T.C.
MİLLİ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN
GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

TCP/IP KONTROL MESAJLARI

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

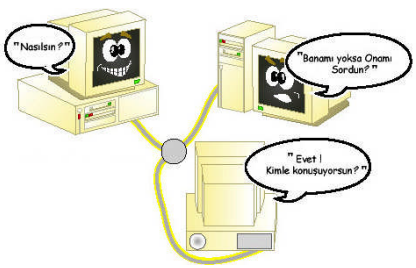
KOD	**481BB0059**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**TCP/IP Kontrol Mesajları**
MODÜLÜN TANIMI	Bilgisayar ağlarında TCP/IP kontrol mesajlarından oluşan öğrenme materyalidir.
SÜRE	40/24
ÖN KOŞUL	Yönlendirme Protokolleri modülünü almış olmak.
YETERLİK	TCP/IP kontrol mesajlarının görevlerini bilerek kullanmak.
MODÜLÜN AMACI	**Genel Amaç** Bu modül ile gerekli ortam sağlandığında, TCP/IP kontrol mesajları ile bağlantıyı test edebileceksiniz. **Amaçlar** ➢ ICMP kontrol mesajlarının işlevini kavrayarak, mesaj gönderebileceksiniz. ➢ Kontrol mesajlarının parametrelerini kullanabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	Ağla birbirine bağlı bilgisayar laboratuvarı, yönlendirici ve modem.
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. Modül sonunda verilen öğretici sorularla edindiğiniz bilgileri pekiştirecek, uygulama örneklerini ve testleri gerekli süre içinde tamamlayarak etkili öğrenmeyi gerçekleştireceksiniz. ➢ Sırasıyla araştırma yaparak, grup çalışmalarına katılarak ve en son aşamada alan öğretmenlerine danışarak ölçme ve değerlendirme uygulamalarını gerçekleştireceksiniz.

GİRİŞ

Sevgili Öğrenci,

Bilgisayarlar çok da uzak olmayan geçmişinde tek başına çalışan makinelerdi. Daha sonra insanların birbirleri ile iletişim imkânları arttıkça ve birlikte çalışmanın önemi kavrandıkça bilgisayarlarındaki bilgileri de paylaşmak ihtiyacı duydular. Bu nedenle bilgisayarları birbirine bağlamanın yollarını aradılar.

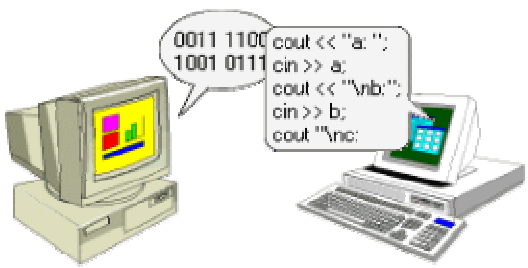
Bu arayışlar sonuç verdi ve öncelikle yakın olan bilgisayarlar birbirine bağlandı; aralarında ortak bir dil oluşturuldu. TCP/IP'nin ilk temelleri burada atıldı. Daha sonra ikiden fazla bilgisayar birbirine bağlandı. Zaman ilerledikçe birbirine bağlı bilgisayarların oluşturduğu aile genişlemeye başladı. Birçok insan bilgilerini paylaşmaya başladı.



Aile büyüdükçe kontrol de zorlaştı ve karmaşıklıklar ortaya çıkmaya başladı ve bütün bu ağ iletişimini bir kurala bağlamak ihtiyacı duyuldu. TCP/IP bu dönemde ortaya çıktı. Bilgisayarların iletişimini kurallara bağlayan bir iletişim protokolleri kümesi olarak ağlar üzerinde yerini aldı.

İnsanlar bilgi paylaştıkları bilgisayarların bazen birbirleri ile olan bağlantısının kesildiğini, karşı tarafın bilgisayarını kapattığını, bazen de bilgisayarları birbirine bağlayan hatlarda sorunlar olabildiğini fark ettiler. Peki, karşı bilgisayarın ayakta olup olmadığını, bağlantısının ne durumda olduğunu ya da hatların yoğunluğundan dolayı iletişimin zayıflayıp zayıflamadığını nereden anlayabileceklerdi. İşte bu noktada TCP bir çözüm üretti.

Bu modülde TCP'nin bu konuya nasıl bir çözüm getirdiğini, bilgisayar ağlarında bilgisayarlar arası iletişimin, bağlantının hangi durumda olduğunu, kullanılabilir durumda olup olmadığını ya da bağlantının kopup kopmadığını nasıl test edebileceğimizi öğreneceğiz.



ÖĞRENME FAALİYETİ–1

AMAÇ

ICMP protokolünün işlevini kavrayıp bu protokolü kullanarak bilgisayarlar arası bağlantıyı test edebileceksiniz.

ARAŞTIRMA

- Bilgisayarlar arası ağlarda bağlantının nasıl yapıldığını, ağ bağlantılarında ne gibi hataların oluşabileceğini araştırınız. Edindiğiniz bilgileri sınıfta paylaşınız.

1. TCP/IP HATA MESAJLARI

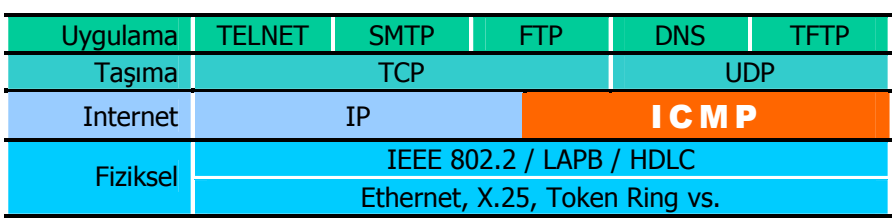
Bilgisayar ağlarının temelini fiziksel bağlantılar oluşturur. Bu fiziksel bağlantılar içerisine ağın kablolama sisteminden tutun, kablosuz ağ cihazlarına, internet gibi geniş bir ağın omurgasını oluşturan iletişim hatlarına kadar her şey girer. Bu ortamda ağları birbirine bağlayan aygıtlara **Gateway** (geçit) denir.

Bu kadar karmaşık ve birbirinden bağımsız birimlere ait yüzlerce elektronik aygıtın birlikte oluşturduğu sistemlerde sorun yaşanma riski her zaman vardır. Bu risk hiçbir zaman yok edilemez. Peki, bağlantı hatlarında herhangi bir nedenle arıza oluşmuşsa bunu nasıl anlayabiliriz? TCP/IP bu konuda bize bir çözüm üretmiş durumda. TCP/IP, bağlantının sağlamlığını ya da iletişim hattındaki hızı kontrol edebilmemizi sağlayan bir protokole sahiptir. Bu protokol bağlantıyı kontrol eder; sorun varsa bu sorunu, nedeniyle birlikte bize bildiren bir mesaj sistemine sahiptir. **ICMP** (Internet Control Message Protocol – İnternet Kontrol Mesaj Protokolü) bize bu imkânları sağlayan protokoldür.

TCP/IP Hata Mesajları, sistemlerin kendilerine gelen paketlere karşılık verdikleri cevap mesajlarıdır.

1.1. ICMP

Hedef sisteme kontrol mesajları göndererek bize gitti-gitmedi bilgisini veren bir protokoldür. TCP/IP katmanları içinde **Internet** katmanında yer alır.



Şekil 1.1: TCP / IP katman protokolleri

İnternet protokolü güvenilir olması için dizayn edilmemiştir. Hata raporlama veya hata düzeltme mekanizmaları yoktur. Bu açığı kapatmak için ICMP'den faydalanılır. ICMP mesajlarının amacı IP'yi güvenli hâle getirmek değil, bağlantı birimleri hakkında muhtemel problemlere karşı geri bildirim almak içindir. Bu mesajlara rağmen veri iletiminin hâlen garantisi yoktur. Yine de bazı veriler hiçbir geri bildirim raporu alınamadan, hedefine ulaşamadan kaybolabilir. IP kullanan üst katman protokolleri bağlantı güvenliğini kendi güvenlik metotlarıyla sağlamalıdırlar.

1.2. ICMP Mesajını Kullanan Komutlar

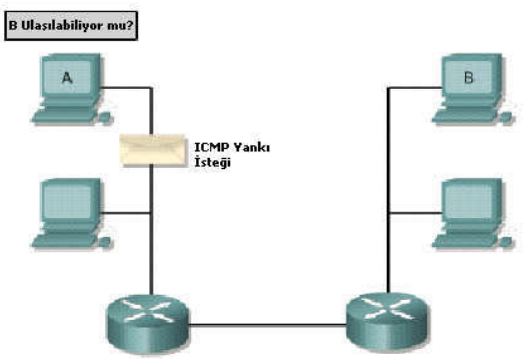
İnternet katmanında bulunan ICMP protokolünü PING ve TRACEROUTE uygulamaları kullanılır. PING komutu hedef sistemin ayakta olup olmadığının kontrolü için kullanılır. Düzenli bir şekilde gönderilen ICMP paketlerine verilen cevaplara göre bağlantı değerlendirmesi yapılır.

TRACEROUTE komutu ile ise TCP/IP protokolü üzerinden bir başka bilgisayara ICMP paketleri gönderebilir ve bu paketlerin diğer bilgisayara ulaşırken hangi noktalardan geçtiğini görebilirsiniz. Kısaca hedefe ulaşmak için takip edilen yolu tek tek görebilirsiniz. Sonuçlar ms (milisaniye) cinsinden gösterilir. Bu komut UNIX tabanlı sistemlerde TRACEROUTE olarak kullanılırken, WINDOWS ve DOS tabanlı sistemlerde sekiz harflik dosya isimleri nedeniyle TRACERT olarak kullanılmaktadır.

1.2.1. PING Komutu

Ping uygulaması 1983 yılında Mike MUSS tarafından yazılmıştır. Bu uygulamada hedef bir bilgisayara 32 bayt uzunluğunda bir ICMP paketi gönderilir ve aynı paketin geri gelmesi beklenir. Bu sayede hedef bilgisayar ile aradaki iletişim hakkında bazı bilgiler elde edilir. Bu bilgiler:

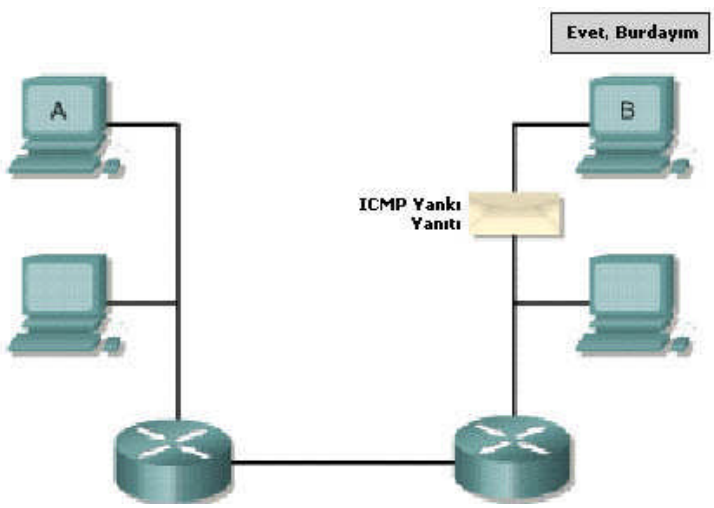
- Paketin gönderildiği sistemin o anda çalışıp çalışmadığını gösterir.
- Aradaki iletişim ağlarında pakette oluşan kayıpları gösterir.
- İki sistem arasındaki iletişim süresini gösterir.



Şekil 1.2: PING komutu gönderimi

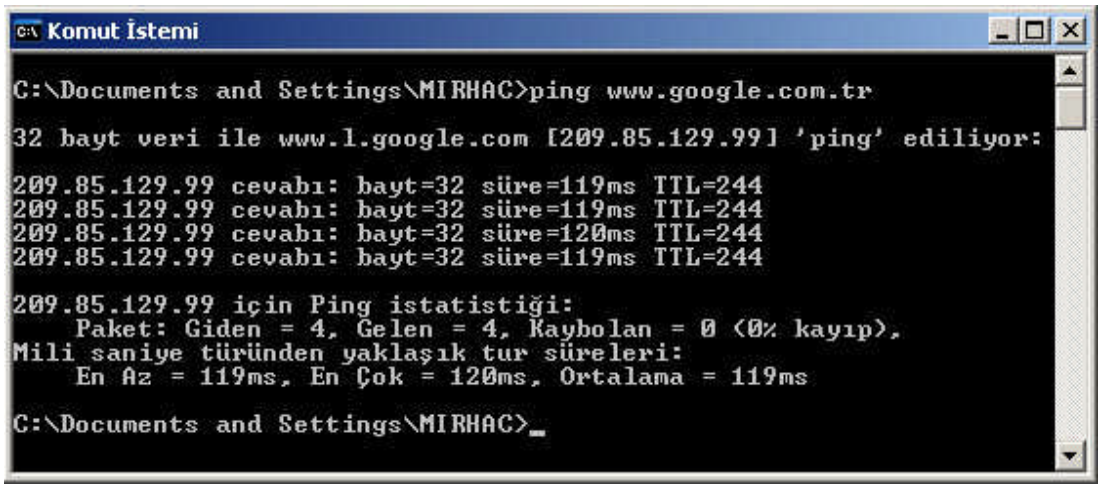
ping	[-t] [-a] [-n sayım] [-l boyut] [-f] [-i TTL] [-v TOS] [-r sayım] [-s sayım] [[-j anabilgisayarlistesi] | [-k anabilgisayarlistesi]] [-w zamanaşımı] hedef_adı
-t	Belirtilen ana bilgisayar durana kadar PING komutunu kullanınız. İstatistikleri görmek ve devam etmek için - Control-Break yazınız; Durdurmak için - Control-C yazınız.
-a	Adresleri ana bilgisayar adlarına çözünüz.
-n sayım	Gönderilecek yankı isteklerin sayısı.
-l boyut	Arabellek boyutunu gönderiniz.
-f	Pakette parçalara ayırma bayrağını ayarlayınız.
-i TTL	Yaşam süresi.
-v TOS	Hizmet türü.
-r sayım	Sayım durakları için kayıt yolu.
-s sayım	Sayım durakları için zaman damgası.
-j anabilg.-listesi	Ana bilgisayar-listesi boyunca belirsiz kaynak yolu.
-k anabilg.-listesi	Ana bilgisayar-listesi boyunca kesin kaynak yolu.
-w zamanaşımı	Her cevap için milisaniye cinsinden beklenecek süre.

