SAKARYA ÜNİVERSİTESİ

BİLGİSAYAR VE BİLİŞİM BİLİMLERİ

FAKÜLTESİ

AĞ PROGRAMLAMA PROJESİ

ICMP İstemci-Sunucu İletişimi Hata ve Raporlama Uygulaması

Seda Nur EREN B201210030

İlayda YILMAZ B201210057

Dilan ÇELİK B201210399

seda.eren@ogr.sakarya.edu.tr
ilayda.yilmaz3@ogr.sakarya.edu.tr
dilan.celik3@ogr.sakarya.edu.tr

2023-2024 Bahar Dönemi

ICMP PROTOKOLÜ NEDİR?

ICMP yani internet control message protocol ağdaki cihazların çalıştıklarını anlamamızı sağlayan protokoldür. Hata mesajları üreterek bilgisayarların kullanılabilirliğini doğrular.

ICMP'nin öncelikli hedefi ağdaki bilgisayarlara ping yollamaktır veya onları izleyebilmektedir. Kullanılabilirliği seyahat süresini ve rotayı bilgisayarlar vasıtasıyla ölçmek için ECHO ICMP talep mesajları gönderir. Yani ICMP, ağ bilgisayarı detaylarını belirleyen Ping ve Trace özelliklerini çalıştırır.

ICMP NERELERDE KULLANILIR?

Hata raporlama:

ICMP hata mesajları; ulaşılamayan hedefler, zaman aşımları veya parçalanma sorunları gibi ağ iletişimi hatalarını bildirir. Mesajlar özellikle de bağlantısız iletişim modeliyle çalışan Kullanıcı Veri Birimi Protokolü (UDP) için önemlidir.

UDP, güvenilir ve sıralı paket teslimatı sağlamaz. Bir UDP paketi gönderildiğinde, paketin kaybolması veya sağlama toplamı hataları gibi hatalarla teslim edilmesi ihtimal dahilindedir. Böyle bir durumda alıcı, sorunu göndericiye bildirmek için ICMP hata raporlama mesajlarını geri gönderir.

Tanılama:

Ağ tanılama için ICMP'yi kullanılabilir. Bu protokol en yaygın olarak ping ve traceroute komutları için kullanılır.

Ping komutu, ICMP yankı isteği paketlerini bir hedef cihaza göndererek ağ cihazlarının erişilebilirliğini test eder. Cihaza ulaşılabiliyorsa bir ICMP yankı yanıtı döndürür. Ağ gecikmesini güvenilir bir şekilde kontrol eder ve cihazın kullanılabilir olduğundan emin olur.

Traceroute komutu, paketlerin bir kaynaktan bir hedefe giderken takip ettiği yolu izler. Dolayısıyla bu komut, hedeflenen varış noktasına yankı isteği ve yankı yanıtı mesajları gönderir.

Yankı isteklerinin birer yaşam süresi (TTL) değeri vardır. Paket bir yönlendiriciden her geçtiğinde bu değer bir azalır. Bir paket TTL değeri sıfır olarak bir yönlendiriciye ulaştığında, yönlendirici kaynağa bir ICMP mesajı gönderir.

Mesaj, paketin izlediği rota hakkında bilgiler içerir. Traceroute, bir paketin izlediği yolu tam olarak ortaya çıkarır. Bu da size ağ performansı öngörüleri sağlayabilir.

ICMP mesajları network layerda iki temel versiyon halinde olur;

1. IPv4 için ICMPv4

2. IPv6 için ICMPv6

Sistem mesajları bir IP başlığı ile sarmalayıp datagramlar halinde iletir. Ve her cihazın IP paketleri için bir TTL değeri olur.

