet ile bağlı olduğunuz yönlendiricinin telnet bağlantılarını show sessions veya where komutlarıyla öğrenebilirsiniz. Telnet bağlantılar disconnect komutuyla kesilmektedir. Ayrıca askıya alınmış mevcut telnet bağlantıları tekrar aktif hale getirmek için resume komutu kullanılmaktadır.



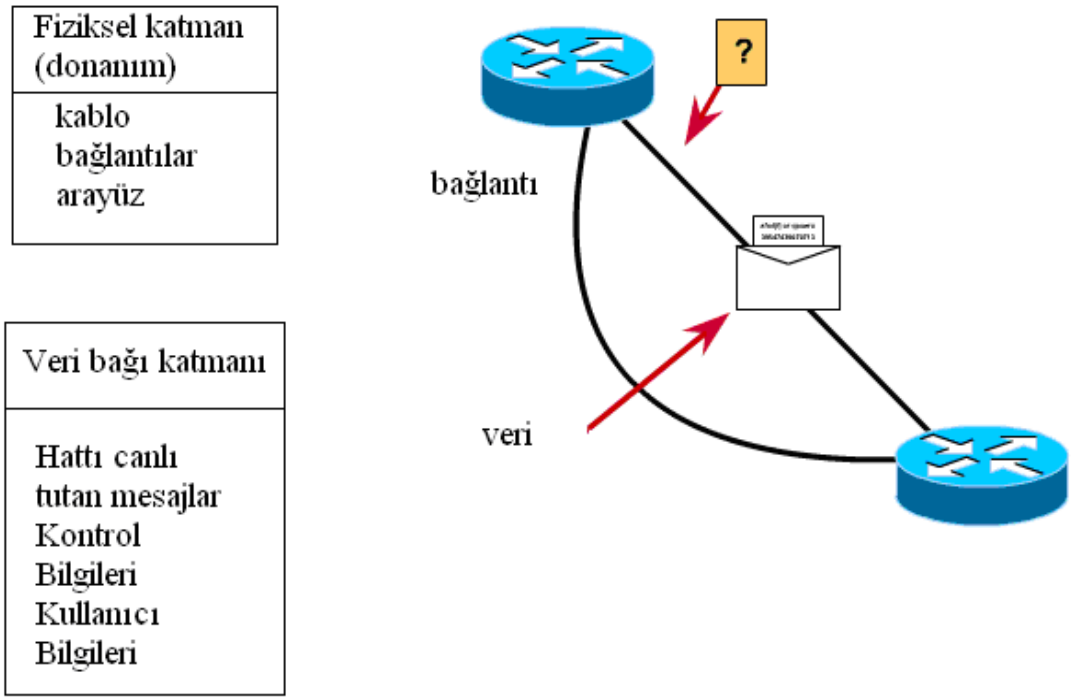
Şekil 3. 7: Örnek bir ağ şeması

```
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'
Microsoft Telnet>telnet Ankara
Trying Ankara (10.0.3.1)... Open
User Access Verification
Password:
Ankara>enable
Password
Ankara#telnet Istanbul
Trying Istanbul (10.0.4.1)… Open
User Access Verification
Password:
Istanbul>
Istanbul>
(Note: User pressed CTL-SHIFT-6, then x)
Ankara#telnet Izmir
Trying NewYork (10.0.4.2)… Open
User Access Verification
Password:
Izmir>
Izmir>
(Note: User pressed CTL-SHIFT-6, then x)
Ankara#show sessions
Conn    Host      Address    Byte   Idle    Conn Name
 1     Istanbul  10.0.4.1     0      0       Istanbul
*2     Izmir     10.0.4.2     0      0       Izmir
Ankara#where
Conn    Host      Address    Byte   Idle    Conn Name
 1     Istanbul  10.0.4.1     0      0       Istanbul
*2     Izmir     10.0.4.2     0      0       Izmir
Ankara#resume 1
[Resuming connection 1 to Istanbul … ]
Istanbul>
Istanbul>
(Note: User pressed CTL-SHIFT-6, then x)
Ankara#(Enter Tuşuna basıldı)
[Resuming connection 1 to Istanbul … ]
Istanbul>
Istanbul>
(Note: User pressed CTL-SHIFT-6, then x)
Ankara#disconnect 1
Closing connection to Istanbul [confirm]
Ankara#(Enter Tuşuna basıldı)
[Resuming connection 2 to Izmir … ]
Izmir>
Izmir>
(Note: User pressed CTL-SHIFT-6, then x)
Ankara#disconnect 2
Closing connection to Izmir [confirm]
Ankara#
```

Şifre girildikten sonra Ankara üzerinde komutlarla çalışılabilir.

3.1.3. Kabloları ve Paketleri Test Etmek

Fiziksel katmandaki kabloları, bağlantıları, arayüzleri, veri bağı katmanındaki donanım adreslerini, alıp gönderilen paket miktarını, kullanıcı bilgilerini ve kaydedilen hataları kontrol etmek amacıyla "show interface" komutundan yararlanılır.



Şekil :3.8

Fiziksel Katman ve veri bağı katmanının test etmek istediğinizde aşağıdaki soruları sormalısınız:

- Hatta sinyal taşınıyor mu?
- Veri bağı katmanı cihazları düzgün çalışıyor mu?
- Hattı canlı tutan mesajlar alınıyor mu?
- Veri paketleri gönderilebiliyor mu?