Tablo 1.1: Ping komutu kullanımı ve parametreleri.



Şekil 1.3: PING komutuna yanıt gönderimi

Ping komutuna cevap geliyorsa karşı sistem ulaşılabiliyor demektir. Eğer cevap gelmiyorsa karşı sistem erişilemez durumdadır.



Şekil 1.4: PING komutu uygulaması

Örnek bir PING komut uygulaması sonucu yukarıdaki gibidir.

Bu örnekte www.google.com.tr adresine 32 bayt uzunluğunda ICMP paketleri ile dört adet yankı isteğinde bulunuluyor. Öncelikle verilen URL' ye ait IP adresi çözümleniyor ve bu IP adresine 32 bayt uzunluğunda paketler gönderiliyor. Bu paketleri alan google sunucusu paketlere cevap veriyor. ICMP paketinin gönderilme süresi ile paketin gelme süresi arasındaki farktan aradaki iletişim zamanı tespit ediliyor.

Bu örnekte dört paketin dördü de google sunucusuna ulaşmış ve cevaplanmıştır. İlk paketin ulaşım süresi 119 ms ve paketin yaşam süresi 244 ms'dir. Paketin üzerinden geçtiği her sistemde paket yaşam süresi 1 ms azalır.

Yaşam ömrü kısa paketler göndererek kaç sistem üzerinden geçtiğimizi görebiliriz. Örneğin TTL = 10 olan bir ICMP paketi ile yapılan PING sorgulamasında paket zaman aşımına uğradı ve hedefe ulaşamadı. Fakat TTL 11 olan bir paket sonuç getirdi. Buna göre hedef sisteme kadar en az 10 ağ aygıtı ya da sistemi üzerinden atlıyoruz demektir.

Ping komutu kullanımında paket yaşam ömrünün nasıl belirlendiğini bulabilirsiniz.

Microsoft sunucuları dışında bütün sunucular PING komutuna cevap verirken, Microsoft sunucuları ICMP paketlerini genelde engellemekte ve cevap vermemektedir.

PING komutunda genellikle ICMP yankı mesajı kullanılır. Alternatif kullanım şekilleri de vardır.

- UDP yankı portu kullanımı (destekleniyorsa),
- SNMP sorgu zamanlamasında,
- TCP bağlantı zamanlamasında.

Şekil 1.5: PING komutu uygulaması

Genel olarak neredeyse bütün istek ve cevaplar gidiş dönüş zamanlaması hakkında bilgi verir. Özellikle yönlendiricilerin ICMP yankı mesajlarını fazla dikkate almamaları düşük öncelikli tutmaları nedeniyle paketin gidiş dönüş süresinin yanlış bilgi vermesi göz önüne alındığı zaman ICMP yankı mesajları dışındaki yöntemler bazen daha verimli olabiliyor.

Şu da unutulmamalıdır ki, gidiş-dönüş zamanını ölçmek için kullanılan çok çeşitli metot vardır ve bu metotların amacı dışında, sistemlere saldırı niteliğinde kötü niyetli kullanımları da mevcuttur. Çok sık gönderilen istek mesajları sistemlerin ve iletişim performanslarının üzerinde negatif bir etkisi vardır. Kullanılmayan bir porta gönderilen isteklerin etkileri tahmin bile edilemez.

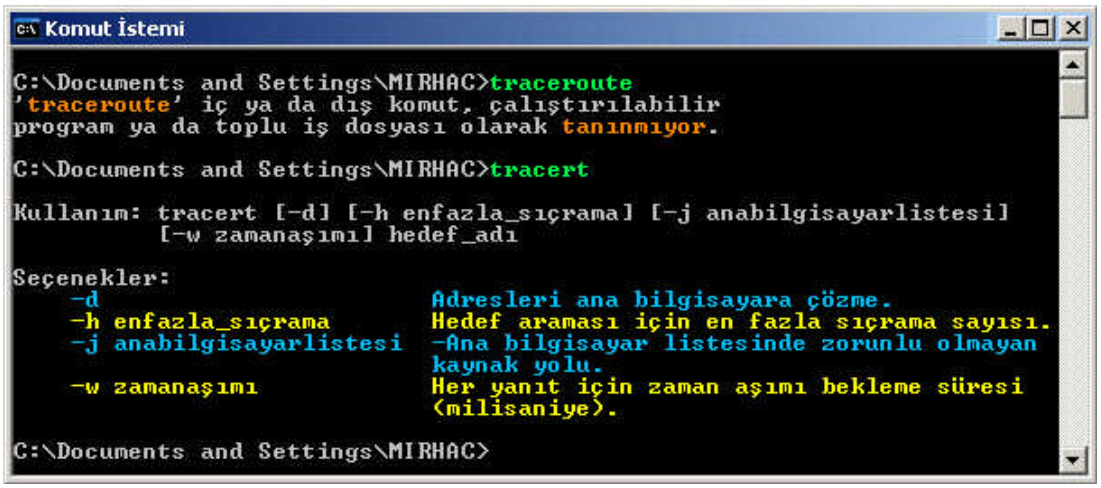
Bir diğer önemli nokta, PING isteği kullanan uygulamaların hangi metodu kullandığına dikkat etmek gerekir. Çünkü her farklı metoda verilen cevap süreleri de farklıdır. ICMP yankı özelliği kullanılırken bu bilgi göz önünde tutulmalıdır.

1.2.2. TRACEROUTE Komutu

TRACEROUTE komutu Windows ve DOS tabanlı sistemlerde sekiz harflik kısaltmalar nedeniyle TRACERT olarak kullanılmaktadır. PING komutu gibi çalışır fakat PING komutundan faklı olarak geçilen her yönlendirici için rapor verir. Her atlama için gidiş dönüş süresi (RTT ReTurn Time) oluşturmak üzere ICMP yankı isteği mesajlarını göndererek yolu izler. Yönlendiricilerin, güvenlik duvarlarının ve diğer güvenlik ağ geçitlerinin paket filtreleme sistemleri bu paketlerin iletilmesini engelleyebilir.

TRACEROUTE genellikle her defasında yaşam süresi değeri sürekli artan bir dizi araştırma paketleri gönderir. Bu araştırma paketleri, IP paketlerinin içerisine yerleştirilmiş UDP paketleridir. Hedef sisteme giden yolda, üzerinden atlanan her ağ aygıt yaşam süresi değeri düşük olan araştırma paketini, iletilebilmesi için yeterli yaşam süresi değerine sahip olana kadar reddeder. TRACEROUTE yol üzerindeki her atlamada atlamayı belirlemek ve gidiş dönüş süresini hesaplamak için bir ICMP mesajı alır.

Bazı sistemler Traceroute işlemleri için UDP paketleri yerine ICMP paketlerini tercih eder. Her iki durumda da Traceroute hedefteki son noktaya kadar giden yolda reddedilen her bir araştırma paketine karşılık kendisine ulaşan ICMP mesajlarına bakar.



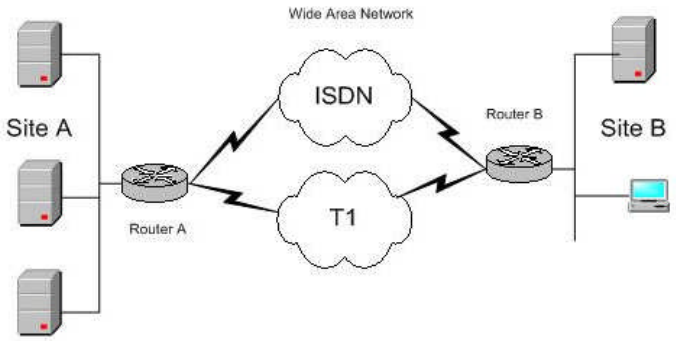
Şekil 1.6: TraceRoute veya tracert komutları

Diğer bir deyişle traceroute, iki nokta arasında bulunan ağ sistemleri üzerinden geçemeyecek kadar düşük yaşam süresine sahip paketler gönderir. Bu aygıtlar paketleri reddeder ve kendi IP adresiyle birlikte bir "Paket Yaşam Süresi Doldu" ICMP hata mesajı gönderir. Traceroute bu mesajdaki IP adresi sayesinde sistemi belirler. Bu sistemin IP adresi ile DNS sorgulaması yapılır ve sisteme ait isim belirlenir. Daha sonra bu sistemi atlayacak yaşam süresi değerine sahip başka bir araştırma paketi gönderir. Bu paket bir sonraki sisteme iletilir. Bu kez de ikinci sistem tarafından reddedilir ve bir hata mesajı daha gelir. Bu işlem hedef sisteme ulaşılıncaya kadar devam eder. Böylece reddedilen her araştırma paketine karşılık gelen "Paket Yaşam Süresi Doldu" mesajlarından, mesajı gönderen sistemin IP adresi alınır, sistemin ismi belirlenerek hedefe giden yol bulunur.

UDP ve ICMP tipi araştırma mesajlarının her ikisi de IP paketleri içerisine yerleştirilmiştir ve yol üzerindeki sistemler tarafından reddedilmesine neden olabilecek Yaşam Süresi Değerleri (TTL - Time To Live) vardır.

Bilindiği üzere ICMP mesajlarında port numarası bulunmaz. Traceroute işlemi belli bir porta yönlendirilmiş UDP paketleri ile yapılmalıdır. ICMP mesajları kullanılmamalıdır. Birçok uygulama ICMP mesajı kullanmaması gerekirken ICMP mesajları ile yol belirlerler. Oysaki ICMP mesajları ile yapılan yol bulma işlemleri çoğunlukla başarısız olurlar. Orta düzey atlamalarda yönlendiriciler bazen ICMP yaşam süresi doldu mesajı göndermeyi veya ICMP yankı isteklerini önemsemeyerek cevap vermeyi reddeder. Bu durumda ICMP ile yapılan yol sorgulamaları başarısız olabilir.

Şimdi bu komutun nasıl kullanıldığına bakalım.



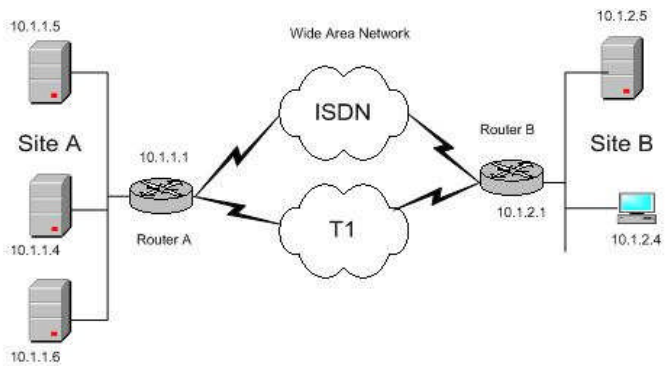
Şekil 1.7: WAN bağlantılı ağ modeli

Şekilde görüldüğü gibi Site A ile Site B'de bulunan bir terminal arasında bir iletişim hattımız var. Paketler iki uç arasında T1 bağlantısı üzerinden gidiyor ve yedek bir de ISDN hattı var. Traceroute uygulamasını doğru bir şekilde kullanmak için, temel olarak hedefinizin IP adresini ve traceroute işlemi sonuç raporunda ne aradığınızı bilmeniz gerekir.

- **TRACEROUTE Nasıl Kullanılır**

Şekil 1.7'de de gördüğünüz gibi test terminalinden (Site A) sunucuya (Site A) araştırma paketleri göndereceğiz. Paketler T1 ve buna paralel ISDN hattından oluşan WAN üzerinden geçecek. Traceroute uygulamasını kullanmak için hedef IP adresini bilmemiz gerekir.

Bildiğiniz gibi traceroute, paketleri TTL değerini arttırarak gönderir. TTL değeri üzerinden geçilen her routerde bir azalarak yoluna devam eder. Böylece bir atlama yapmış oluruz. Bir routerden bir sonraki routere geçtiğimiz anda buna atlama diyoruz. Bu şekilde her atlamada azalan yaşam süresi "0" olduğu anda hangi router ya da aygıta gelmişsek, oradan "Yaşam Süresi Doldu" ICMP hata mesajı alırız. Şekil 1.8'de kaynak ve hedef IP adresini görebileceğimiz bir ağ modeli gösterilmektedir.