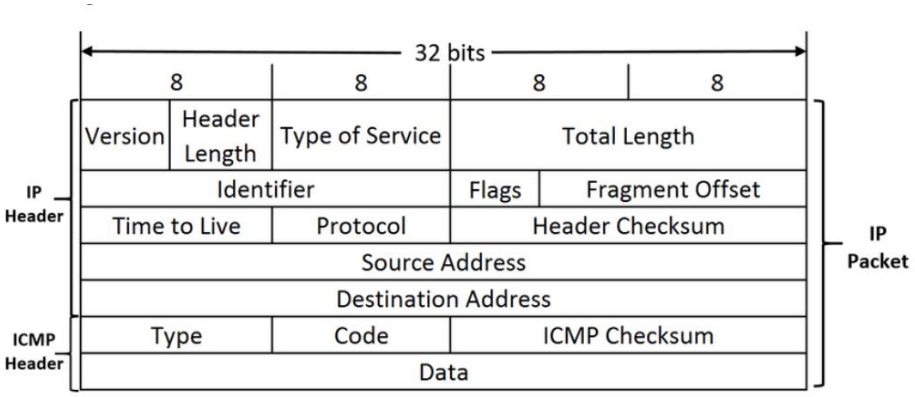
TTL (Time To Live) değeri 0 olunca kaynak için verilen süre aşıldı anlamına gelir ve ICMP de bu paket ile bağlantıyı doğrular.

Local Ağlarda sorunların tespitinde önemli rol oynayan ICMP, hata ve kontrol mesajları oluşturabilir. Bunun yanında problemlerin tespiti ve çözülmesine yardımcı olur. Web uygulamalarının ve protokollerinin birçoğu ICMP mesajlarını kullanır. Örneğin HTTP ve HTTPS gibi.

Ağ Güvenliği:

Yetkisiz ağ trafiğini saptamak ve ağ üzerinde yalnızca meşru trafiğe izin vermek için ICMP kullanılabilir. Güvenlik duvarları, belirli trafik türlerine izin vermek veya belirli trafik türlerini engellemek için ICMP kullanır. Ağ yöneticileri de hem ağ cihazlarının durumunu ve bağlantısını izlemek hem de bilinmeyen cihazları saptamak için ICMP izleme araçlarını kullanır.

Yetkisiz etkinliğe işaret edebilecek olağan dışı trafik örüntülerini tespit etmek için de bu protokol kullanılabilir.



ICMP Protokolü başlık yapısı

ICMP'nin bazı temel özellikleri şunlardır:

1. Hata Bildirimleri: ICMP, ağdaki hataları tespit etmek ve bildirmek için kullanılır. Örneğin, "Hedef Ulaşılamaz" hatası veya "Zaman Aşımı" hatası gibi durumlar ICMP mesajlarıyla bildirilir. Bu sayede ağ yöneticileri hataları tespit edebilir ve gerekli önlemleri alabilir.
2. Ping ve Traceroute: ICMP, ağdaki cihazların erişilebilirliğini kontrol etmek ve yolları belirlemek için kullanılan araçlardan olan "ping" ve "traceroute" komutlarında kullanılır. Ping komutu, bir hedef cihaza ICMP Echo Request (ping) mesajı göndererek yanıt alıp alamayacağını kontrol eder. Traceroute ise paketlerin hedefe giderken hangi ağ cihazlarından geçtiğini ve hangi yolları izlediğini belirlemek için ICMP Time Exceeded mesajlarını kullanır.
3. Yol Durumu Kontrolü: ICMP, ağ üzerindeki yolların durumunu izlemek için kullanılır. Örneğin, bir rota üzerindeki bir ağ cihazı hedefe ulaşamazsa, ICMP mesajlarıyla rota üzerindeki cihazların erişilebilirlik durumu kontrol edilir ve iletişim sorunları tespit edilir.