Bu soruların yanıtını show interfece komutu kullanılarak alınabilir.

```
Router# show int s 1
Serial is up , line protokol is up

Hardware is cxBus serial
Description 56Kb Line San Jose –Mp
```

Serial is up , line protokol is up -Kablo ve Ethernet kartı çalışıyor, Hat canlı (Kullanıma hazır.)
Serial is up , line protokol is down - Bağlantı problemi var. Kablo çalışıyor fakat hat canlı değil.
Serial is down , line protokol is down -Arayüz problemi var.Diğer arayüzler kapalı olabilir.
Serial is administratively down , line protokol is down -Bağlantı yok. Arayüzler shutdown komutuyla kapatılmış.

```
Router#show interface serial 0
Serial0 is up, line protocol is up
Internet address is 10.0.5.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:05, output 00:00:04, output hang never
Last clearing of “show interface” counters never
Queuing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
     273 packets input, 18621 bytes, 0 no buffer
     Received 215 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     309 packets output, 20175 bytes, 0 underruns
     0 output errors, 0 collisions, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     149
     DCD=up DSR=up DTR=up RTS=up CTS=up
```

3.1.3. CDP (Cisco Keşif Protokolü-Cisco Discovery Protocol)

CDP, komşu cihazların şifrelerini bilmeye gerek kalmadan, komşu router ve switch’ler hakkında temel bilgilerin elde edilmesini sağlar. CDP, LAN, HDLC, Frame Relay ve ATM arabirimlerini destekler. CDP, SNAP başlıklarının kullanımını destekleyen tüm arabirimleri destekler. Router ya da switch’ler, komşu router’ların Katman 2 ve Katman 3 adresleme detaylarını, Katman 3 protokolünü konfigüre etmeden öğrenebilirler-bu, CDP’nin Katman 3 protokollerine bağlı olmaması sayesinde gerçekleştirilir.

CDP, komşu cihaz hakkında çeşitli kullanışlı bilgiler edinir:

Cihaz tanımlayıcısı—Genelde makine ismi

Adres listesi—Ağ ve veri bağlantı adresleri

Port tanımlayıcısı—Arabirim için kullanılan bir başka isim olan portu tanımlayan metin bilgisi.

Yetenekler Listesi—Cihazın hangi tipte olduğu (router ya da switch) hakkında bilgi.

Platform—Cihazın modeli ve işletim sisteminin sürümü

CDP varsayılan konfigürasyonda etki durumdadır, **no cdp run** global komutu, CDP'yi kapatır, **cdp run** global komutu ise CDP kullanımını yeniden etkin konuma getirir. Benzer şekilde, **no cdp enable interface** alt komutu, CDP'yi komutun kullanıldığı arabirimde kapatırken, **cdp enable** komutu CDP'yi yeniden etkin hale getirir.

CDP protokolünün edindiği bilgileri görüntülemek için bazı komutlar kullanılmaktadır. **Show cdp neighbor** komutuyla komşulukta bulunan cihazların genel bilgilerini görüntülersiniz. **Show cdp entry** (cihaz host adı) komutuyla da belli bir cihazın detay bilgilerini görüntülersiniz. **Show cdp neighbor detail** komutuyla komşulukta bulunan cihazların detay bilgilerini görüntülersiniz. **Show cdp interface** komutuyla bağlı olduğunuz cihazın ara yüzleri ve cdp mesajları hakkında bilgi alırsınız. **show cdp traffic** komutuyla cdp trafiği ile ilgili istatistikleri görüntülersiniz.

```
Istanbul#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
S - Switch, H - Host, I - IGMP, r – Repeater
Device ID    Local Intrfce  Holdtme Capability  Platform     Port ID
Ankara        Ser 1         172     R           2500        Ser 1
Izmir         Ser 0.2       161     R           2500        Ser 0.1

Istanbul#show cdp entry Ankara
Device ID: Ankara
Entry address(es):
IP address: 163.5.8.3
Platform: cisco 2500, Capabilities: Router
Interface: Serial1, Port ID (outgoing port): Serial1
Holdtime : 168 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE
SOFTWARE (fc1)
Copyright 1986-1999 by Cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Istanbul#show cdp neighbor detail
Device ID: Ankara
Entry address(es):
IP address: 163.5.8.3
Platform: cisco 2500, Capabilities: Router
Interface: Serial1, Port ID (outgoing port): Serial1
Holdtime : 164 sec
Version :
Cisco Internetwork Operating System Software
```

```
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE
SOFTWARE (fc1)
Copyright 1986-1999 by Cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Device ID: Izmir
88
Entry address(es):
IP address: 10.1.5.252
Novell address: 5.0200.bbbb.bbbb
Platform: cisco 2500, Capabilities: Router
Interface: Serial0.1, Port ID (outgoing port): Serial0.1
Holdtime : 146 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE
SOFTWARE (fc1)
Copyright 1986-1999 by Cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Istanbul#show cdp interface
Ethernet0 is up, line protocol is down
Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial0.1 is up, line protocol is up
Encapsulation FRAME-RELAY
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial1 is up, line protocol is up
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

Istanbul #show cdp traffic
CDP counters :
Packets output: 41, Input: 21
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid packet: 0, Fragmented: 0
```

3.1.4. Debug Komutu

Debug komutu, router'da karşılaşacağınız problemlerin sebebini anlamak için kullanacağınız teşhis araçlarından birisidir. Debug, IOS içindeki çeşitli noktalarda, IOS'un neler yapmakta olduğunu açıklayan mesajlar üretilmesini sağlar.

Dikkat: Bazı debug seçenekleri, IOS'un işleyemeyeceği kadar fazla sayıda mesaj üretilmesine sebep olarak, IOS'un çökmesine sebep olabilir.

no debug all komutu tüm debug seçeneklerini kapatır. Daha önceden kullanmadığınız bir debug seçeneğini aktif hale getirmeden önce, no debug all komutunu

kullanınız. Ardından, debug seçeneğini aktif hale getiriniz. Böylelikle, çok fazla sayıda mesajla karşılaşmaya başladığınızda, no debug all komutunu hızlı bir şekilde kullanabilirsiniz. Mesajlar fazlalaştığında, "Enter" tuşuna bastıktan sonra, no debug all komutunu çalıştırarak, router'ın çökmesini engellemeye çalışınız.

Debug ip packet komutu ile yönlendirici üzerinden geçen IP paketleri hakkında bilgi alınabilmektedir.

Debug ip rip komutun uygulandığı sürece alınan ve gönderilen RIP mesajlarının logları görüntülenir.