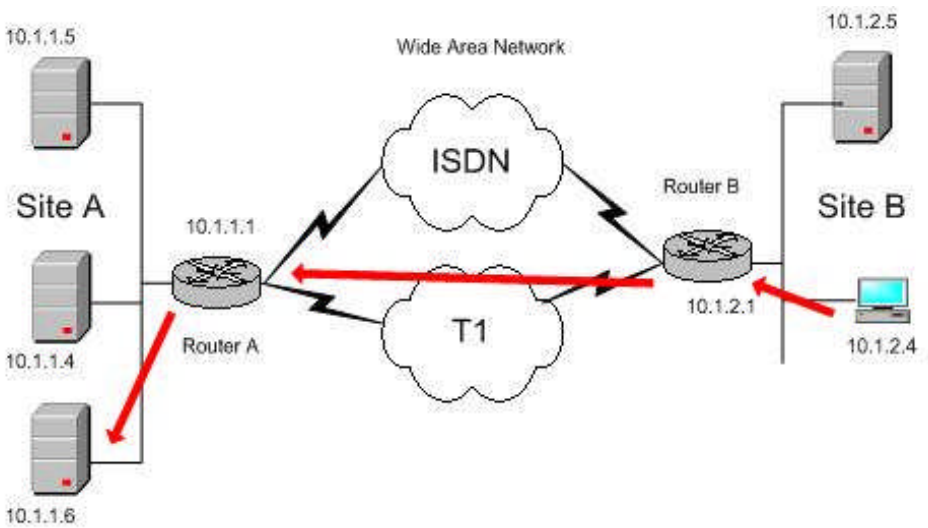
Şekil 1.8: WAN üzerinde kaynak ve hedef IP adresleri

Bu şekle göre 10.1.2.4 kaynak IP adresimiz, 10.1.1.6 ise hedef IP adresimiz olacaktır. Gönderilen araştırma paketlerinin normal rotası yüksek hız kapasitesine sahip T1 hattı üzerinden olacaktır. Çünkü T1 1.544 Mbps, ISDN ise 128 Kbps hızında hatlardır. ISDN hattı eğer T1 hattında problem olursa kullanılmak üzere tutulan yedek hattır. Traceroute işlemine başlandığı anda paketler 10.1.2.4 Site B IP adresinden 10.1.1.6 Site A IP adresine doğru T1 hattı üzerinden Şekil 1.9'daki gibi yola çıkarlar.

Routerler paketleri nereye ileteceklerini bilirler. Router A ise paketi 10.1.1.1 numaralı ağ adresi üzerindeki son olarak 10.1.1.6 sistemine nasıl ileteceğini bilir.

Paketler gönderildikten sonra traceroute uygulaması ilk router arabiriminden başlayarak atlamalarınızın raporlama işlemine geçer. Şimdi test paketlerini göndermeden önce yolumuzun tamamına şekil üzerinde bir göz atalım.

Şekil 1.9'da paketlerin kaynak ve hedef sistemler arasında izleyeceği yol gösterilmiştir. Hatırlanması gereken önemli bir nokta, raporlama yapılırken en yakın arabirimler kullanılır. Yakın arabirimler, gönderici sisteme en yakın olan routerlerdir. Bu örnekte Site A'dan Site B'ye T1 üzerinden yapılan iletişimi görüyorsunuz. Şimdi bunun neden önemli olduğunu görelim.

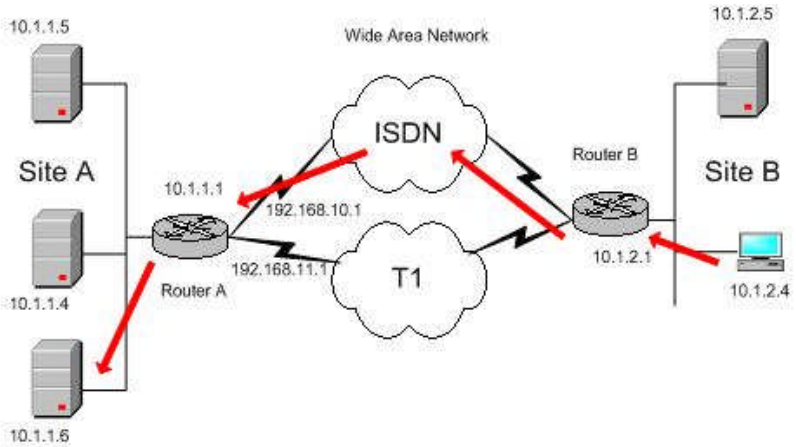


Şekil 1.9: kaynak ve hedef arası paket iletim modeli

Traceroute çalıştığı yol üzerinde ulaşıp üzerinden geçtiği cihazlardan geri dönüt mesajları alır. Bu mesajlardan birçok şey öğrenebilirsiniz. Eğer en yakın arabirimlerden mesajlar alıyorsanız Şekil 1.10'da göreceğiniz 192.168.10.1 ve 192.168.11.1 gibi yeni IP setleri karşınıza çıkar. 192.168.10.1 ISDN hattı için, 192.168.11.1 ise T1 hattı için kullanılmaktadır. Bunun önemi nedir?

Traceroute sonucunda aldığımız raporlarda bu komutu kullanmaya aşina olmayan kişiler için anlamsız gelebilir. Her iki hat üzerinden de Site A hedef adresi yerine WAN

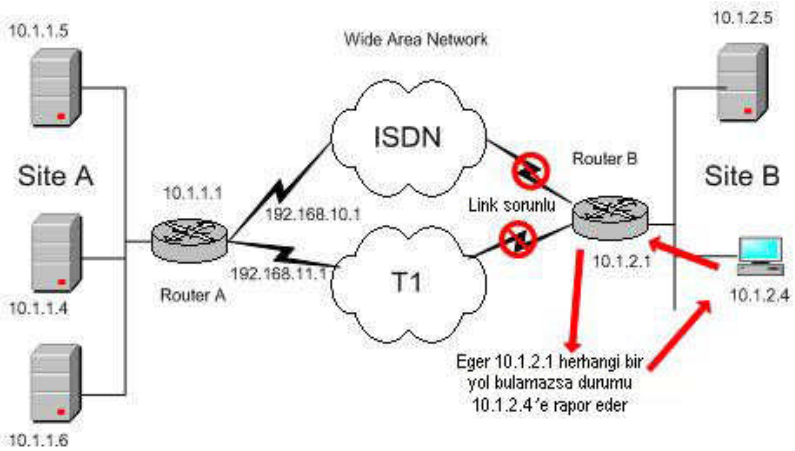
adresleri, 10.1.1.1 gibi varsayılan ağ geçidi adresi karşımıza geliyor. Aynı routere ulaşılıyor fakat arabirim farklı. Bu sizin için traceroute testi yaparken gerekli olabilir. Çünkü bu noktada kafanız karışırsa okuduğunuz raporun ne anlama geldiğini anlayamayabilirsiniz.



Şekil 1.10: Farklı hatlara ait bağlantı noktaları

Örneğin, Şekil 1.10'da gördüğünüz yolda, paketler 10.1.2.4'ten varsayılan ağ geçidi olan 10.1.2.1'e oradan ISDN WAN hattı üzerinden 10.1.1.1 Site A router varsayılan ağ geçidine, oradan da hedef sistem olan 10.1.1.6'ya doğru ilerliyor.

ISDN hattının Site A routerindaki uç adresi 192.168.10.1 ve T1 uç adresi şekildeki gibi 192.168.11.1. traceroute işleminde ulaşılan adres 10.1 ile bitiyorsa ISDN, 11.1 ile bitiyorsa T1 hattı kullanılmış demektir. Bu nedenle traceroute raporuna dikkatli bakmak gerekiyor. ISDN bağlantılar T1 bağlantılardan daha yavaştır. ISDN kullanılıyorsa T1 hattı problemli ya da aşırı yoğun olabilir. Bu örnekte, bağlantılarda öncelikli olarak T1 hattı kullanılır.



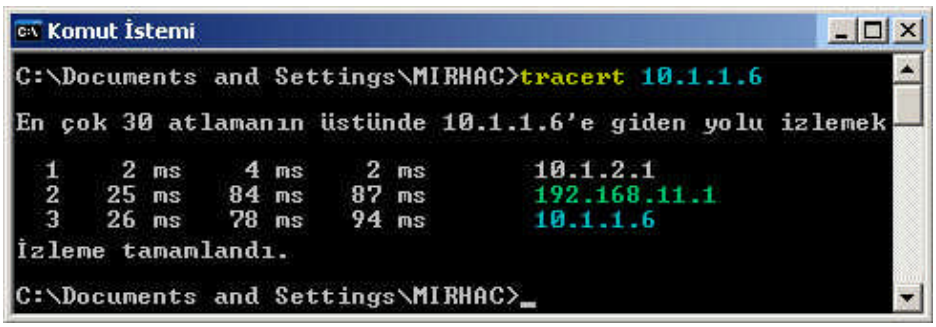
Şekil 1.11: Sorunlu hatlarda traceroute uygulaması

Eğer şekildeki gibi hatların ikisinde de sorun varsa ve hedefe ulaşılabilecek herhangi bir alternatif yoksa, bir sonraki atlamaya ulaşamayan router 10.1.2.1 bu durumu paketlerin geldiği 10.1.2.4 sistemine rapor ederek bildirir.

- **TRACEROUTE Testi**

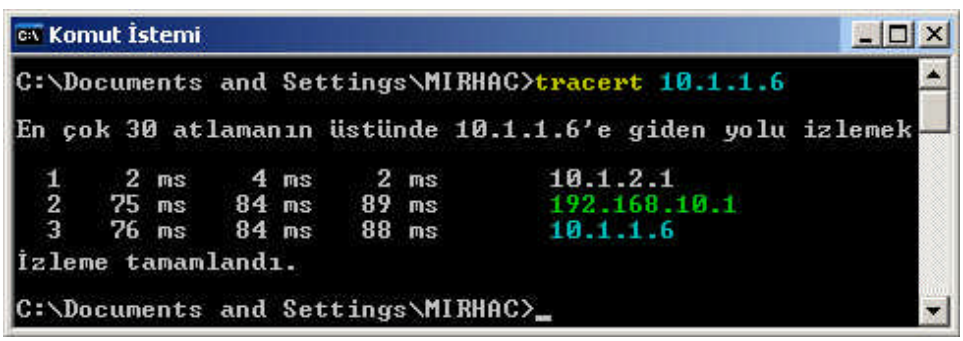
Aşağıdaki hraceroute örneğinde tracert komutu ile tracert raporunda paketler 10.1.1.6 bilgisayarına ulaşmak için Şekil 1.12'deki gibi iki router üzerinden geçmektedir. Bu örnekte Site B varsayılan ağ geçidi 10.1.2.1, T1 ve ISDN WAN IP adresleri sırasıyla 192.168.11.1 ve 192.168.10.1 olarak belirlenmiştir.

Şimdi T1 kullanılır durumdayken yapılan uygulamasında sonuç ne olur, görelim.



Şekil 1.12: T1 üzerinden tracert raporu

Şimdi de T1 hattı problemli ve ISDN hattı kullanılırken tracert raporuna bakalım. Raporda 2. adımda farklı bir IP adresi kullanılarak hedefe gidildiğini görebilirsiniz. Ayrıca 2. adımın bir önceki örneğe göre daha uzun süre aldığını da görebilirsiniz. T1 hattının ISDN hattından daha hızlı bir iletişim sağladığını hatırlayınız. Bu nedenle 2. adımda T1 yerine servis sağlayıcının sizi ISDN hattına yönlendirmesi nedeniyle paket iletim süresinde üç kata kadar bir uzama söz konusudur.



Şekil 1.13: ISDN hattı üzerinden tracert raporu

Gördüğünüz gibi tracert kullanımı size kullandığınız ağ yolunu tanımanıza ve bilgi paketlerinizin izlediği yolu görmenize yardımcı olur.

- **Tracert Komutu Parametreleri**

Tracert komutunu kullanmak için aşağıdaki parametreleri bilmeniz yararınıza olacaktır. En çok kullanılan ilk parametre olan "-d" parametresidir.

Tracert	[-d] [-h enfazla_sıçrama] [-j anabilgisayarlistesi] [-w zamanaşımı] hedef_adı
-d	Belirlenen IP adreslerini DNS sorgularıyla çözümlemez. Bu parametre tracert komutuna zaman kazandırır ve hızlandırır.
-h enfazla_sıçrama	Hedef araması için en fazla sıçrama sayısı. (Varsayılan değer 30'dur)
-j anabilg.listesi	Ana bilgisayar listesinde zorunlu olmayan kaynak yolu. Bu parametrede bir ana bilgisayar listesi belirtebilir, hedefi genişletebilirsiniz. Birden fazla hedefi birden fazla router ile sorgulayabilirsiniz. Bu listede kullanılabilecek en fazla 9 hedef bilgisayar sorgulayabilirsiniz. Hedef bilgisayar listesi bir dizi IP adresinden oluşur ve aralarında boşluk bırakılarak birbirinden ayrılır.
-w zamanaşımı	Her cevap için zaman aşımı bekleme süresini belirler. Varsayılan değer 4 saniye = 4.000 ms'dir.
-?	Komut hakkında yardım listesini gösterir.

Tablo 1.2: Tracert komut parametreleri

Tracert işleminde şu noktalara dikkat etmelisiniz:

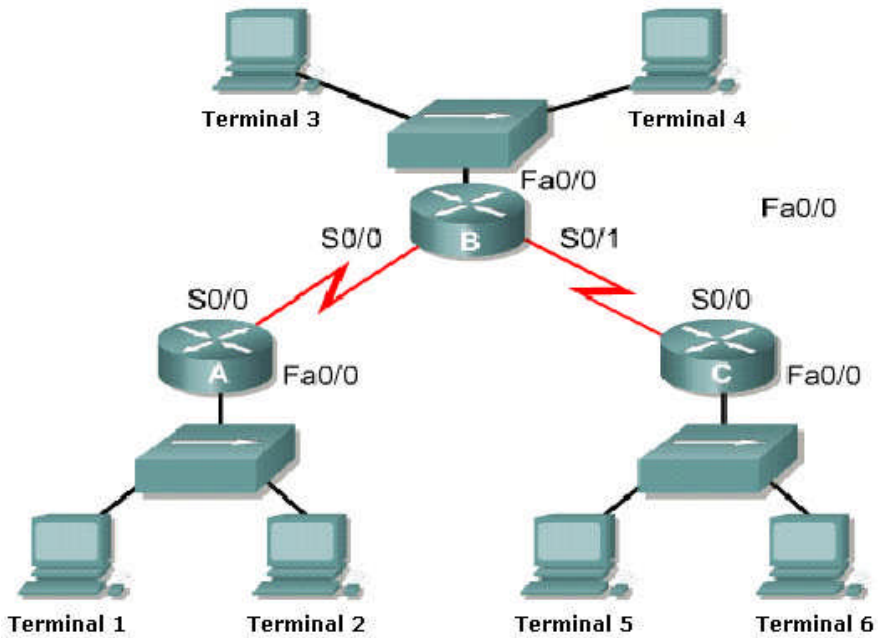
- Tracert, gecikmeleri tespit etmenize yardımcı olmaz. Bir yolu takip ederek yol üzerindeki ağ gecikmeleri, her bir router geçişinde paket kayıpları hakkında bilgi edinmek istiyorsanız pathping komutunu kullanmalısınız.
- Tracert işlemini, yalnızca sisteminizdeki TCP/IP protokolü ağ bağlantılarınızın ağ bağdaştırıcısı özelliklerinde yüklenmiş ise uygulayabilirsiniz.
- Son Linux sistemlerinde **Traceroute** (Linux tracert kullanmaz) uygulamasında 33434 numaralı portu üzerinden UDP paketleri kullanır. Windows ise daha çok Ping paketleri olarak bilinen ICMP yankı istekleri (tip 8) kullanır.