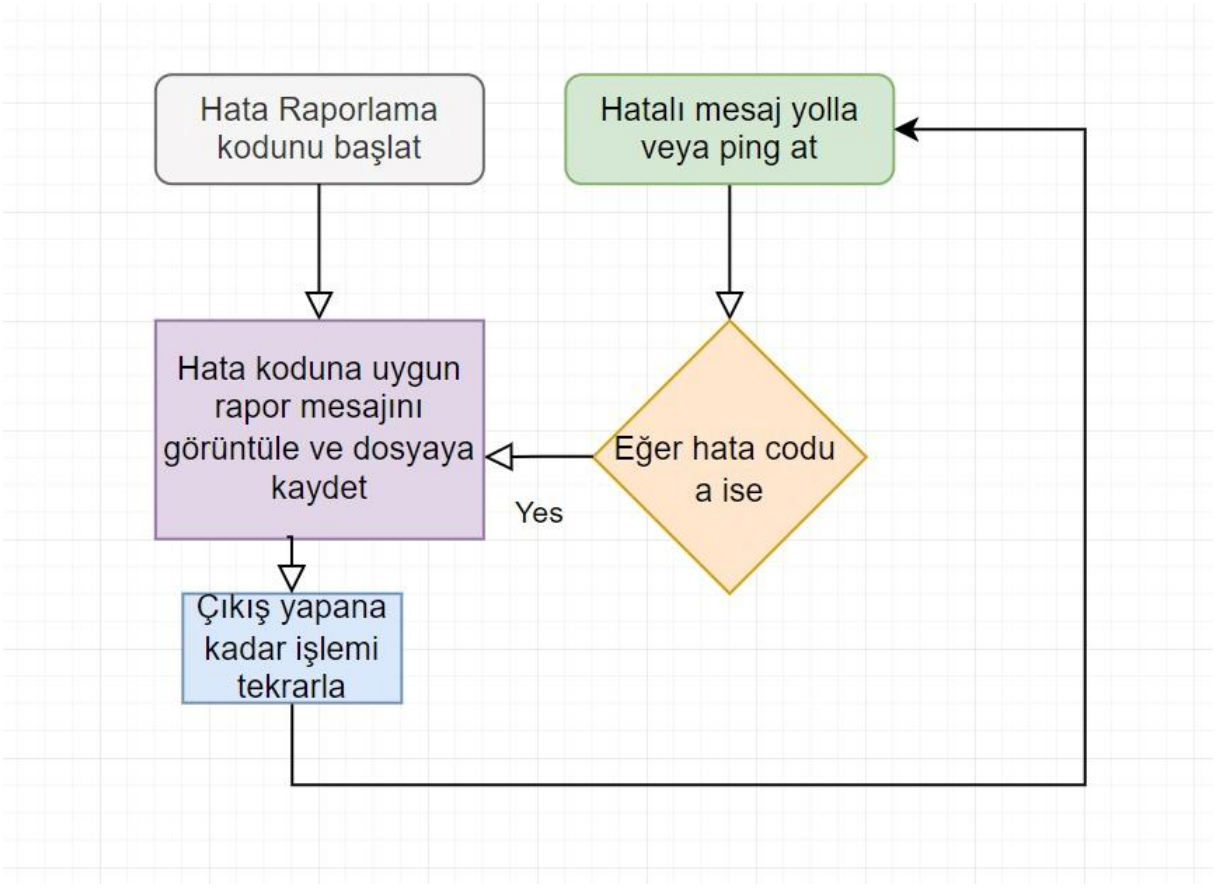
ICMP Hata Kodları Aşağıda Verilmiştir:

ICMP Message Category	Type	Message
Error / Reporting Messages	3	Destination Unreachable
	4	Source Quence
	5	Redirection
	11	Time Exceeded
	12	Parameter Problem
Information / Query Messages	0	Echo Request
	8	Echo Reply
	9	Router Advertisement
	10	Router Solicitation
	13	Timestamp Request
	14	Timestamp Reply
	15	Information Request
	16	Information Reply
	17	Timestamp Request
	18	Timestamp Reply

	Code	Meaning
Destination Unreachable	0	Network Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Fragmentation is Needed
	5	Source Route Failed
	6	Destination network Unknown
	7	Destination Host Unknown
	8	Source Host Isolated
	9	Destination Net Prohibited
	10	Destination Host Prohibited
	11	Network Unreachable for ToS
	12	Host Unreachable for ToS
	13	Communication Prohibited
	14	Host Precedence Violation
	15	Precedence cutoff in effect

Projemizde hata kodlarının hepsinin senaryosu uygulanmıştır.

ICMP İstemci sunucu hata raporlama uygulamasının UML Diyagramı aşağıdaki gibidir.