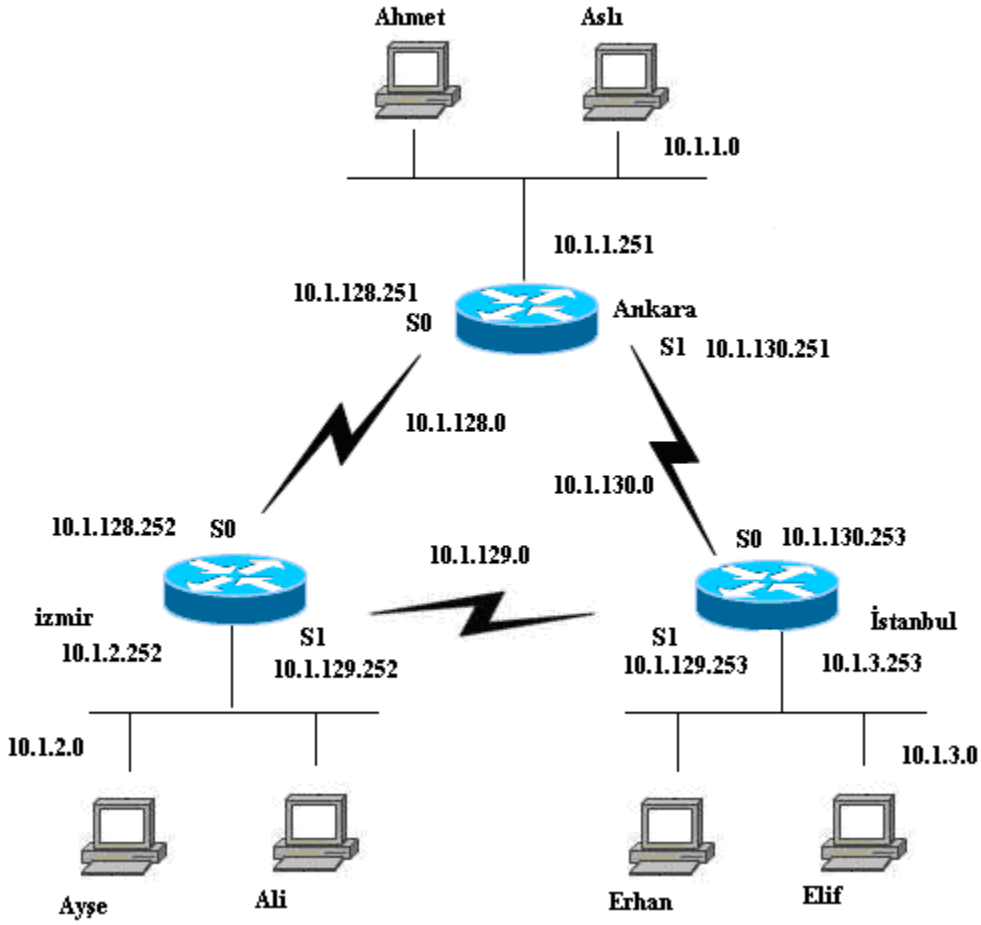
Debug ip igrp transactions komutun uygulandığı sürece alınan ve gönderilen IGRP mesajlarının logları görüntülenir.

debug ip igrp events komutun uygulandığı sürece alınan ve gönderilen her IGRP paketinin logları görüntülenir.

3.1.5. Örnek Bir Ağı Test Etmek

Şekil 3.9 her birinde iki seri bağlantı ve bir Ethernet bulunan üç yönlendirici bulunmaktadır. Yapılandırma aşağıdaki detaylar göz önüne alınarak yapılmıştır.

- 10.1.1.100 ve 10.1.2.100 adreslerindeki isim sunucuları kullanıldı.
- Router'ların IP adresleri bağlı oldukları alt ağ içindeki geçerli son birkaç IP adresinden biri olmalıdır, maske olarak 255.255.255.0 adresini kullanıldı.



Şekil 3.9: Noktadan noktaya seri bağlantılar ile bağlanmış olan üç router kullanan örnek ağ

Ankara Router'ının konfigürasyonu ve komutlar çalıştırıldığında elde edilen çıktılar:

```
Ankara#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ankara(config)#interface serial 0
Ankara(config-if)#ip address 10.1.128.251 255.255.255.0
Ankara(config)#interface serial 1
Ankara(config-if)#ip address 10.1.130.251 255.255.255.0
Ankara(config)#interface ethernet 0
Ankara(config-if)#ip address 10.1.1.251 255.255.255.0

Ankara#show running-config Building configuration...
Current configuration : 872 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Ankara
!
enable secret 5 $l$J3Fz$QaEYNIiI2aMu.3Ar.qOXm.
!
!
ip name-server 10.1.1.100
ip name-server 10.1.2.100
!
interface Serial 0
ip address 10.1.128.251 255.255.255.0
!
interface Seriall
ip address 10.1.130.251 255.255.255.0
!
interface EthernetO
ip address 10.1.1.251 255.255.255.0
!
no ip http server
banner motd ^C
Should’ve taken a left turn here! ThisTs Ankara... ^C
!
line con 0
   password cisco
   log in
line aux 0
line vty 0 4
password cisco
log in
!
End

Ankara#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP erternal, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll -
IS-IS level-l, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic
downloaded static route

Gateway of last resort is not set
10.0.0.0/24 is alt ağted, 3 alt ağs
C 10.1.1.0 is directly connected, EthernetO
C 10.1.130.0 is directly connected, Seriall
C 10.1.128.0 is directly connected, SerialO

Ankara#terminal ip netmask-format decimal
Ankara#show ip route
Codes:
```

```
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll -
IS-IS level-l, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic
downloaded static route

Gateway of last resort is not set

10.0.0.0 255.255.255.0 is alt ağted, 3 alt ağs
C 10.1.1.0 is directly connected, EthernetO
C 10.1.130.0 is directly connected, Seriall
C 10.1.128.0 is directly connected, SerialO
Ankara#
```

Şekil 3.9'da, gösterilen arabirimler için IP adresleri seçilmiştir, daha sonra, IP adreslerini konfigüre etmek için konfigürasyon modu seçilmiştir. Show running-config komutu, konfigürasyonun sonuçlarını ve daha önceden konfigüre edilmiş bazı detayları göstermektedir.

"Show" komutları sonucunda elde edilen alt ağ maskesi örnek gösterimini kullanmaktadır. Örneğin, 10.1.4.0/24 24 ağ ve alt ağ biti olduğunu ve bu alt ağ düzenlemesinde makine bitleri için 8 bit bırakıldığını belirtmektedir, terminal ip netmask komutu, görüldüğü gibi oturum boyunca biçimlendirmenin daha farklı şekilde gösterilmesini sağlamak için kullanılabilir.