1.3. ICMP Mesajlarının İletimi

IP en zahmetli iletim sistemi olduğu için sınırlıdır. Verinin iletilip iletilmediğine dair herhangi bir bilgilendirme sistemi yoktur.

Bu eksiklikleri belirlemede yardımcı olması için IP, gönderilen verinin iletimi işleminde hata oluştuğu zaman göndericiyi bilgilendirmek üzere Internet Control Message Protocol (ICMP) kullanır.

IP, ağ verilerinin iletiminde güvenilir bir metot değildir. En zahmetli metot olarak bilinir. Datagram (TCP/IP temel bilgi birim miktarı) iletim hatası oluştuğu zaman; ICMP, datagramın kaynağına bu hataları rapor etmek için kullanılır.



Şekil 1.14: Genel ağ bağlantı yapısı

Eğer şekildeki gibi Terminal 1, Terminal 6'ya bir datagram gönderiyor. Fakat Router C'deki Fa0/0 arayüzü çöküyor. Bu durumda Router C Terminal 1'e datagramın iletilemediğini bildirir bir mesaj göndermek için bir ICMP mesajı hazırlar. ICMP hataları düzeltmez. Yalnızca hata hakkında bilgilendirir.

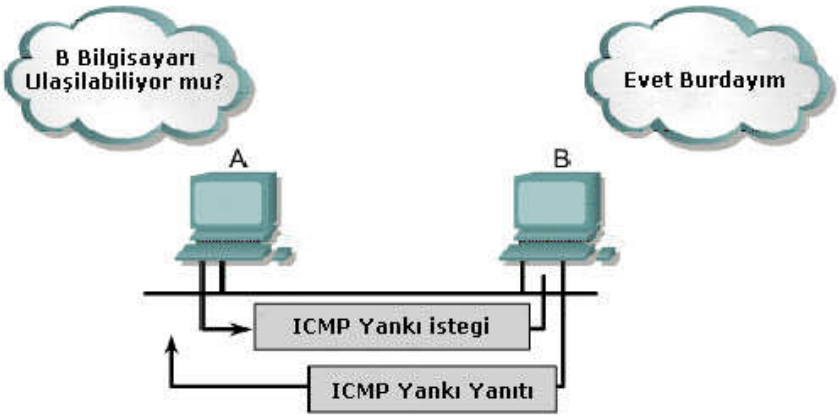
ICMP mesajları, IP kullanarak iletim yapan diğer verilerle aynı şekilde datagramlara dönüştürülürler. Diğer verilerle aynı şekilde iletilmesi nedeniyle, diğerleriyle aynı iletim hatalarına uğrarlar.

Ağ iletişimi bazı kesin temellere dayanır. Öncelikle, alıcı ve gönderici sistemler düzgün bir şekilde ayarlanmış TCP/IP protokolüne sahip olmalıdır.

- TCP/IP kurulumu,
- Düzgün bir şekilde ayarlanmış IP adresi ve alt ağ maskesi,
- Eğer datagramlar yerel ağ dışına da gönderilecekse düzgün ayarlanmış bir de varsayılan ağ geçidi.

İkincil olarak, aracı aygıtlar da gönderici sistemi, bulunduğu ağla birlikte alıcı sistem ağına bağlayarak paketleri yönlendirecek şekilde yerleştirilmiş olmalı.

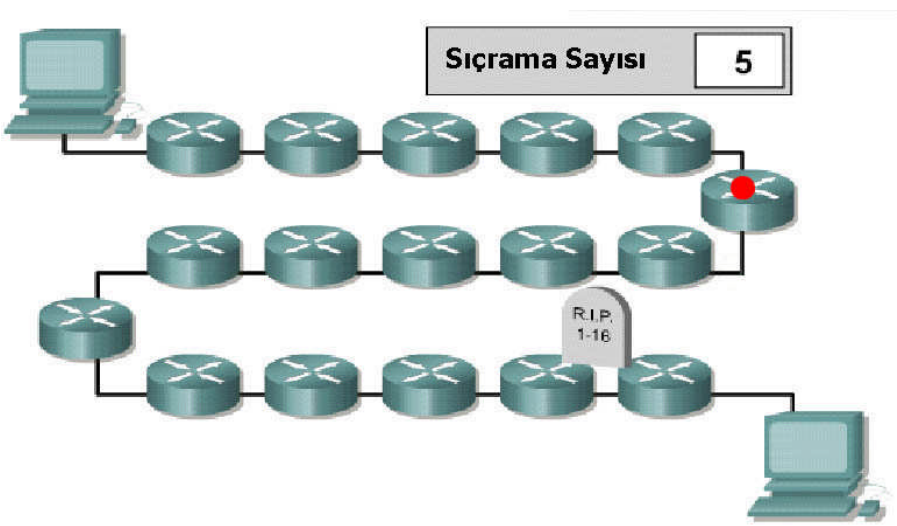
Aynı zamanda yönlendirici de arayüzünde düzgün şekilde ayarlanmış bir TCP/IP protokolüne ve uygun bir yönlendirme protokolüne sahip olmalıdır.



Şekil 1.15: Yankı isteği gönderimi

ICMP protokolü belirli bir hedefin iletişim için uygun olup olmadığını test etmek için kullanılabilir. Şekil 1.15'te hedef aygıta ICMP yankı isteği gönderiliyor.

Hedef aygıt ICMP yankı isteğini alıyor ve bu yankı isteğine karşılık bir yanıt mesajı oluşturarak istek sahibine gönderiyor.



Şekil 1.16: Azami sıçrama sayısına ulaşan paket

Şekilde sıçrama sayısı 5 olarak belirlenmiş bir paketin ağ üzerinde ilerlemesi görülmektedir. Paket, 6. sıçramayı yapamadan router üzerinden atılıyor. Bu durum aynı

zamanda paket yaşam süresi (TTL) dolumu demektir. Çünkü paket yaşam süresi azami sıçrama sayısıyla uyumlu ve orantılıdır.

Bütün ICMP mesajları tip, kod ve hata kontrol alanları ile başlamasına rağmen her bir mesaj paketinin özel formatı vardır.

1.4. ICMP Mesajları

ICMP hata mesajları belirli durumlarda otomatik olarak oluşturulup ilgili sisteme gönderilirler. Bu ICMP mesajları şu durumlarda oluşturulurlar:

- TTL süresi dolduğu zaman paket sahibine bildirmek için.
- Herhangi bir durumda paket yok edildiğinde geribildirim için.
- Parçalanmaması belirtilmiş paket parçalandığında geribildirim için.
- Hata durumlarında geribildirim için.
- Paket gideceği yol değiştirildiği zaman geribildirim için.

Bu durumlar oluştuğu zaman bazı mesajlar üretilerek paket sahibi bilgilendirilir. Bu gibi durumlarda üretilen belli başlı ICMP mesajları şunlardır.

- Destination Unreachable (Hedef Ulaşılamaz Mesajı)
- Time Exceeded (Paket Yaşam Süresi Doldu Mesajı)
- Parameter Problem (Parametre Hatası Mesajı)
- Source Quench (Kaynak Yavaşlatma Mesajı)
- Redirect (Yeniden Yönlendirme Mesajı)
- Echo or Echo Reply (Yankı veya Yankı Yanıt Mesajı)

Bu mesajların her birinin paket yapısı farklıdır. Şimdi genel bir ICMP mesajının yapısını ve bu yapılardaki mesajların ayrı ayrı mesaj alanlarını inceleyelim.

1.4.1. ICMP Hata Mesaj Yapısı ve Mesaj Çeşitleri

ICMP mesajları temel IP başlığı kullanılarak gönderilir. Datagramın ilk 8 bitlik kısmı ICMP tipi alanıdır. Bu alanın değeri geri kalan bilginin formatını belirler. “Unused” (kullanılmıyor) olarak etiketlenmiş bütün alanlar gelecekte kullanılmak için ayrılmış olup mesaj gönderilirken “0” değeri ile doldurulmalıdır. Özel bir tanımlama yapılmadıkça mesaj alanları aşağıdaki gibidir.

Sürüm: 4 (IPv4)
IHL (Internet Header Length) - İnternet Başlık Uzunluğu, 32 bitlik kelime.
Servis Tipi : 0
Toplam Uzunluk : İnternet başlığı ve veri (Byte olarak)
Tanımlama, bayraklar, veri parçası konumu.

TTL (Time To Live) : Bu alan değeri saniye cinsindendir ve paketin üzerinden geçtiği her aygıtta azalarak hedefe doğru iletilir. Bu alanın değeri hedefe ulaşabilecek büyüklükte olmalıdır. Aksi hâlde hedefe ulaşamadan paket ömrü dolar ve paket atılır.

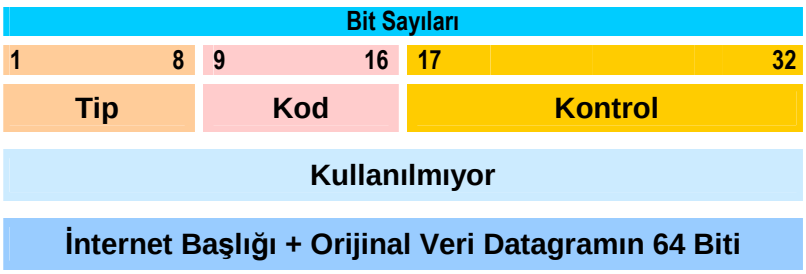
Protokol : ICMP = 1

Hata Kontrol Başlığı: 16 bitlik bütün alanların tümleyen aritmetiğine göre 1'in tümleyenleri toplamının 16 bit uzunluğunda 1'in tümleyenleridir. Bu kontrol gelecekte değiştirilebilir.

Kaynak Adres: ICMP mesajını hazırlayan sistemin ya da gatewayın adresidir. Aksi belirtilmedikçe bu alan herhangi bir gateway adresi olabilir.

Hedef Adres: Mesajın gönderileceği gateway veya sistemin adresidir.

Hedef Ulaşılamaz Mesajı



Şekil 1.17: Hedef ulaşılamaz mesajının yapısı

IP Alanları:

Hedef Adres: Orijinal datagram verisinden alınan kaynak ağ ve adres.

ICMP Alanları

Tip: 3

Kod:

0 Ağ ulaşılamaz,
1 Hedef sistem ulaşılamaz,
2 Protokol ulaşılamaz,
3 Port ulaşılamaz,
4 Bölünmeye ihtiyaç var ve bölünmez bayrağı ayarlanmış,
5 Kaynak yol başarısız,
6 Hedef ağ bilinmiyor,
7 Hedef sistem bilinmiyor,
8 Kaynak sistem koruma altında,
9 Hedef ağ ile iletişim yönetimsel olarak yasaklanmış,
10 Hedef sistem ile iletişim yönetimsel olarak yasaklanmış,
11 Aygıt tipi için ağ ulaşılamaz,
12 Servis tipi için sistem ulaşılamaz.

Kontrol: ICMP tipiyle başlayan ICMP mesaj toplamının 1'in tümlerinin 16 bitlik 1 tümleyeni.

İnternet Başlığı + Orijinal Veri Datagramlarının 64 Biti: İnternet başlığı ile orijinal datagram verisinin ilk 64 bitinin toplamı. Bu bilgiyi sistem, mesaj ile mesaj için belirtilen işlemin uyumlu olup olmadığını kontrol etmek için kullanır. Eğer üst katman protokolleri port numarası kullanmışsa, bu bilginin datagram verisinin ilk 64 bitinde bulunduğu varsayılır.

Açıklama

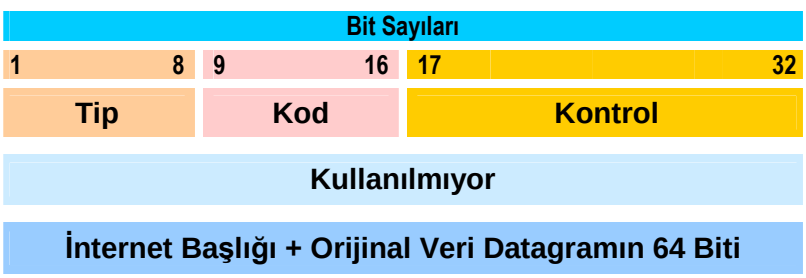
Eğer gateway yönlendirme tablosuna göre datagramın internet hedef alanında tanımlanmış ağa ya da bilgisayara erişilemezse, örneğin; hedefe olan mesafe sonsuz ise gateway, datagramı gönderen bilgisayara "hedef ulaşılamaz" mesajı gönderir.

Eğer hedef bilgisayarda IP modülü belirtilen protokol modülü ya da işlem görecek portun aktif olmaması nedeniyle datagramı iletemezse, kaynak sisteme "hedef ulaşılamaz" mesajı gönderilebilir.

Diğer bir ihtimal ise, ağ geçidinin datagramı iletebilmesi için parçalaması gerekebilir. Fakat datagramda "parçalanmasın" bayrağı aktif olabilir. Bu durumda ağ geçidi datagramı iptal edecek ve kaynak adrese "hedef ulaşılamaz" mesajı gönderecektir.