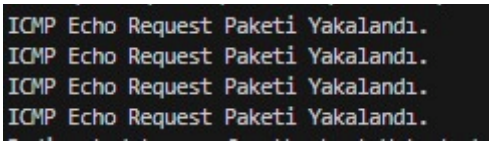


Program çalıştırıldığında aşağıdaki gibi bir menü ekrana çıkar ve kullanıcı yapmak istediği işlem için seçim yapar.

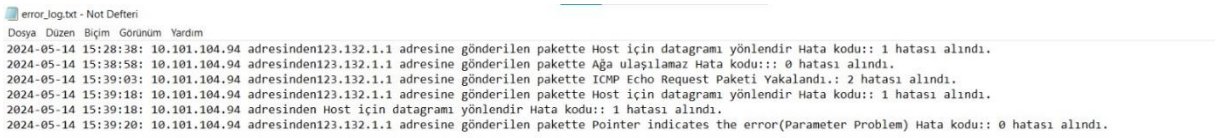
```
Yapmak istediğiniz işlemi giriniz:
1) Ping atmak
2) Hedefe ulaşılamadı hatası
3) Protokole ulaşılamadı hatası
4) Redirect for host hatası
5) Pointer indicates the hatası
Seçiminizi yapın (Çıkmak için 'c' girin): 1
Ping işlemi başlatılıyor...
Ping atmak istediğiniz IP adresini girin: 10.101.104.94
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Yukarıda ping atma işlemi yapılmaktadır. IP'si girilen cihaza ping atılmıştır fakat Windows işletim sistemi firewall'ı bu işlemin gerçekleşmesine izin vermemiştir.

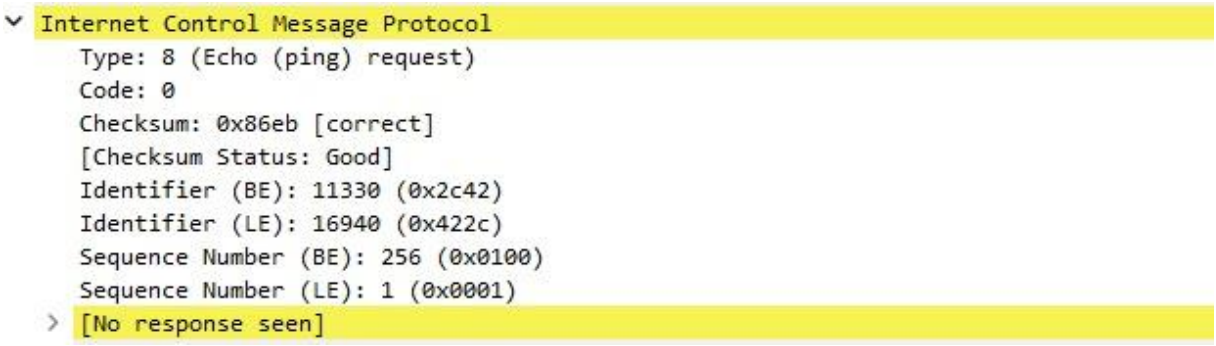
Sunucudan istemciye ping atıldığı zaman hata raporlama işlemini yapan kod aşağıdaki gibi bir çıktı vermektedir. Raporlama için ise dosyaya yazma işlemini gerçekleştirmektedir. Dosyanın içerisinde hata, kodu ıp adresleri ve hatanın gerçekleştiği tarih ve saat bilgileri yazılmaktadır.

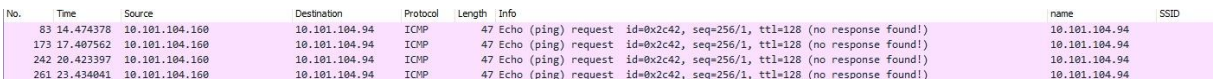


Dosyanın içeriği aşağıdaki gibidir.



Bu ping atma işlemi sırasında wireshark üzerinde trafik analizi yapıldı ve yakalanan paketin detayları aşağıda verilmiştir. Paketin içeriği aşağıdaki gibidir.





Programa başka bir hatalı icmp paketi yollandığında aldığımız trafik ve içeriği aşağıdaki gibidir.