İzmir Router'ının konfigürasyonu ve komutlar çalıştırıldığında elde edilen çıktılar:

```
Izmir#show running-config Building configuration...
Current configuration : 867 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Izmir
!
enable secret 5 $l$J3Fz$QaEYNIiI2aMu.3Ar.qOXm.
!
!
ip name-server 10.1.1.100
ip name-server 10.1.2.100
!
interface SerialO
ip address 10.1.128.252 255.255.255.0
no fair-queue
!
interface Seriall
```

```
ip address 10.1.129.252 255.255.255.0
!
interface Ethernet0
ip address 10.1.2.252 255.255.255.0
!
no ip http server

banner motd ^C
This is the Rootin-est Tootin-est Router in these here parts!
^C
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
End

Izmir#show ip interface brief
interface    IP-Address       OK?       Method Status Protokol
Serial0      10.1.128.252     YES       manual up up
Serial1      10.1.129.252     YES       manual up up
Ethernet0     10.1.2.252      YES       manual up up
Izmir#
```

Konfigürasyondaki IP adresleri "show ip interface brief" komutunun çıktısı ile eşleşmektedir. Bu detaylar eşleşmiyorsa, dalgınlıkla RAM'deki konfigürasyon yerine NVRAM'deki konfigürasyona bakıyor olabilirsiniz. Etkin konfigürasyonu görüntülemek için "show running-config" ya da "write terminal" komutlarını kullandığınızdan emin olunuz.

İstanbul Router'ının konfigürasyonu ve komutlar çalıştırıldığında elde edilen çıktılar:

```
Istanbul#show running-config
Building configuration...
Current configuration : 869 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname İstanbul
!
!
enable secret 5 $l$J3Fz$QaEYNIiI2aMu.3Ar.qOXm.
!
ip name-server 10.1.1.100
ip name-server 10.1.2.100
```

```
!
interface SerialO
ip address 10.1.130.253 255.255.255.0
no fair-queue
!
interface Seriall
ip address 10.1.129.253 255.255.255.0
!
EthernetO
   ip address 10.1.3.253 255.255.255.0
!
no ip http server
banner motd ^C
Take a little off the top, Wabbit! (Erhan) AC
!
line con 0
password cisco
   login
   line aux 0
   line vty 0 4
password cisco
   login
!
End

Istanbul#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP externa1, O - OSPF, IA - OSPF inter area Nl -
OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, Ll - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gatevuay of last resort is not set

10.0.0.0/24 is alt ağted, 3 alt ağs
C 10.1.3.0 is directly connected, EthernetO
C 10.1.130.0 is directly connected, SerialO
C 10.1.129.0 is directly connected, Seriall

Istanbul#show ip interface serial 1
Seriall is up, line protocol is up
Internet address is 10.1.129.253/24
Broadcast address is 255.255.255.255
Address determıned by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing Access list is not set
```

```
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is disabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are neversent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabied
IP Feature Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled

Istanbul#show interface serial 0
SerialO is up, line protocol is up
Hardware is HD64570
Internet address is 10.1.130.253/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, ndoad 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, Otoytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
```

```
O carrier transitions
DCD=up      DSR-up           DTR=up      RTS=up      CTS=up

Istanbul#show ip arp
Protocol   AddressA     Age(min)  Hardware Addr Type Interface
Internet  10.1.3.102     0         0060.978b.1301 ARPA EthernetO
Internet  10.1.3.253     -          0000.0c3e.5183 ARPA EthernetO

Istanbul#debug ip packet
IP packet debugging is on
Istanbul#ping 10.1.130.251
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 10.1.130.251, timeout is 2
seconds:!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
80/81/84 ms
Istanbul#
00:09:38 IP s=10.1.130.251 (local), d=10.1.130.251 (Seriall), len
100, sending
00:09:38 IP s=lO.1.130.251(Serial1), d=10.1.130.253 (Seriall), len
100, rcvd 3
00:09:38 IP s=10.1.130.253 (local), d=10.1.130.251 (Seriall), len
100, sending
00:09:38 IP s=10.1.130.251 (Serial1), d=10.1.130.253 (Seriall), len
100, rcvd 3
00:09:38 IP s=10.1.130.253 (local), d=10.1.130.251 (Seriall), len
100, sending
00:09:38 IP s=10.1.130.251 (Seriall), 4=10.1.130.253 (Seriall), len
100, rcvd 3
00:09:38 IP s=10.1.130.253 (local), d=10.1.130.251 (Seriall), len
100, sending
00:09:38 IP s=10.1.130.251 (Seriall), d=10.1.130.253 (Seriall), len
100, rcvd 3
00:09:38 IP s=10.1,130.253 (local), d=10.1.130.251 (Seriall), ien
100, sending
00:09:38 IP s=10.1.130.251 (Seriall), d=10.1.130.253 (Seriall), len
100, rcvd 3
```

"show ip arp" komutu sonucunda elde edilen ARP önbelleği görülmektedir. İlk kayıt, Ethernet üzerindeki bir başka makinenin IP adresini (10.1.3.102) ve MAC adresini göstermektedir. Sayacın değerinin 0 olması kaydın yeni oluşturulduğunu gösterir. Sayaç değeri kayıt kullanılmadıkça büyür ve sonunda kaydın zaman aşımına uğramasını sağlar. ARP tablosunda zaman aşımına uğramayacak kayıt, router'ın Ethernet arabiriminin kendisi ile ilgili olan kayıttır.

"debug ip packet" komutu, gönderilen ve alınan her IP paketi için bir kayıt listeler. Bu komut oldukça tehlikeli bir komuttur. Debug mesajlarının işlenmesinden dolayı aşırı bir işlem yükü oluşacak ve bu da router'ın çökmesine neden olacaktır. Bir router'ın saniyede 50000 paket ilettiği düşünülürse, 9600 bps hızda çalışan konsol bağlantısı üzerinden saniyede 50000 mesaj gönderemeyeceği, bu nedenle router'ın mesajları arabelleğinde

tutacağı ve bunu yaparken tüm hafızasını kullanacağı kesindir. Router'ın çökmesine neden olabilecek bu komutu ağınızda etkin olarak çalışan bir router'da çalıştırmadan önce bir kez daha düşününüz. Çıktıda hem kaynak hem de hedef IP adresleri gösterilmektedir.