Kod 0, 1, 4 ve 5 ağ geçidinden (gateway), kod 2 ve 3 ise alıcı sistemden gelir.

Paket Yaşam Süresi Doldu Mesajı



Şekil 1.18: Paket yaşam süresi doldu mesajının yapısı

ICMP Alanları

Tip: 11

Kod:

0 Geçişte paket yaşam süresi dolmuştur.
1 Parçaları yeniden birleştirme süresi dolmuştur.

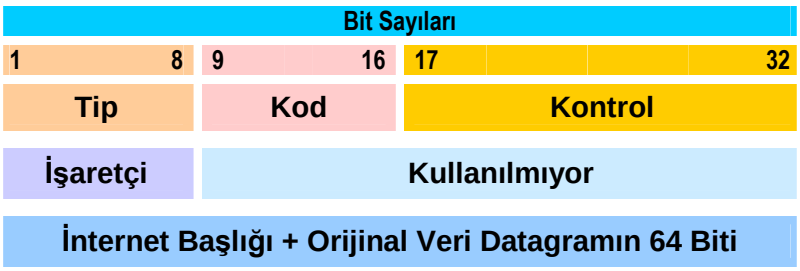
Açıklama

Eğer ağ geçidi işlediği datagramın yaşam ömrü alanının değeri 0 olursa, ağ geçidi bu datagramı iptal eder ve gönderen sistemi "Paket Yaşam Süresi Doldu" mesajı ile bilgilendirir.

Ayrıca, alıcı sistem datagram parçalarını yeniden birleştirirken eksik parçaların geçerli süre içerisinde gelmediğini görürse datagramı iptal eder ve gönderen sistemi "Paket Yaşam Süresi Doldu" mesajı ile bilgilendirir.

Kod "0" ağ geçidi, kod "1" ise alıcı sistemden gelir.

Parametre Hatası Mesajı



Şekil 1.19: Parametre hatası mesajının yapısı

ICMP Alanları

Tip: 12

Kod: 0 İşaretçi hata gösteriyor.

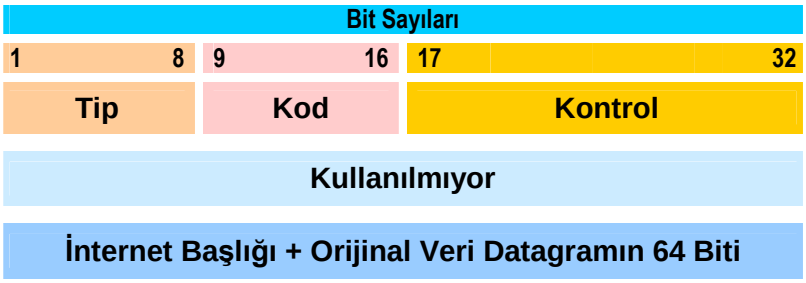
Parametre: Eğer kod "0" ise, hatanın nerede tespit edildiğini gösterir.

Açıklama

Eğer ağ geçidi veya alıcı sistem datagramı işlerken başlık parametrelerinde bir hata ile karşılaşırsa paketi işlemeyi bırakır ve iptal eder. Böyle bir durumda muhtemel hata bir işlem bildiriminde yanlış parametre kullanımıdır. Ağ geçidi veya alıcı sistem bu gibi durumlarda gönderici sistemi "Parametre Hatası" mesajı ile bilgilendirir. Bu mesaj hata sadece datagramın iptal edilmesine neden olursa gönderilir.

Kod "0", ağ geçidi veya alıcı sistemden gelir.

Kaynak Yavaşlatma Mesajı (Source Quench)



Şekil 1.20: Kaynak yavaşlatma mesajının yapısı

ICMP Alanları

Tip: 4
Kod: 0

Açıklama

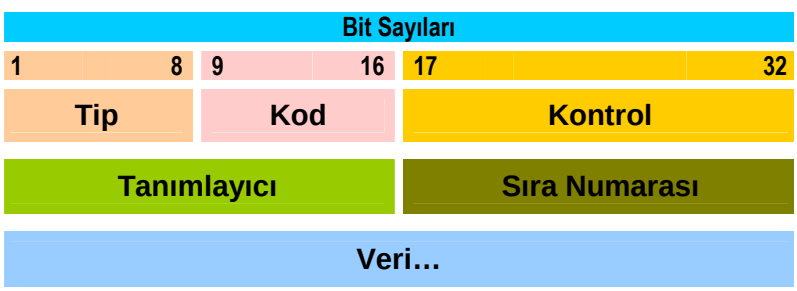
Ağ geçidi, kendisine gelen datagramları önbelleğine alır ve sırayla hedef ağlara yönlendirir. Eğer gelen datagramlar önbelleğe sığmazsa sonra gelenleri iptal eder. Ağ geçidi bu gibi bir durumda gelen datagramı iptal ederse gönderici sistemi "Kaynak Yavaşlatma" mesajı ile bilgilendirerek datagramları daha sonra göndermesini ister. Hedef sistem de üst üste işleyebileceğinden daha fazla datagram gelirse aynı mesajla göndericiyi yavaşlaması için bilgilendirir.

Gönderici sistem böyle bir mesaj aldığında aynı mesajı tekrar gelmeyinceye kadar datagramları göndermeyi yavaşlatmaya devam eder. Daha sonra tekrardan aynı mesaj gelene kadar gönderim hızını arttırmaya başlar.

Ağ geçidi ya da hedef sistem kapasitesi taşana kadar beklemek yerine kapasite üst sınırına ulaşılmasına yakın bu mesajı gönderir. Bu bir süre sonra kapasite aşılacak demektir.

Kod "0", ağ geçidi ya da alıcı sistemden gelir.

Yankı veya Yankı Yanıt Mesajı (Echo or Echo Reply)



Şekil 1.21: Yankı veya yankı yanıt mesajının yapısı

IP Alanları

Adresler: Yankı mesajının gönderen adresi yankı yanıt mesajındaki alıcı adresi olacaktır. Bir yankı yanıt mesajı oluşturulurken yalnızca kaynak ve hedef adresleri yer değiştirilir, tip kodu 0'a değiştirilir ve kontrol kısmı yeniden hesaplanır.

ICMP Alanları

Tip: 8 Yankı mesajı için,
0 Yankı yanıt mesajı için.

Kod: 0

Tanımlayıcı: Eğer kod "0" ise, yankıların ve yanıtların uyumuna yardımcı bir tanımlayıcıdır, "0" olabilir.

Sıra Numarası: Eğer kod "0" ise, yankı ve yanıtlarının uyumuna yardımcı bir sıra numarasıdır, "0" olabilir.

Açıklama

Yankı mesajında alınan veri, yankıya verilen yanıt mesajında aynı şekilde geri gönderilmelidir.

Tanımlayıcı ve sıra numarası yankı gönderen tarafından gelen yanıtların gönderilen mesaja ait olup olmadığını denetlemek için kullanılır. Örneğin, tanımlayıcı TCP ya da UDP'ye benzer şekilde oturum tanımlamak için bir port gibi kullanılmış olabilir. Bununla birlikte sıra numarası da aynı TCP'de olduğu gibi her yankı isteğinde bir artırılarak kullanılır. Yankıya yanıt veren sistem de bu bilgileri verdiği yankı yanıtında aynı şekilde geri gönderir. Böylece gönderici, gelen yanıtların gönderdiği yankı mesajlarına ait olup olmadığını belirleyebilir.

Kod "0" bir ağ geçidinden veya alıcı sistemde gelebilir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Açıklama
➢ Başlat – Tüm Programlar – Donatılar – Komut İstemi seçeneklerini takip ederek MSDOS komut istemini açınız.	➢ Başlat – Çalıştır komutu vererek çalıştır penceresinden CMD yazarak da komut istemine ulaşılabilir.
➢ Komut isteminde IPCONFIG komutunu kullanarak kendi IP adresinizi öğreniniz. 	➢ IP adresi kısmında kendi bilgisayarınızın IP adresi bilgisini bulacaksınız.
➢ PING komutu ile kendi IP adresinize ping atınız.	➢ Gelen yanıtlarda paket erişim bilgilerini göreceksiniz.
➢ Ağınızda bulunmayan bir IP adresine PING atınız.	➢ Yanıt gelmediğini göreceksiniz.
➢ Bildiğiniz bir internet adresine PING atınız. Örneğin www.google.com.tr	➢ Paket erişim sürelerini kontrol ediniz. Kendi ağınız üzerindeki PING sonuçlarıyla karşılaştırınız.
➢ PING raporundan www.google.com.tr sitesinin IP adresini alınız.	➢ Ping raporu satırlarında IP adresini göreceksiniz.
➢ TRACERT komutu ile bu IP adresini kontrol ediniz.	➢ www.google.com.tr sitesine ulaşmak için üzerinden geçtiğiniz ağ aygıtlarını göreceksiniz.

Öğretmenlerinizin ayrıca vereceği önerileri uygulama faaliyeti tablosuna not ediniz.

ÖLÇME VE DEĞERLENDİRME

Bu bölümde birinci öğrenme faaliyetinde verilen bilgilere hâkimiyetinizi ve konuyu kavrama düzeyinizi ölçecek sorular sorulacaktır. Soruları bu düşünce doğrultusunda cevaplayınız.

ÖLÇME SORULARI

Aşağıda verilen sorular için uygun cevap seçeneğini işaretleyiniz.

1. Aşağıdakilerden hangisi ICMP mesajı kullanan komutlardan biridir?
A) COPY
B) NETSTAT
C) PING
D) IPCONFIG

2. PING komutunun kullandığı mesaj türü aşağıdakilerden hangisidir?
A) Yeniden Yönlendirme Mesajı
B) Yankı ve Yankı Yanıt Mesajı
C) Hedef Ulaşılamaz Mesajı
D) Bilgi İsteği ve Yanıt Mesajı

3. Aşağıdakilerden hangisi hata mesajlarından biri **değildir**?
A) Hedef Ulaşılamaz Mesajı
B) Tıkanıklık ve Akış Kontrol Mesajı
C) Parametre Hatası
D) Paket Yaşam Süresi Doldu Mesajı

4. Paketlerin geçebileceğini ağ elemanı sayısını hangi parametre belirler?
A) Hizmet Türü
B) Yankı İstek Sayısı
C) TTL (Yaşam Süresi)
D) Zaman Aşımı

5. Ping ile kontrol edilen hedef sistem kapalı ise aşağıdaki mesajlardan hangisi gelir?
A) Yankı Yanıtı
B) Paket Yaşam Süresi Doldu
C) Kaynak Yavaşlatma Mesajı
D) Hedef Ulaşılamaz

6. Tracert komutu aşağıdaki mesajlardan hangisini kullanır?
A) Yankı İsteği Mesajı
B) Yönlendirme Mesajı
C) Geçiş Zamanı Tahmin Mesajı
D) Hedef Ulaşılamaz Mesajı

7. Mesajın başlık parametreleri hatalı ise geri döndürülen mesaj aşağıdakilerden hangisidir?
A) Hatalı Başlık Mesajı
B) Yankı İsteği Mesajı
C) Parametre Hatası Mesajı
D) Yaşam Süresi Doldu Mesajı

8. Parçalı mesajlar birleştirilirken eksik parçalar geçerli süre içerisinde gelmez ise geri döndürülen mesaj aşağıdakilerden hangisidir?

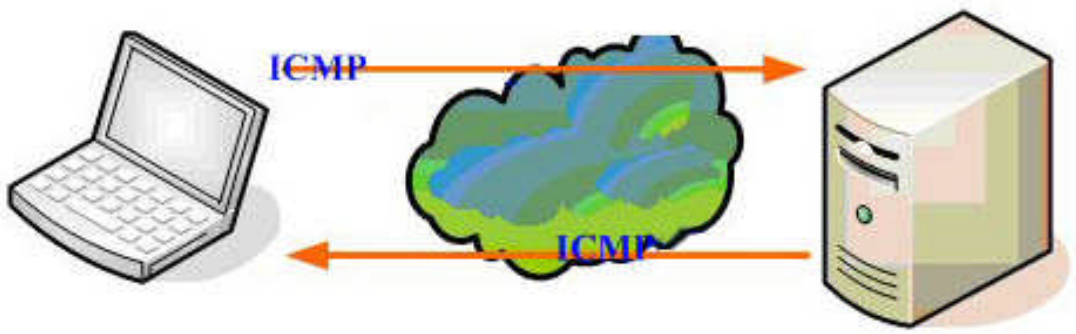
A) Azami Atlama Sayısı Aşıldı
C) Bekleme Süresi Doldu Mesajı
B) Parametre Hatası Mesajı
D) Paket Yaşam Süresi Doldu Mesajı

9. Gönderilen bir paket, yönlendirici üzerinde küçük parçalara ayrılması gerekirken ayrılması "parçalanmasın" bayrağı ile engellenmişse geri dönen mesaj aşağıdakilerden hangisidir?

A) Hedef Ulaşılamaz Mesajı
B) Paket Yaşam Süresi Doldu Mesajı
C) İşaretçi Hata Gösteriyor
D) Parçaları Yeniden Birleştirme Süresi Dolmuştur

10. Aşırı mesaj trafiği nedeniyle hedef sistemin istemciyi bilgilendirmek için kullandığı mesaj aşağıdakilerden hangisidir?

A) Kaynak Yavaşlatma Mesajı
C) Zaman Ayarlama Mesajı
B) Yaşam Süresi Mesajı
D) Yankı Mesajı



DEĞERLENDİRME

Sorulara verdiğiniz cevap seçeneklerini modül sonunda verilmiş olan cevap anahtarı ile karşılaştırınız. Kendinizi değerlendirdiğinizi unutmayınız. Yanlış cevapladığınız ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konular için bilgi sayfalarına tekrar dönerek eksiklerinizi gideriniz.

