ICMP (İnternet Control Message protocol) Protokolu

IP protokolu bağlantısız bir protokol olduğundan, ağda seyahat eden datagramların iletim ve teslimat sürecinde meydana gelen beklenmedik hata, uyarı, kontrol bilgilerinin alışverişi için ICMP protokolu kullanılır. Daha çok routerlar tarafından kullanılır. ICMP protokolu ağ hakkında bilgi sahibi olmak için de kullanılır (istek/cevap). ICMP iletileri IP datagramları içerisinde kapsüllenerek seyahat eder. Yani ICMP, IP protokolunun dahili bir parçasıdır ve her IP modülünde mevcuttur.

• **ICMP mesajları iki ana kategoriye ayrılır.**

***Sorgu mesajları :** Bilgisayar veya ağ testleri için veya ağ özelliklerinden bilgi elde etmek için ICMP mesajları kullanılır (ping, traceroute komutları v.b).

- İstekler (Requests)

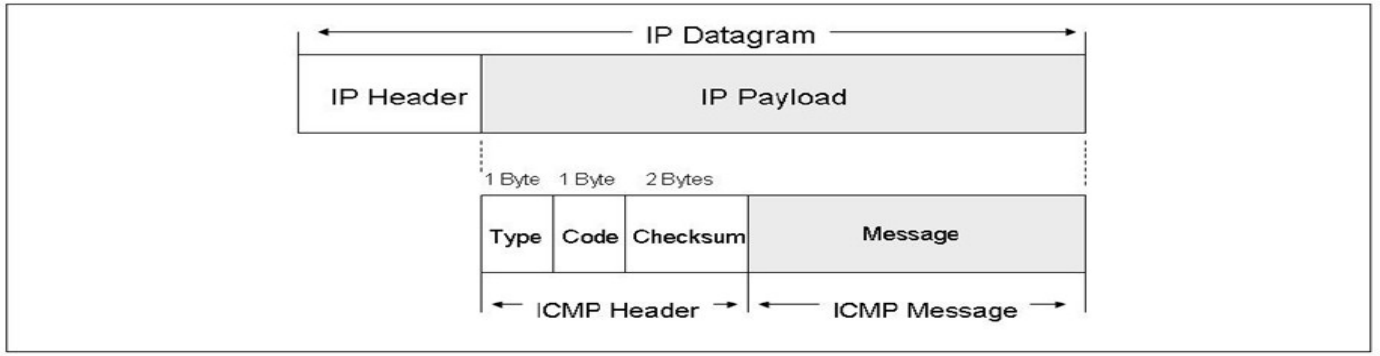
- Yanıtlar (Responses - reply)

* **Hata mesajları** : ICMP hata mesajını ağdaki tüm cihazlar, routerlarda dahil olmak üzere işleyebilir (Switchler işleyemez).

ICMP Hata mesajları aşağıdaki durumlarda üretilir.

- IP datagramların hedefe ulaşamaması durumunda
- Ağ geçitlerinin, datagramları hedefe yönlendiremeyecek kadar yoğun olmaları durumunda
- Datagramların hedeflerine gidebileceği daha uygun bir yol olması durumunda.
- Routerlar, datagramları yönlendirirken oluşabilecek problemleri bildirmek için
- Bilgisayarlar; protokol ve servis problemleri yaşadıkları zaman.
- **Sadece IP datagramlarla ilgili olaylarda ICMP mesajı üretilir.**
- Parçalanmış IP datagramlarda oluşacak hatalarda sadece ilki için ICMP mesajı iletilir.
- ICMP mesajlarının seyahat ile ilgili problemler için ICMP mesajı üretilmez.

ICMP Mesaj Formatı



ICMP header : **ICMP mesaj başlığı - 4 byte'tır.**

Type (Tür) : **ICMP mesajının türü - 1 byte,**

Code (Kod) : **ICMP mesajının alt türü, mesajı daha detaylı tanımlamak için -1 byte)**

Checksum : **ICMP mesajı için doğrulama, IP cehecsum'a benzer – 2 byte**

ICMP message : **Ek veri yoksa, 4 byte'lık 0 değeri olur.**

Her ICMP mesajı en az 8 bayttır.