Yönlendirme tablosunda tüm alt ağlar listelenmemiştir çünkü yönlendirme protokolü konfigürasyonu henüz yapılmamıştır. Tüm routerların yanında C değeri bulunduğuna dikkat ediniz. C değeri yolun bağlı bir alt ağı tanımladığı anlamına gelmektedir.

ip route 10.1.2.0 255.255.255.0 10.1.128.252
ip route 10.1.3.0 255.255.255.0 10.1.130.253

Ankara yönlendiricisine "ip route" komutları kullanılarak statik yol bilgileri eklenmiştir. Ankara'daki bir yol İzmir'den çıkan ve 10.1.2.0'a giden bir yol tanımlamaktadır. Bu nedenle, bir sonraki atlamanın IP adresi Izmir'in Seri 0 arabiriminin IP adresi olan 10.1.128.252 olarak konfigüre edilmiştir. Benzer şekilde, Istanbul'un alt ağ'i olan 10.1.3.0'e giden yol da, İstanbul'un Seri 0 Arabiriminin IP adresi olan 10.1.130.253 olarak konfigüre edilmiştir. Bu konfigürasyonlann yapılmasının ardından, Ankara bu alt ağlere paket iletebilecektir.

Ankaraya 10.1.2.0 ve 10.1.3.0 statik yolları eklendikten sonra "show" komutlarının çıktısı:

```
ankara#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D
- EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA externai type 1, N2 - OSPF NSSA externa! type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll -
IS-IS Ievel-1, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic
down!oaded static route

Gateway of last resort is not set

      10.0.0.0/24 is alt ağted, 5 alt ağs
      S 10.1.3.0 [1/0] via 10.1.130.253
      S 10.1.2.0 [1/0] via 10.1.128.252
      C 10.1.1.0 is directly connected, EthcrnetO
      C 10.1.130.0 is directly connected, Seriall
      C 10.1.128.0 is directly connected, SerialO

Ankara#ping 10.1.128.252
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 10.1.128.252, timeout is 2
seconds:!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8
ms
! Note: the folloıving extended ping command will result in some
debug
messages
```

```
!

Ankara#ping
Protocol [ip]:
Target IP address: 10.1.2.252
Repeatcount [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [nj: y
Source address or interface: 10.1.1.251
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbosefnone]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Ankara#
```

Ankaraya statik yollar eklenmesin ardından İzmir yönlendiricisi üzerinde çalıştırılan "show" komutlarının çıktısı:

```
Izmir#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D
- EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area Nl - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF
external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, Ll -
IS IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic
downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is alt ağted, 3 alt ağs
C 10.1.2.0 is directly connected, EthernetO
C 10.1.129.0 is directly connected, Seriall
C 10.1.128.0 is directly connected, SerialO

Izmir#ping 10.1.128.251
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 10.1.128.251, timeout is 1 seconds
!!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max =4/4/8
 ms

Izmir#ping 10.1.1.251
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 10.1.1.251, timeout is 2 seconds:
```

```
Success rate is 0 percent (0/5)

Izmir#debug ip icmp
ICMP packet debugging is on
Izmir#
Izmir#show debug
Generic IP:
    ICMP packet debugging is on
Izmir#
```

Aşağıdaki derleme mesajları Ankara üzerinde çalıştırılan genişletilmiş ping komutunun bir sonucudur; bu mesajlar Izmir tarafından üretilmektedir.

```
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
```

"ping" komutları, aksi genişletilmiş *bir* ping ile belirtilmediği sürece paketin kaynak adresi olarak çıkış arabiriminin IP adresini kullanır. İzmir üzerinde çalıştırılan ilk ping kaynak olarak **10.1.128.251** kullanmaktadır: genişletilmiş ping kullanıcının girdiği kaynak adresi (10.1.1.251) kullanmaktadır.

ICMP Echo Yanıtı mesajları (ping yanıtları) yanıtladıkları ICMP Echo işlemlerindeki *IP* adreslerini tersine çevirir.

Ping seçeneklerini daha açık hale getirmek için bu konfigürasyon İzmir ya da İstanbul'dan Ankara'ya (10.1.1.0) giden yolları içermez. Gerçek bir ağda, statik yollar yerine yönlendirme protokolleri kullanılacaktır. Statik yollar kullanıldığında, yolları her iki doğrultuda da tanımlamanız gerekir. Ancak bu örnekte, İzmir üzerinde **10.1.1.0'a** giden statik bir yol tanımlı olmadığından, 10.1.1.0'dan gelen paketler **10.1.2.0'a** iletilebilecek, ancak geri dönemeyecektir.

Bu ağdaki sorunları gidereceğinizde, o alt ağdaki bir kullanıcıyı çağırıp bilgisayarından bir ping komutu çalıştırmasını istemek yerine, genişletilmiş ping komutunu kullanarak o alt ağdaki bir PC'den ping komutunu çalıştırmışçasına sonuçlar elde edebilirsiniz, ping komutunun genişletilmiş sürümü problemin nedenini tam olarak anlamak için kullanılabilir. Aslında, ping router'da çalışıyor ancak ulaşılmaya çalışılan makineden çalıştırılan ping yanıt vermiyorsa, genişletilmiş ping komutunu kullanarak problemi inceleyebilmek için ping komutunu ulaşılmaya çalışılan makine üzerinden çalıştırmanız mümkün olacaktır. Örneğin, Ankara üzerinde çalıştırılan genişletilmiş ping komutu, 10.1.1.251'den (Ankara'ın Ethernet arabirimi) 10.1.2.252'ye (İzmir'in Ethernet arabirimi) bir Echo istemi göndermiştir ancak Ankara hiçbir yanıt alamaz. Normalde, echo'lar çıkış arabiriminin IP adresini kaynak olarak kullanır. Ancak genişletilmiş ping adres seçeneğini kullanarak echo paketinin kaynak IP adresi değiştirilebilir.