Konu ilginizi çektiyse araştırma yaparak daha detaylı bilgi edinip kendinizi geliştirebilirsiz.

ÖĞRENME FAALİYETİ–2

AMAÇ

ICMP kontrol mesajlarının parametrelerinin kullanımını kavrayıp bu mesajları ağda kullanarak bağlantıları test edebileceksiniz.

ARAŞTIRMA

- Bilgisayarlar arası bağlantıların neden kontrol edilmesi gerektiğini ve bu bağlantıların test edilme şekillerini araştırınız. Edindiğiniz bilgileri sınıfta paylaşınız.

2. TCP/IP KONTROL MESAJLARI

IP protokolü tek başına paketlerin gönderildiği sistemlere bilgilendirme ya da kontrol mesajları gönderemez. Böyle bir yeteneğe sahip olmadığı için de ICMP kontrol mesajlarından faydalanır. ICMP, hedef sisteme gönderdiği kontrol mesajları ile elde ettiği bilgileri kaynak sisteme taşır.

ICMP hata mesajları aşağıdaki durumların oluşması sonucu hazırlanır ve kaynak sisteme gönderilir.

- İletim esnasında paketler kaybolursa,
- İletimi sırasında hata oluşursa.

ICMP kontrol mesajları ise aşağıdaki durumlarda kaynak sistemi bilgilendirmek için kullanılır.

- Ağ tıkanıklığı gibi durumlarda,
- Hedef sisteme giden daha iyi bir yol olduğunda.

ICMP hata mesajları herhangi bir hata oluştuğu zaman, bu hataları kaynak sisteme bildirmek amacıyla kullanılırken ICMP kontrol mesajları ise hata durumlarını değil ağ durumunu kontrol etmek, ağ hakkında bilgi edinmek amacıyla kullanılırlar.

Bu bölümün ilerleyen başlıklarında ICMP kontrol mesajlarını, bu kontrol mesajlarının içeriklerini ve hangi amaçlarla, neden kullanıldıklarını öğreneceksiniz.

2.1. ICMP Kontrol Mesajları

Bağlı bulunulan ağ hakkında bilgi toplamak amacıyla kullanılan ICMP kontrol mesajları diğer protokol paketlerinde olduğu gibi IP datagramı içine yerleştirilerek gönderilirler.

Bilgi edinmek amacıyla kullanılan ICMP kontrol mesajları şunlardır:

- Yeniden yönlendirme / değiştirme isteği,
- Zaman eşlemesi ve geçiş zamanı tahmini,
- Bilgi isteği ve yanıt mesajı,
- Adres maskesi isteği,
- Yönlendirici belirleme mesajı,
- Yönlendirici talep mesajı,
- Tıkanıklık ve akış kontrol mesajı.

Şimdi bu mesajları ayrı ayrı inceleyelim.

2.1.1. Yeniden Yönlendirme / Değiştirme İsteği

ICMP Redirect/Change Request - Bu tip mesajlar yalnızca ağ geçitleri tarafından hazırlanıp gönderilebilirler.

Bir bilgisayar doğrudan bağlı iki veya daha fazla yönlendirici bulunan bir ağ segmentine bağlandığı zaman bilgisayarın varsayılan ağ geçidi, diğer yönlendiricilerden biri hedef sisteme giden daha iyi bir yola sahipse yeniden yönlendirme mesajını kullanabilir.

Şekil 2.1: Yeniden yönlendirme/değiştirme kontrol mesajı yapısı

Kod Degeri	Gerekli İşlem
0	Ağ için Yönlendirilen Datagramlar
1	Hedef Sistem için Yönlendirilen Datagramlar
2	Servis Tipi ve Ağ için Yönlendirilen Datagramlar
3	Servis Tipi ve Hedef Sistem için Yönlendirilen Datagramlar

Şekil 2.2: Yeniden yönlendirme/değiştirme kontrol mesaj kod değerleri

Tip: 13 Zaman Eşleme İsteği
14 Zaman Damga Yanıtı

Kod: 0

Açıklama

Varsayılan ağ geçidinin yeniden yönlendirme ve değiştirme mesajı, veri paketinin geldiği sistemle yönlendirilen bir sonraki sistem arabirimleri aynı olduğu durumlarda kullanılır. Diğer bir deyişle paketin geldiği IP adresi ile paketin yönlendirildiği IP adresinin alt ağ maskeleri aynı ise veya yönlendirici yeniden yönlendirme için ayarlanmışsa gönderilir.

2.1.2. Zaman Eşleme ve Geçiş Zamanı Tahmini

Şekil 2.3: Zaman eşleme ve geçiş zamanı tahmin mesajı

IP Alanları

Adresler: Zaman damga mesajının gönderen adresi zaman damga yanıt mesajındaki alıcı adresi olacaktır. Bir yankı yanıt mesajı oluşturulurken yalnızca kaynak ve hedef adresleri yer değiştirilir, tip kodu 0'a değiştirilir ve kontrol kısmı yeniden hesaplanır.

ICMP Alanları

Tip: 13 Zaman damga mesajı
14 Zaman damga yanıt mesajı

Kod: 0

Tanımlayıcı: Eğer kod "0" ise, zaman damga ve zaman damga yanıtının uyumuna yardımcı bir tanımlayıcıdır, "0" olabilir.

Sıra Numarası: Eğer kod "0" ise, zaman damga ve zaman damga yanıtının uyumuna yardımcı bir sıra numarasıdır, "0" olabilir.

Açıklama

Karşılıklı zaman eşlemesi yapmak amacıyla kullanılır. Gelen mesajda alınan zaman bilgisi, yanıt mesajına değiştirilmeden yerleştirilir, ek birkaç zaman bilgisi daha eklenerek yanıt mesajı oluşturulur ve gönderilir. Zaman bilgisi 32 bit uzunluğunda gece yarısından itibaren hesaplanan milisaniye cinsindendir.

Orijinal zaman bilgisi, göndericinin mesaja göndermeden önceki son dokunuş zamanıdır. Alım zamanı ise alıcının mesajla ilk temas zamanıdır. Son olarak gönderim zamanı ise alıcının yanıt mesajını göndermeden önceki mesaja son dokunuş zamanıdır.

Eğer zaman bilgisi milisaniye cinsinden veya gece yarısından itibaren hesaplanmış bir zaman değilse, alıcı rastgele bir zaman belirler ve zaman bilgisinin en yüksek değerlikli bitini "1" yaparak bu bilginin standart bir zaman bilgisi olmadığını belirtir.

Tanımlayıcı ve sıra numarası, gönderici tarafından mesajlarının gelen yanıtlarla uyumluluğunu belirlemek için kullanılır.

2.1.3. Bilgi İsteği ve Yanıt Mesajı

Şekil 2.4: Bilgi isteği ve yanıt mesajı

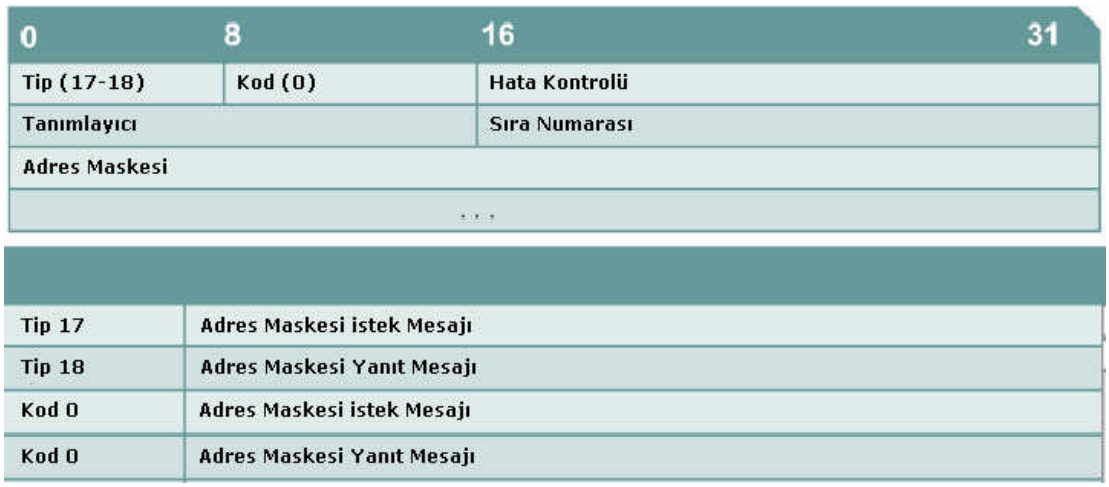
Tip: 15 Bilgi istek mesajı
16 Bilgi yanıt mesajı

Kod: 0

Açıklama

Bir bilgisayarın bağlı bulunduğu ağın ağ adresini öğrenmek için kullandığı bir çeşit ICMP kontrol mesajıdır.

2.1.4. Adres Maskesi İsteği



Şekil 2.5: Adres maskesi isteği

Tip: 17 Adres maskesi isteği
18 Adres maskesi yanıtı

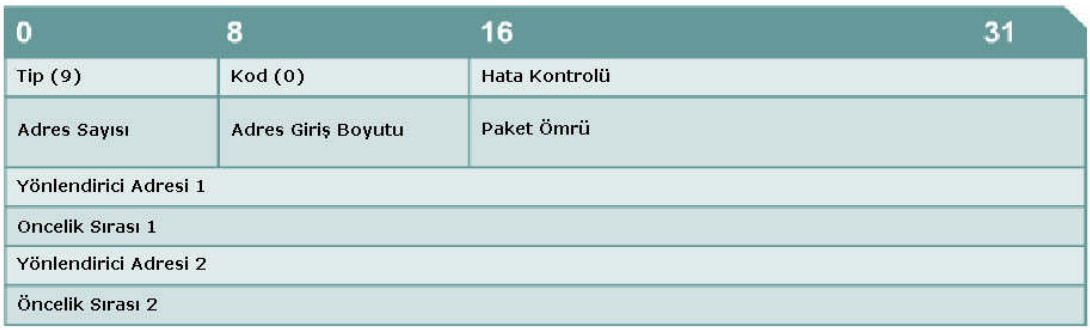
Kod: 0

Açıklama

Alt ağlara ayrılmış bir sistemde bulunan bir bilgisayar tarafından bağlı bulunduğu ağın alt ağ maskesini belirlemek için kullandığı bir mesajdır. Yönlendirici adresi biliniyorsa mesaj doğrudan yönlendiriciye gönderilir. Aksi hâlde ağ üzerinde yayın yapılarak ilgili sistemin cevabı beklenir.

Bu mesaj türü sabit diski bulunmayan sistemlerde kullanılır. Sistemde kullandığı aygıtların IP adreslerini ve adres maskelerini kaydedebileceği bir diski bulunmadığı için kullanacağı ağ aygıtlarının adres maskelerini bu mesaj aracılığı ile ister. Bu mesaja karşılık verilen yanıt mesajlarında da istenilen aygıtın adres maskesi bulunur.

2.1.5. Yönlendirici (Router) Belirleme Mesajı



Şekil 2.6: Yönlendirici belirleme mesajı

Adres Sayısı: Mesajda belirtilen yönlendirici sayısı.

Adres Giriş Boyutu: Her bir yönlendirici adres bilgileri için 32 bitlik kelime sayısı.

Yaşam Süresi: Yönlendirici adreslerin geçerli olduğunun düşünüldüğü saniye cinsinden azami süre.

Yönlendirici Adresi [i]: Bu mesajı gönderen yönlendiricinin [i] IP adresidir.

Öncelik Sırası [i]: Her bir yönlendiricinin tercih edilebilirlik değeridir. Yüksek değer tercih edilebilirliği gösterir.

Açıklama

Ağ üzerindeki yetkili yönlendiriciyi belirlemek için kullanılan bir mesajdır. Ağ üzerinde yönlendirici yayın adresine gönderilir ve yetkili yönlendirici yanıt verir.

2.1.6. Yönlendirici (Router) Talep Mesajı

Bilgisayar, eksik olan varsayılan ağ geçidi adresi almak için yönlendirici talep mesajı oluşturur. Bu mesaj bütün ağa gönderilir ve bu işlem yönlendirici belirleme sürecinin ilk adımıdır. Yerel (ağa bağlı) bir yönlendirici bu mesaja karşılık varsayılan ağ geçidi adresini içeren bir yanıt mesajı gönderir.

Şekil 2.7: Yönlendirici talep mesajı

IP Alanları

Kaynak Adres : Bu mesajı gönderen sisteme ait IP adresi.
Hedef Adres : Talep edilen adres.
Yaşam Süresi : Hedef adres bir ağ yayın adresi. Değeri en az 1 olmalıdır.

ICMP Alanları

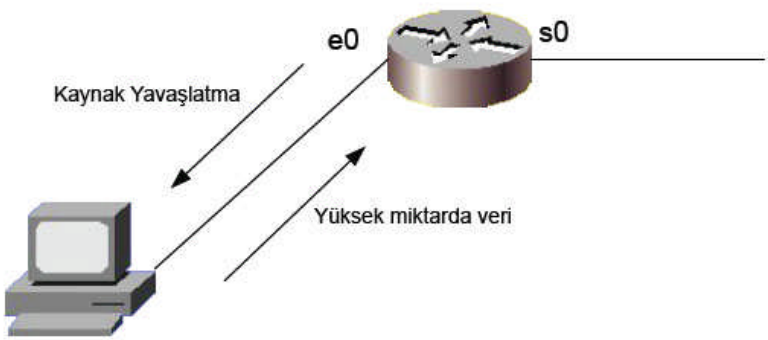
Tip: 10

Kod: 0

Hata Kontrolü: ICMP tipiyle başlayan ICMP mesaj toplamının 1'in tümlerinin 16 bitlik 1 tümleyeni.

Rezerve: Gelecekte kullanılmak üzere ayrılmış alan.