ICMP Mesaj Formatı

MAC header	IP header	ICMP header	Data :::

ICMP header:

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type	Code	ICMP header checksum
Data :::		

Type. 8 bits.
Specifies the format of the ICMP message.

Type	Description
0	Echo reply.
1	
2	
3	Destination unreachable.
4	Source quench.
5	Redirect.
6	Alternate host address.
7	
8	Echo request.
9	Router advertisement.
10	Router solicitation.
11	Time exceeded.
12	Parameter problem.
13	Timestamp request.
14	Timestamp reply.
15	Information request. Obsolete.
16	Information reply. Obsolete.
17	Address mask request.
18	Address mask reply.
19	reserved (for security).
20 - 29	reserved (for robustness exp
30	Traceroute.
31	Conversion error.
32	Mobile Host Redirect.
33	IPv6 Where-Are-You.
34	IPv6 I-Am-Here.
35	Mobile Registration Request.
36	Mobile Registration Reply.
37	Domain Name request.
38	Domain Name reply.
39	SKIP Algorithm Discovery Prot
40	Photuris, Security failures.
41	Experimental mobility protocols.
42 - 255	Reserved.

Type	Code	Description
0 - Echo Reply(Yankı cevabı)	0	
1 and 2		*Reserved*
3 - Destination Unreachable (Hedef Ulaşılamaz)	0	Destination network unreachable (Ağ Ulaşılamaz)
	1	Destination host unreachable (Hedef Ulaşılamaz)
	2	Destination protocol unreachable (Protokol Ulaşılamaz)
	3	Destination port unreachable (Port Ulaşılamaz)
	4	Fragmentation required, and DF flag set (Parçalama Gerekli ama izin yok)
	5	Source route failed (Kaynaklı Yönlendirme başarısız)
	6	Destination network unknown (Bilinmeyen Hedef Ağ)
	7	Destination host unknown (Bilinmeyen Hedef Bilgisayar)
	8	Source host isolated (Kaynak Tecrit Edilmiş)
	9	Network administratively prohibited (Hedef Ağa Erişim Yasaklanmış)
	10	Host administratively prohibited (Hedef Bilgisayara Erişim Yasaklanmış)
	11	Network unreachable for TOS (Belirtilen Servis Hedef Ağ Üzerinde Erişilemez)
	12	Host unreachable for TOS (Servis Türü için Bilgisayar Erişilemez)
	13	Communication administratively prohibited (Hedef ile iletişim yasaklanmış)

Type	Code	
4 - Source Quench (Sıkışık trafik)	0	Source quench (congestion control)
5 - Redirect Message (Yeni Rota Yönlendirme)	0	Redirect Datagram for the Network (Ağ için Yönlendirme)
	1	Redirect Datagram for the Host (Bilgisayar için Yönlendirme)
	2	Redirect Datagram for the TOS & network (Servis ve Ağ için Yönlendirme)
	3	Redirect Datagram for the TOS & host (Servis ve Bilgisayar için Yönlendirme)
6 - Alternate Host Address (Alternatif Adres)		Alternate Host Address (Alternatif Bilgisayar Adresi)
7		*Reserved*

Type	Code	
8 - Echo Request (Yankı isteği)	0	Echo request
9 - Router Advertisement (Yönlendirici Bildirimi)	0	Router Advertisement
10 - Router Solicitation (Router Şeçimi)	0	Router discovery/selection/solicitation
11 - Time Exceeded (Zaman aşımı)	0	TTL expired in transit (İletimde TTL Süresi Sıfırlanması)
	1	Fragment reassembly time exceeded (Parça Birleştirme Zaman Aşımı)
12 - Parameter Problem: Bad IP header (Parametre Hatası)	0	Pointer indicates the error (İşaretçi hatayı gösterir)
	1	Missing a required option (Gerekli opsiyon eksikliği)
	2	Bad length (Datagram uzunluk hatası)