Genişletilmiş ping ile oluşturulacak ICMP echo, **10.1.1.0** içindeki bir adresi kaynak olarak kullanacağından, o alt ağdaki bir uç kullanıcı tarafından oluşturulmuş gibi gözükecektir. Genişletilmiş ping tarafından üretilen ICMP Echo İstemleri Izmir tarafından alınıyor gibi gözükmektedir çünkü İzmir üzerinde debug mesajları incelendiğinde ICMP Echo Yanıtlarının 10.1.1.251 adresine geri gönderildiği anlaşılmaktadır. ICMP echo yanıtlarını oluşturan İzmir ile bunları alan Ankara arasında bir problem ortaya çıkmıştır.

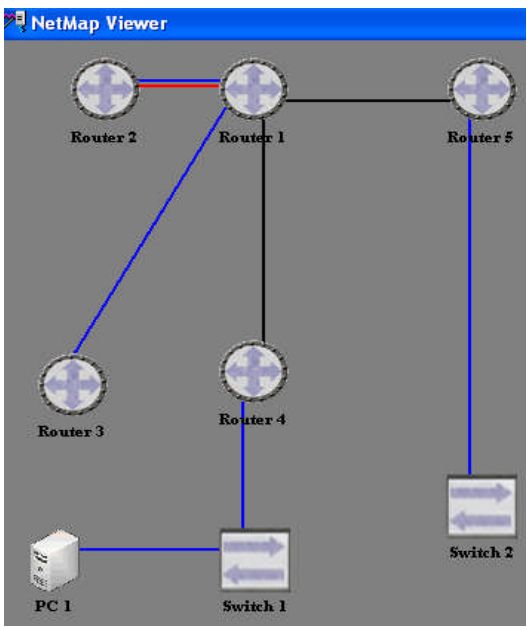
Problem daha önceden de bahsedildiği gibi, İzmir'in paketleri 10.1.1.0 adresine nasıl ileteceğini söyleyen bir yol bilgisine sahip olmamasından kaynaklanmaktadır. Bu örnekteki problemi anlamak için İzmir tarafından yaratılan Echo Yanıtlarından sonraki adımların incelenmesi gerekmektedir. ICMP, Izmir'deki IP yazılımına paketleri iletmesini söylemektedir. IP kodu, bu paketler için hedefi 10.1.1.251 olan doğru yolu bulabilmek üzere yönlendirme tablosuna bakar. Ancak İzmir'de çalışan show ip route komutunun çıktısı İzmir'in **10.1.1.0** alt ağına giden bir yol bilgisine sahip olmadığını göstermektedir. İzmir Echo Yanıtı mesajlarını yaratmıştır ancak **10.1.1.0/24'**e giden bir yol bilgisine sahip olmadığından bu mesajları gönderememiştir.

Genişletilmiş **ping** ile birlikte kullanılabilen diğer seçenekler de oldukça kullanışlıdır. Parçalama (Don't Fragment-DF) biti ile echo içinde gönderilecek veri miktarı ayarlanarak gönderilebilecek MTU'nun ne olacağı deneysel olarak keşfedilebilir. MTU kısıtlamaları nedeniyle ve DF biti ayarlanmış olduğundan bir bağlantı üzerinden iletilemeyecek Echo paketleri düşürülebilir (atılabilir). Zaman aşımı değeri ayarlanarak, ping komutunun Echo Yanıtı için varsayılan zaman olan 2 saniyeden daha uzun süre beklemesi sağlanabilir. Bunların yanında, bir ICMO Echo mesajı için sadece tek bir boyut değil, birçok boyut ayarlanarak, daha gerçekçi bir paket kümesi elde edilebilir.

Ping komutu ile gerçekleştirilecek hata tespiti işlemlerinde, komutun alabildiği yanıtlar ile ilgili olarak kullandığı çeşitli kodları anlamak önemlidir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ IOS yazılımını çalıştırmak için yönlendirici bağlı olan bilgisayarın hyper terminallini çalıştırınız ve CLI komut satırı arabirimine geçiniz.	Öğrenme faaliyeti-1' de olduğu gibi bu öğrenme faaliyetindeki işlem basamaklarını simulatör ya da emulatör programları ile de yapabilirsiniz. Boson Netsim simulator programını "Load Simulator with default Labs and Netmap" seçeneği ile açtığınızda netmap olarak karşınıza gelen ağ şemasında bulunan yönlendiricilerin yapılandırmasını Öğrenme Faaliyeti-1'de yapmıştınız. Bu uygulama faaliyetinde bu yapılandırmayı kontrol edeceksiniz.



Statik yönlendirme yaparken yönlendiricilerin IP adresleri

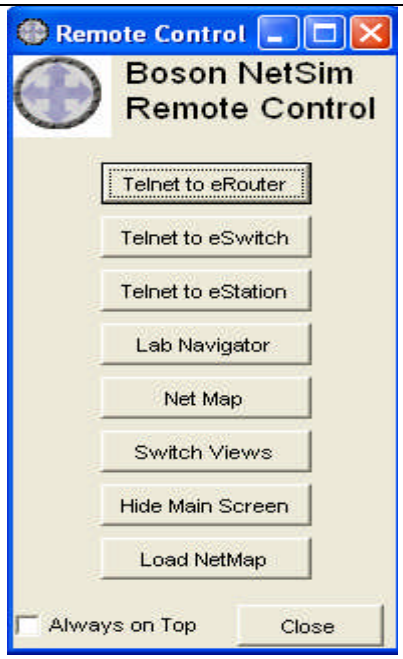
	eRouter1	eRouter2	eRouter4
arayüz Ethernet 0	10.1.1.1 255.255.255.0	10.1.1.2 255.255.255.0	
arayüz Seri 0	12.5.10.1 255.255.255.0		12.5.10.2 255.255.255.0

RIP yönlendirme protokolü ile yönlendirme yaparken yönlendiricilerin IP adresleri:

➢	<table><tr><td></td><td>eRouter1</td><td>eRouter2</td><td>eRouter4</td></tr><tr><td>Arayüz Ethernet 0</td><td>10.1.1.1 255.255.255.0</td><td>10.1.1.2 255.255.255.0</td><td></td></tr><tr><td>Arayüz Serial 0</td><td>172.16.10.1 255.255.0.0</td><td></td><td>172.16.10.2 255.255.0.0</td></tr></table> .
➢ Ağda bulunan yönlendirici ya da yönlendiricileri n arayüzlerini, kablolarını, donanım adreslerini, alınıp gönderilen paket miktarlarını kontrol ediniz.	➢ Ağda bulunan yönlendiricilerin arayüzlerinin, kablo bağlantılarının kontrolü için show interface komutu kullanılır. Bu komutu kullanırken komutun hangi modda çalıştığını biliniz. Daha sonra teker teker yönlendiricilerin arayüzlerini show interface (arayüz no) komutuyla kontrol ediniz. Komutu çıktısı olarak: **Serial is up, line protokol is up –** Bu mesaj gelirse bağlantı var, hat canlı problem yok anlamındadır. **Serial is up, line protokol is down** –Bu mesaj gelirse kablo çalışıyor ama ikinci katmanda problem var, hat canlı değil(keepalives). **Serial is down, line protokol is down** -Arayüz problemi var. Diğer arayüzler kapalı olabilir. **Serial is administratively down, line protokol is down** - Bağlantı yok. Arayüzler shutdown komutuyla kapatılmıştır. ➢ Alınıp gönlendirilen paket miktarlarını inceleyiniz. ➢ Çarpışma olmuş mu ona bakınız. **T**üm arayüz istatistiklerini ve IP numaralarını görmek için “show interfaces” komutunu kullanabilirsiniz.
➢ ➢ Yönlendirme yollarını kontrol ediniz.	Statik ya da dinamik olarak belirtmiş olduğumuz yolları görüntüleyerek sorun var mı yok mu anlayabiliriz. “Show ip route” komutu yönlendiricideki tüm yolları gösterir. Örneğin statik yönlendirme yapıldıktan sonra eRouter2 yönlendiricisinin yolları: **eRouter2#show ip route** **Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP** **D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area**

➢ Sorunları tespit ediniz	**E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP** **i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default** **U - per-user static route** **Gateway of last resort is not set** **C 10.1.1.0/24 is directly connected, 10.1.1.2** **S 12.5.10.0/24 [1/0] via 10.1.1.1** "Show ip route" komutunun başındaki açıklayıcı bilgiler, yönlendirme bilgisinin kaynağını belirtmek için kullanılan harf kodlarının ne anlama geldiğini açıklar. Örneğin, C harfi bağlı (connected) yollar, R harfi, RIP, I harfi IGRP için kullanılır. Daha sonra her A, B ya da C sınıfı ağ ve o ağdaki alt ağlar listelenir. Köşeli parantezin içindeki sayılardan ilki, yönetimsel uzaklığı *(administmtive distance)* tanımlar. Yönetimsel uzaklık, bir tam sayı değeridir ve her yönlendirme bilgisinin kaynağına atanmıştır. Yönetimsel uzaklık değeri daha düşük olan yönlendirme bilgisi kaynağı daha iyi demektir. İkinci sayı ise, yolun metrik değeridir.
➢ Bağlantıları ping komutuyla test ediniz.	Statik ve RIP protokolü ile tanımlamış olduğunuz yolların çalışıp çalışmadığını yani bağlantının olup olmadığını anlamak için ping komutunu kullanınız. Ping komutundan sonra IP adresi yazılabildiği gibi host adıda yazılabilir ama bunun için hostun adını önceden belirtmemiz gerekir. Örneğin RIP ile yolları belirttikten sonra ping komutunun kullanımı: **eRouter2#ping 172.16.10.1** **eRouter4#ping 10.1.1.2** Ping komutundan sonra her şey yolunda ise !!!!! işaretleri çıkar. Bu işaretten bir tane çıksa bile problem yoktur ama ağ yoğundur. '!' işaret harici çıkan işaretler ağ da bir bağlantı problemi olduğunu gösterir. **. Hiçbir şey alınamadı.** **U ICMP erişilemiyor (hedefe) mesajı alındı** **N ICMP erişilemiyor (ağa) mesajı alındı** **P ICMP erişilemiyor (porta) mesajı alındı** **Q ICMP kaynak yavaşlamak mesajı alındı** **M ICMP parçalara ayrılamıyor mesajı alındı** **? Bilinmeyen bir paket alındı.**

➢ Bağlantıları trace komutuyla test ediniz.	Trace komutuyla uçtan uca kontrol yerine aşamalı kontrol yapılır. Yani bir uçtan diğer uca varana kadar her noktayı kontrol eder. Bu kontrol daha etkilidir. Unutmayın en fazla 15 basamak kontrol yapar. Kullanımı, "Ping" komutunun kullanımı gibidir. Komuttan sonra IP adresi yazınız. Ağda bulunan her noktayı kontrol etmek için bu komutu kulanınız. Komutu kullandıktan sonra ağda bir problem varsa aşağıdaki hata mesajlarını çıkar. *** Zaman Aşımı (süre içinde cevap gelmiyorsa)** **!H Paket karşı taraftan alındı fakat geri bildirim gelmedi.** **N Ağa ulaşılamadı.** **U Porta ulaşılamadı.** **P Protokole ulaşılamadı.**
➢ Bağlantıları telnet komutuyla test ediniz.	Uygulama katmanında bağlantıyı kontrol etmek için telneti kullanınız. Telnet ile birden fazla cihaza bağlanabilir bu cihazları askıya alabilirsiniz. Telnet bağlantısını askıya almak için CTRL+SHIFT+6 ve X tuşlarını hep birlikte kullanınız. Bir telnet oturumunu askıya alındıktan sonra, enter a bastığınızda en son askıya alınmış telnet bağlantısı devam eder.

	 **router1# telnet 175.10.1.2** **router3>** **router3> ctrl-shift-6 x** **router1#** **router1# show sessions**
➢ Komşu aygıtların bağlantı bilgilerini görüntüleyiniz.	Yönlendirme yaparken komşu yönlendiricilerin bilgilerine ihtiyaç duyucaksınız. Bunun için "show cdp neighbor" komutunu kullanabilirsiniz. Bu komut genel bilgileri görüntüler. "show cdp entry <cihaz host adı>" komutuyla da belli bir cihazın detay bilgilerini görüntülersiniz. "show cdp neighbor detail" komutuyla komşulukta bulunan cihazların detay bilgilerini görüntülersiniz. "show cdp interface" komutuyla bağlı olduğunuz cihazın arayüzleri ve cdp mesajları hakkında bilgi alırsınız. "show cdp traffic" komutuyla CDP trafiği ile ilgili istatistikleri görüntülersiniz.