2.1.7. Tıkanıklık ve Akış Kontrol Mesajı



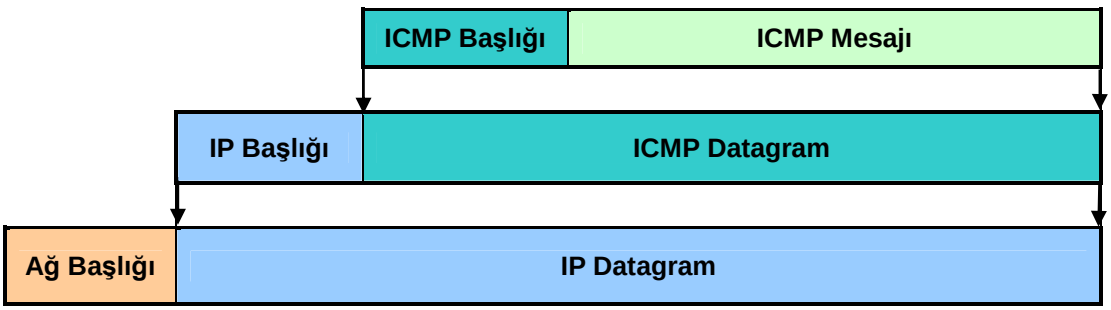
Şekil 2.8: Tıkanıklık ve akış kontrol mesajı

Bir sisteme çok fazla istekte bulunulur veya aynı sisteme hızlı bir şekilde yoğun bilgi gönderilirse hedef sistem aşırı talebi karşılayamayacağı için tıkanıklık oluşur. Bu tıkanıklığı önlemek için istekte bulunan sistemlere kaynak yavaşlatma ICMP mesajı gönderir.

2.2. ICMP Kontrol Mesajlarının Ağda İletimi

ICMP kontrol mesajları bir ağ hakkında bilgi toplamak amacıyla kullanılır. Örneğin bilgisayarınızın statik bir IP adresi, varsayılan ağ geçidi gibi bilgileri yok. Varsayılan ağ geçidi ve IP adresi bilgilerini ortamdaki bir yönlendiriciden veya DHCP sunucudan alması gerekmektedir. Ağ geçidi adresini almak için ağ geneline bir istek mesajı yayınlar ve bunu alan yönlendirici mesaj sahibine istediği bilgiyi derhal gönderir.

Kontrol mesajları hata bildirimi için değil bilgi toplamak için kullanılırlar. Yapısal olarak UDP'ye benzer. UDP veri paketlerinde olduğu gibi, mesajlarını datagrama yerleştirerek gönderir, fakat UDP'den daha basit bir yapıya sahiptir. UDP veri paketlerinde kaynak ve hedef portlar bulunurken ICMP paketinde port numarası bulunmaz. Bütün ICMP mesajları ağda kullanılan yazılım tarafından yorumlanır. Bu nedenle mesajın hangi porta gideceğinin önemi yoktur. Bütün yazılımlar ICMP mesajlarını tanırlar.



Şekil 2.9: ICMP mesaj paket yapısı

Şekilde gösterilen ICMP mesaj paketinde ICMP mesajına ICMP başlığı eklenerek IP katmanına iletiliyor. IP katmanında hedef bilgisayarın IP adresini içeren bir IP başlığı eklenerek fiziksel katmana iletiliyor. Fiziksel katmanda, fiziksel adresleri içeren ağ başlığı eklenerek ICMP mesajı gönderilmeye hazır hâle geliyor.

ICMP, IP katmanı ile aynı seviyede olmasına rağmen bir üst katman protokolü gibi davranarak temel IP desteğini kullanır. Bununla birlikte ICMP aslında IP'nin önemli bir parçasıdır ve IP modülleri tarafından tamamlanmalıdır.

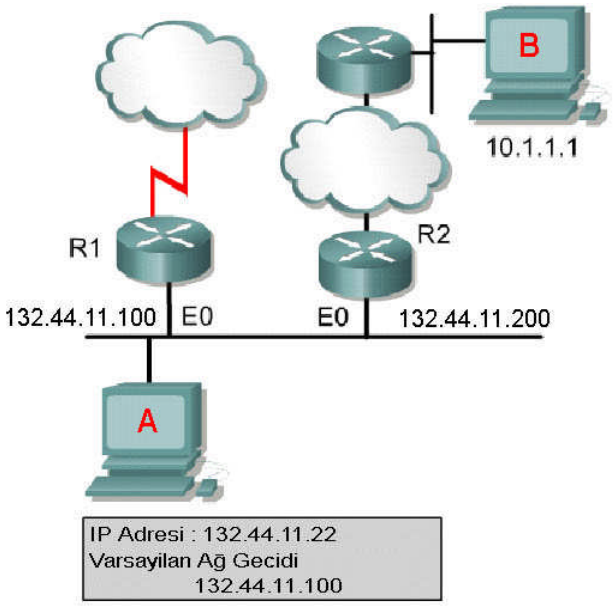
ICMP mesajları birçok durumda gönderilebilir.

ICMP mesajı ICMP başlığı ile birlikte paketlenerek ICMP datagramı hâline getirilir. Daha sonra bu datagrama gönderen sistemin ve hedef sistemin IP adreslerini içeren IP başlığı eklenerek IP datagram hâline getirilir ve iletilmek üzere bir altta bulunan fiziksel katmana geçer. Fiziksel katmanda ise ağ başlığı bilgileri eklenen IP datagramı artık hedefe doğru gönderilmeye hazırdır.

ICMP mesajını alan sistem mesajdaki isteğe yanıt verir. Yanıt adresini de gelen paketteki gönderici adresinden alır. Böylece yapılan bilgi isteğinin yanıtı gelmiş ve ağ hakkında istenilen bilgi alınmış olur.

ICMP mesajları oldukça yararlı bir sistem olmasına karşın kötü amaçlarla da kullanılabilmektedir. Örneğin bir ağ üzerinde bir bilgisayara yüksek sıklıkta ICMP mesaj paketleri gönderilerek ağ yavaşlatılabilmekte ve hatta ilgili sistemin ağ bağlantısı kullanılamaz hâle getirilebilmektedir. Yeni Windows sürümleri bu gibi durumlara karşın PING istemlerine yanıt vermez. Ağı çok meşgul eden TRACERT işlemine de engel olabilmektedir.

2.2.1. Yeniden Yönlendirme ve Değiştirme İstek Mesajı İletimi



Şekil 2.10: Yeniden yönlendirme işlemi

Şekil 2.10'daki sistemde A bilgisayarının bağlı bulunduğu ağ R1 ve R2 olmak üzere iki adet yönlendirici ile WAN bağlantısı yapılmıştır. A bilgisayarı B bilgisayarı ile iletişim kurmak istiyor. Varsayılan ağ geçidi R1 üzerinde E0'dır. Fakat şekilde de görüldüğü gibi, R2 üzerinden hedef bilgisayara ulaşmak için daha iyi bir yol var. R1 yönlendiricisi A bilgisayarına R1 yönlendiricisinin üzerinden bağlanması için yeniden yönlendirme/ değiştirme ICMP kontrol mesajı gönderiyor.

2.2.2. Zaman Eşleme ve Geçiş Zamanı Tahmin Mesajı İletimi

Farklı ağlarda bulunan ve zaman eşlemesi gerektiren yazılım kullanan sistemler bazen problem çıkarabilir. ICMP Zaman Eşleme mesajı bu problemi azaltmada yardımcı olmak için tasarlanmıştır. ICMP Zaman Eşleme mesajı (13) hedef sisteme göre o andaki saati sorma fırsatı tanır. Hedef sistem ICMP Zaman Eşleme Yanıt mesajı (14) kullanarak isteğe yanıt verir. Uzak sistem ve ağdaki toplam iletim zamanı üzerinde yaklaşık bir zaman almanın kolay bir yoludur.

Şekil 2.11: Zaman eşleme mesajı

TCP/IP'nin üst katmanlarındaki Ağ Zaman Protokolü (NMP – Network Time Protocol) daha güvenilir bir zaman eşlemesi sağlar.

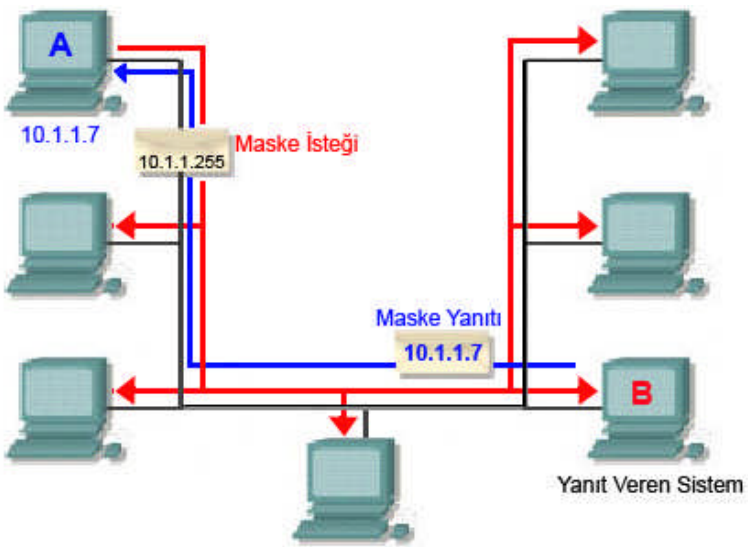
2.2.3. Bilgi İsteği ve Yanıt Mesajı

ICMP bilgi isteği ve yanıt mesajı sistemin kendi ağ adresini belirlemesine imkân sağlamak için tasarlanmıştır.

Bilgi isteği dış ağdan veya yerel ağdan gelebilir. Eğer yerel ağ içerisinden geliyorsa hedef adres 0 olur. Dış ağdan gelen bir istekte ise hedef adres boş olmaz. Bu isteğe yanıt veren yönlendirici kaynak ve hedef adresleri yer değiştirir, mesaja ağ adresini ekleyerek yanıt verir.

Günümüzde bu mesaj kullanılırlığını yitirmiştir. Bunun yerine daha etkili olan DHCP ve BOOTP gibi protokoller geliştirilmiştir. ICMP mesajları genellikle firewall engeline takılmaktadırlar. DHCP ve BOOTP protokollerinin yaygın olarak kullanılmaktadır.

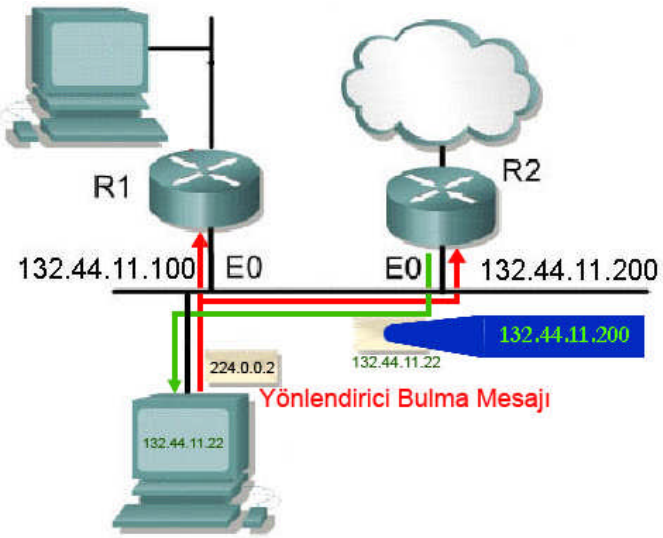
2.2.4. Adres Maskesi İsteği ve Yanıt Mesajı İletimi



Şekil 2.12: Adres maske isteği iletimi

Diski bulunmayan bu sistemler kendilerine bir IP adresi aldıktan sonra bulundukları ağ içerisinde 10.1.1.255 yayın adresine adres maskesi isteğinde bulunur. Ağ üzerinde adres maskesi isteklerine cevap vermek üzere ayarlanmış olan bir sistem bu mesajı aldıktan sonra mesaj içerisine adres maskesi bilgisini ekler, mesaj tipini 18 olarak, kaynak adresi de hedef adres olarak değiştirir, adres maskesi istek mesajını adres maskesi yanıt mesajına dönüştürür ve mesaj sahibine gönderir.

2.2.5. Yönlendirici (Router) Belirleme ve Talep Mesajı



Şekil 2.13: Yönlendirici belirleme mesajı

Eğer ağdaki bilgisayarın varsayılan bir ağ geçidi yoksa hedef adres olarak 224.0.0.2 numaralı çoklu yayın IP adresini kullanarak ağında bulunan bütün yönlendiricilere "yönlendirici bulma mesajı" gönderir. Eğer mesaj gönderilen yönlendirici, yönlendirici belirleme mesajını desteklemiyorsa, bu istek yanıtsız kalır. Eğer destekleniyorsa mesaj, yönlendirici kendisine ait bilgileri istekte bulunan siteme göndererek kendini tanıtacaktır.

Aynı yöntemle yönlendirici talep mesajı gönderilerek varsayılan ağ geçidi bilgisi de alınır.

2.2.6. Tıkanıklık ve Akış Kontrol Mesajı İletimi

Şekil 2.14: Tıkanıklık ve kaynak yavaşlatma mesaj iletimi

Aynı hedef sisteme aynı anda birçok erişim istemlerinde yüksek hızlı ağlar gittikçe yavaşlar. Bir süre sonra yoğun erişimden dolayı tıkanır. Eğer ağ trafiği çok yoğun ise paket kayıpları gittikçe artmaya başlar. Bu kayıpları azaltmak için sistem istek paketleri gönderen sistemlere gönderdikleri paketleri azaltmaları için ICMP kaynak yavaşlatma mesajı ile istekte bulunur. Bu mesajı alan sistemler paket gönderim hızlarını düşürürler.

İstekte bulunan sistemler yeteri kadar yavaşlamadıkları sürece bu mesajı almaya devam ederler. Yeteri kadar yavaşladıktan sonra tekrar kaynak yavaşlatma isteği gelene kadar yavaş yavaş hızlarını arttırmaya başlarlar.