Komutları yazarken hangi modda olduğunuza dikkat ediniz**!**

ÖLÇME VE DEĞERLENDİRME

Bu faaliyet sonunda hangi bilgileri kazandığınızı, aşağıdaki soruları yanıtlayarak belirleyiniz.

ÖLÇME SORULARI

Aşağıdaki sorulardan; sonunda parantez olanlar doğru yanlış sorularıdır. Verilen ifadeye göre parantez içine doğru ise "D" , yanlış ise "Y" yazınız. Şıklı sorularda doğru şıkkı işaretleyiniz.

1. Yönlendiriciye yapılmış olan o anki Telnet bağlantılarını aşağıdaki komutlardan hangisi görüntüler?

A) show telnet
B) show history
C) show version
D) show sessions

2. Yönlendirme tablosu girdilerini gösteren komut aşağıdakilerden hangisidir?

A) ping
B) trace
C) show ip route
D) show interface

3. Çalışan bir seri port için show interface s1 komutu çıktısı aşağıdakilerden hangisidir?

A) Serial1 is up, line protocol is up
B) Serial1 is up, line protocol is down
C) Serial1 is down, line protocol is down
D) Serial1 is administratively down, line protocol is down

4. "show ip route" komutunun çıktısındaki köşeli parantezlerin içindeki sayılar aşağıdakilerden hangi değeri tanımlar?

A) Gateway, alt ağ
B) Network, route source
C) Memory, overhead
D) Yönetimsel uzaklık, metrik değer

5. "Ping" komutu uygulandığında ekrana PPPPP harfinin çıkmasının sebebi aşağıdakilerden hangisidir?

A) Hiçbir şey alınamadı.
B) Bilinmeyen bir paket alındı.
C) Hedef bilgisayarın portuna erişilemiyor.
D) Hedef bilgisayara ulaşılamıyor.

6. "Trace" komutu tarafından gönderilen orijinal paketler, sıklıkla kullanılan bir hedef port numarası kullanır. ( )

7. Telnet bağlantısını askıya almak için aşağıdaki tuş takımlarından hangisi kullanılmaktadır?

A) ctrl-shift–6 ardından x
B) ctrl-shift–6 ardından y
C) ctrl-shift–7 ardından x
D) ctrl-shift–7 ardından y

8. Hat üzerinde çarpışmaların olup olmadığını anlamak için kullandığımız komut aşağıdakilerden hangisidir?

A) ping
B) trace
C) show ip route
D) show interface

9. Komşu cihazların genel bilgilerini görüntülemek için kullanılan komut aşağıdakilerden hangisidir?

A) cdp enable
B) show cdp traffic
C) show cdp neighbor
D) show cdp

10. Debug komutu, IOS'un işleyemeyeceği kadar fazla sayıda mesaj üretilmesine sebep olarak, IOS'un çökmesine sebep olabilir. ( )

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz.

Bu öğrenme faaliyetini tam anlamıyla anladığınızı düşündüğünüzde modül değerlendirmeye geçiniz.

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ (YETERLİK ÖLÇME)

Modül ile kazandığınız yeterliği aşağıdaki kriterlere göre değerlendirdiniz mi?

Değerlendirme Ölçütleri	Evet	Hayır
1. Yönlendirici yazılımını çalıştırdınız mı?		
2. Yönlendirme yolunu gösterdiniz mi?		
3. Ağ geçitini belirttiniz mi?		
4. Yönlendirmeleri gösterdiniz mi?		
5. Hedefe giden yolları incelediniz mi?		
6. Bağlantıları kontrol ettiniz mi?		
7. Ping komutunu kullanıp çıkan sonucu değerlendirdiniz mi?		
8. Net Diag ile ağınızı kontrol ettiniz mi?		
9. Ipconfig komutunu kullandınız mı?		
10. Route print komutunu kullanıp var olan yolları incelediniz mi?		
11. Tracert ve pathping komutlarını kullandınız mı?		
12. Yönlendirici ya da yönlendiricilerin arayüzlerini, kablolarını, donanım adreslerini, alınıp gönderilen paket miktarlarını kontrol ettiniz mi?		
13. Yönlendirme yollarını kontrol edip, sorunları tespit ettiniz mi?		
14. Ping komutunuyla bağlantı testi yapıp çıkan mesajı değerlendirdiniz mi?		
15. Trace komutuyla bağlantı testi yapıp çıkan mesajı değerlendirdiniz mi?		
16. Telnet ile yölendiricilere bağlandınız mı?		
17. Komşu aygıtların bağlantı bilgilerini görüntülediniz mi?		

DEĞERLENDİRME

Yapılan değerlendirme sonunda hayır cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız modülü tekrar ediniz!

Modülü tamamladınız, tebrik ederiz. Öğretmeniniz size çeşitli ölçme araçları uygulayacaktır. Öğretmeninizle iletişime geçiniz.

CEVAP ANAHTARLARI

ÖĞRENME FALİYETİ 1 CEVAP ANAHTARI

1	**C**
2	**B**
3	**D**
4	**D**
5	**YANLIŞ**
6	**DOĞRU**
7	**DOĞRU**
8	**DOĞRU**
9	**DOĞRU**
10	**YANLIŞ**

ÖĞRENME FALİYETİ 2 CEVAP ANAHTARI

1	**DOĞRU**
2	**YANLIŞ**
3	**YANLIŞ**
4	**YANLIŞ**
5	**DOĞRU**
6	**DOĞRU**
7	**B**
8	**D**
9	**B**
10	**D**

ÖĞRENME FALİYETİ 3 CEVAP ANAHTARI

1	**D**
2	**C**
3	**A**
4	**D**
5	**C**
6	**YANLIŞ**
7	**A**
8	**D**
9	**C**
10	**DOĞRU**

KAYNAKÇA

- TURGUT Hulisi**, Ağ Teknolojisine Giriş,** 2004.
- ÇÖLKESEN Rıfat, **Ağ Yönetimi**, Papatya Yayıncılık, İstanbul,2001