ICMP Tip Numaraları

Internet Control Message Protocol (ICMP) tip alanıyla tanımlanmış birçok mesaja sahiptir. Bu tip numaraları ve ilgili mesajlar şunlardır:

Tip	Mesaj	Kod	Referans
0	Yankı Yanıtı	0 Kod Yok	RFC792
1	*Tanımlanmamış*		*Jon Postel*
2	*Tanımlanmamış*		*Jon Postel*
3	Hedef Ulaşılamaz	0 Ağ Erişilemez 1 Sistem Erişilemez 2 Protokol Erişilemez 3 Port Erişilemez 4 Bölünme gerekli bölünmez bayrağı işaretli 5 Kaynak yol başarısız 6 Hedef ağ bilinmiyor 7 Hedef sistem bilinmiyor 8 Kaynak sistem korumada 9 Hedef ağ bağlantısı yönetimsel olarak yasaklanmış 10 Hedef sistem bağlantısı yönetimsel olarak yasaklanmış 11 Servis tipi için hedef ağ erişilmez 12 Servis tipi için hedef sistem erişilmez 13 Bağlantı yönetimsel olarak yasaklanmış 14 Kaynak önceliği yok 15 Öncelik kesimi etkili	RFC792
4	Kaynak Yavaşlat	0 Kod yok	RFC792
5	Yeniden Yönlendirme	0 Ağ için datagram yönlendir. 1 Sistem için datagram yönlendir. 2 Servis tipi ve ağ için datagram yönlendir. 3 Servis tipi ve sistem için datagram yönlendir.	RFC792
6	Alternatif Sistem Adresi	0 Sistem için adres alternatifi	Jon Postel
7	*Tanımlanmamış*		*Jon Postel*
8	Yankı İsteği	0 Kod yok	RFC792
9	Yönlendirici Bildirimi	0 Normal yönlendirici bildirimi 16 Genel trafiği yönlendirme	RFC1256
10	Yönlendirici Talebi	0 Kod yok	RFC1256

11	Zaman Aşımı	0 İletimde yaşam süresi doldu 1 Bölüm yeniden düzenleme süresi doldu	RFC792
12	Parametre Problemi	0 İşaretçi hata veriyor 1 Gerekli seçeneklerden biri eksik 2 Geçersiz uzunluk	RFC792
13	Zaman Damgası	0 Kod yok	RFC792
14	Zaman Damga Yanıtı	0 Kod yok	RFC792
15	Bilgi İsteği	0 Kod yok	RFC792
16	Bilgi Yanıtı	0 Kod yok	RFC792
17	Adres Maskesi İsteği	0 Kod yok	RFC950
18	Adres Maskesi Yanıtı	0 Kod yok	RFC950
19	*Güvenlik İçin Ayrılmış*		*Solo*
20-29	*Sağlamlık Deneyleri İçin Ayrılmış*		*Zaw-Sing Su*
30	Traceroute		RFC1393
31	Datagram Dönüşüm Hatası		RFC1475
32	Mobil Sistem Yeniden Yönlendirmesi		David Johnson
33	IPv6 Neredesin		Bill Simpson
34	IPv6 Buradayım		Bill Simpson
35	Mobil Kayıt İsteği		Bill Simpson
36	Mobil Kayıt Yanıtı		Bill Simpson
37	Domain İsim İsteği		RFC1788
38	Domain İsim Yanıtı		RFC1788
39	Atla		Tom Markson
40	Photuris	0 = Geçersi SPI 1 = Doğrulanamadı 2 = Genişletme Başarısız 3 = Kod çözümü başarısız 4 = Doğrulama gerekli 5 = Yetki gerekli	RFC2521
41	*Seamoby gibi deneysel mobil protokol değerlendirme mesajları*		*RFC4065*
42-255	*Rezerve*		*Jon Postel*

Tablo 2.1: ICMP mesajları tip ve kod numaraları

UYGULAMA FAALİYETİ

İşlem Basamakları	Açıklamalar
➢ Ağınıza bağlı olan yönlendiricinin IP adresini öğreniniz.	➢ Ağınızda yönlendirici bağlı ise öğretmeninizden öğrenebilirsiniz.
➢ Başlar – Programlar – Internet Explorer seçeneğinden Internet Explorer programını açınız.	➢ Internet Explorer sayfası ile yönlendirici kontrollerine ulaşacağız.
➢ Internet Explorer penceresinde “adres” satırına yönlendirici IP adresini yazınız.	➢ Adres çubuğunda daha önceden bulunan adres varsa tamamen siliniz ve IP adresini yazınız.
➢ Yönlendiricinizin kontrol yazılımına girmiş oldunuz.	➢ Yönlendiricinizin yapılandırma ayarlarını buradan yapabilirsiniz.
➢ Yönlendirici kontrol sayfasında Firewall özelliklerine giriniz	➢ Firewall özelliklerinde yönlendiricinizin yapılması muhtemel saldırılara karşı koruma ayarları yapılır.
➢ Firewall ayarlarından Protection Policy ayarlarına giriniz.	➢ Saldırı önlemleri veya muhtemel güvenlik açıkları kapatılır.
➢ Protection Policy sayfasında göreceğiniz ICMP Redirection Checking özelliğinin yanındaki işaretini kaldırınız.	➢ Bu özellik iptal edilirse yönlendiriciniz yeniden yönlendirme ve değiştirme işlemi yapmaz.

Öğretmenlerinizin ayrıca vereceği önerileri uygulama faaliyeti tablosuna not ediniz.

ÖLÇME VE DEĞERLENDİRME

Bu bölümde birinci öğrenme faaliyetinde verilen bilgilere hâkimiyetinizi ve konuyu kavrama düzeyinizi ölçecek sorular sorulacaktır. Soruları bu düşünce doğrultusunda cevaplayınız.

ÖLÇME SORULARI

Aşağıda verilen sorular için uygun cevap seçeneğini işaretleyiniz.

1. Aşağıdakilerden hangisi ICMP kontrol mesajlarından biri **değildir**?
A) Adres Maskesi İstek Mesajı
B) Yeniden Yönlendirme Mesajı
C) Yönlendirici Talep Mesajı
D) Parametre Hatası Mesajı

2. Aşağıdakilerden hangisi hedefe giden daha uygun bir yol olduğu zaman gönderilen mesajdır?
A) Yeniden Yönlendirme Mesajı
B) Yönlendirici Belirleme Mesajı
C) Bilgi İsteği Mesajı
D) Yol Belirleme Mesajı

3. Bir sisteme yoğun bağlantı talebinde bulunulduğu zaman oluşan tıkanıklığı gidermek amacıyla hedef sistemin gönderdiği mesaj türü aşağıdakilerden hangisidir?
A) Bilgi İstek Mesajı
B) Geçiş Zamanı Tahmin Mesajı
C) Tıkanıklık ve Akış Kontrol Mesajı
D) Yönlendirici Talep Mesajı

4. Kaynak ve hedef sistemlerin zamanlarını karşılıklı ayarlamak için kullandıkları mesaj aşağıdakilerden hangisidir?
A) Zamanlama Kontrol Mesajı
B) Zaman Eşleme ve Geçiş Zamanı Tahmin Mesajı
C) Adres Maskesi İstek Mesajı
D) Akış Kontrol Mesajı

5. Ağ geneline gönderilen kontrol mesajı aşağıdakilerden hangisidir?
A) Yönlendirici Belirleme Mesajı
B) Adres Maskesi İstek Mesajı
C) Bilgi Yanıt Mesajı
D) Kaynak Yavaşlatma Mesajı

6. IP adresini otomatik olarak almış bir sistem varsayılan ağ geçidini bulmak için hangi mesajı kullanır?
A) Yönlendirici Talep Mesajı
B) Yeniden Yönlendirme ve Değiştirme İstek Mesajı
C) Yönlendirici Bulma Mesajı
D) Geçiş Zamanı Tahmin Mesajı

7. Mesaj paketlerinde bulunan tip numaralarının görevi nedir?
A) ICMP mesajına uygulanacak işlemleri belirler.
B) ICMP mesajının gideceği hedefi belirler.
C) ICMP mesajının türünü belirler.
D) ICMP mesajının takip edeceği yolu belirler.

8. ICMP mesaj paketinde bulunan kod alanının görevi nedir?
A) Mesajın gideceği sistemi belirler.
B) Mesajın üzerinden geçeceği ay aygıtlarının sayısını belirler.
C) Mesajın geldiği sistemi belirler.
D) Mesaj tipinin taşıdığı bilgi tipini belirler.

9. Ağdaki bir bilgisayar alt ağ maskesini bulmak için hangi mesajı kullanır?
A) Adres Maskesi İstek Mesajı
B) Yönlendirici Talep Mesajı
C) Bilgi İstek Mesajı
D) Yankı İstek Mesajı

10. Aşağıdaki ICMP mesajlarından hangisi ağ geneline gönderilen fakat yalnızca yönlendiriciler tarafından alınır?
A) Yeniden Yönlendirme Mesajı
B) Bilgi Yanıt Mesajı
C) Yönlendirici Belirleme Mesajı
D) Tıkanıklık ve Akış Kontrol Mesajı

DEĞERLENDİRME

Sorulara verdiğiniz cevap seçeneklerini modül sonunda verilmiş olan cevap anahtarı ile karşılaştırınız. Kendinizi değerlendirdiğinizi unutmayınız. Yanlış cevapladığınız yada cevap verirken tereddüt ettiğiniz sorularla ilgili konular için bilgi sayfalarına tekrar dönerek eksiklerinizi gideriniz.

Konu ilginizi çektiyse araştırma yaparak daha detaylı bilgi edinip kendinizi geliştirebilirsiz.

MODÜL DEĞERLENDİRME

YETERLİK ÖLÇME

Bu kısımda modül içerisindeki öğrenme faaliyetlerinde öğrendiğiniz bilgilerle ilgili, düşünce gücünüzü ölçecek sorular sorulacaktır. Bazı soruların cevaplarını hemen bulabilir, bazılarını cevaplamanız ise zaman alabilir. Bu düşünce ile hareket ederek soruları cevaplayınız

ÖLÇME SORULARI

Aşağıda verilen sorular için uygun cevap seçeneğini işaretleyiniz.

1. ICMP, TCP/IP katman mimarisinde hangi katmanda yer alır?
A) Uygulama Katmanı
B) Internet Katmanı
C) Taşıma Katmanı
D) Fiziksel Katman

2. Ping komutu ile kullanıcı durdurana kadar belirli aralıklarla kontrol yapmak için kullanılan parametre aşağıdakilerden hangisidir?
A) -t
B) -k
C) -l
D) -w

3. Aşağıdakilerden hangisi ICMP iletişiminin gerçekleşebilmesi için ihtiyaç **duyulmaz**?
A) Düzgün ayarlanmış IP ve alt ağ maskesi
B) Düzgün kurulmuş TCP/IP
C) Düzgün ayarlanmış ağ geçidi
D) En hızlı kablo bağlantısı kullanılmalı

4. Aşağıdaki ICMP mesaj alanlarından hangisi hata mesajlarında ortak değildir?
A) Kontrol Alanı
B) Kod Alanı
C) Sıra Numarası Alanı
D) Tip Alanı

5. Tracert komutunda gönderilen ICMP paketlerinin kaç ağ aygıtı üzerinden geçeceğini belirleyen parametre aşağıdakilerden hangisidir?
A) -d
B) -w
C) -j
D) -h

6. Aşağıdakilerden hangisi ICMP Hata Mesajı **değildir**?
A) Hedef Ulaşılamaz Mesajı
B) Tıkanıklık ve Akış Kontrol Mesajı
C) Paket Yaşam Süresi Doldu Mesajı
D) Yankı ve Yankı Yanıt Mesajı

7. Ağ içerisinde bir yönlendiriciye gelen pakette hedef sistem aynı ağ üzerinde bulunuyorsa hangi ICMP mesaj üretilerek kaynak sisteme gönderilir?
A) Yeniden Yönlendirme Mesajı
B) Yönlendirici Talep Mesajı
C) Hedef Ulaşılamaz Mesajı
D) Kaynak Yavaşlatma Mesajı

8. Yönlendirici Talep Mesajı aşağıdakilerden hangisine gönderilir?
A) Talep isteyen sisteme
B) İnternet servis sağlayıcısına
C) Yerel ağa
D) Talep isteyen yönlendiriciye

9. IP sisteminde ICMP mesajlarının kullanım en önemli sebebi aşağıdakilerden hangisidir?
A) IP sisteminin zahmetli olması.
B) IP sisteminde paketlerin iletilip iletilmediğine dair bilgilendirme sistemi olmaması.
C) IP sisteminin yavaş olması.
D) Ağ sistemlerinin kararlı çalışmaması.

10. Yönlendiricilere yayın yapılan IP adresi aşağıdakilerden hangisidir?
A) 224.0.0.2
B) 192.168.1.1
C) 127.0.0.1
D) 10.0.0.2

DEĞERLENDİRME

Modül sonunda ilgili testlere ait cevap anahtarları bulunmaktadır. Bu cevap anahtarlarını kontrol ederek kendinizi değerlendirebilirsiniz. Yaptığınız değerlendirme sonucunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

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

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

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

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

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

MODÜL DEĞERLENDİRME CEVAP ANAHTARI

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

KAYNAKÇA

- MALKING G., **Traceroute Using an IP Option**, RFC 1393, Xylogics, Inc., January 1993.
- POSTEL J., **Internet Control Message Protocol, DARPA Internet Program Protocol Specification**, RFC:792, USC/Information Sciences Institute, September 1981.
- QUITTEK J. Ed., WHITE K. Ed., **Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations**, IBM Corp. June 2006.
- SHIMONSKI Robert J., **Using Tracert**, Sep 29, 2005.
- http://www.cisco.com
- http://ictlab.tyict.vtc.edu.hk
- http://www.governmentsecurity.org