Type	Code	
13 - Timestamp (Zaman belirteci)	0	Timestamp
14 - Timestamp Reply (Zaman Belirteci Cevabı)	0	Timestamp reply
15 - Information Request (Bilgi İsteği)	0	Information Request
16 - Information Reply (Bilgi isteği cevabı)	0	Information Reply
17 - Address Mask Request (Adres Mask isteği)	0	Address Mask Request
18 - Address Mask Reply (Adres Mask cevabı)	0	Address Mask Reply
19		*Reserved* for security
20 through 29		*Reserved* for robustness experiment

Code	Type	
30 - Traceroute	0	Information Request
31 - Datagram Conversion Error (Datagram dönüşüm Hatası)		
32 - Mobile Host Redirect (Mobil Yönlendirme)		
33 - Where-Are-You (originally meant for IPv6) (IPv6 Neredesin)		
34 - Here-I-Am (originally meant for IPv6) (IPv6 Buradayım)		
35 - Mobile Registration Request (Mobil Kayıt isteği)		
36 - Mobile Registration Reply (Mobil Kayıt cevabı)		
37 - Domain Name Request (Domain İsmi isteği)		
38 - Domain Name Reply (Domain ismi cevabı)		
39 - SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol		
40 - Photuris, Security failures		
41 - ICMP for experimental mobility protocols such as Seamoby [RFC4065]		
42 through 255		*Reserved*

Çok kullanılan ICMP Mesajları

Type

0 Echo Reply (Yankı): hedefin ulaşılabilir olduğu denetimi için.

3 Destination Unreachable: hedefin erişilemez olduğunu belirler

4 Source Quench: Rotadaki router'ın çok yoğun olduğunu belirtir.

5 Redirect: Routerlar rota belirlemek için kullanır.

8 Echo Request

11 Time Exceeded : Zaman aşımı- TTL'in 0'landığı bilgisi

12 Parameter Problem : IP datagramda oluşan problemleri bildirir.

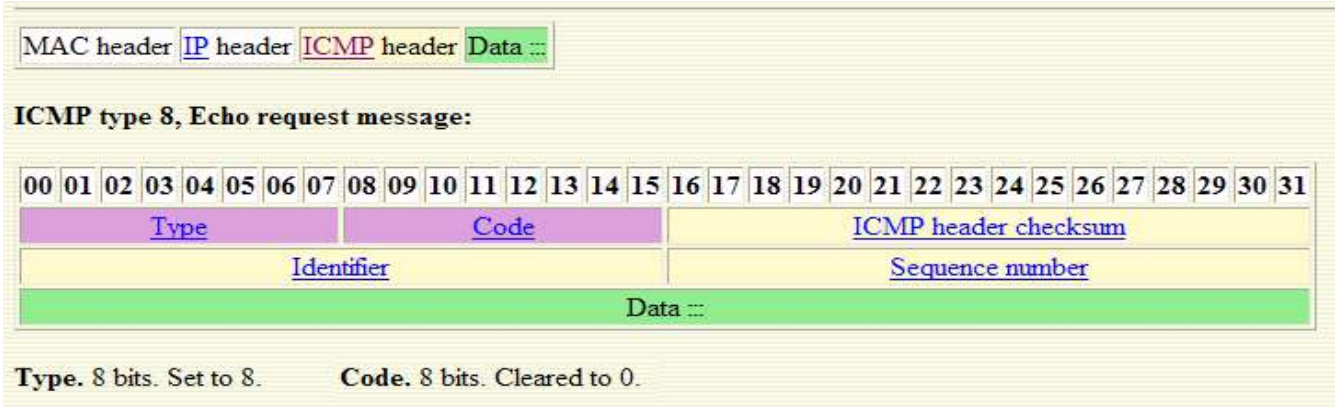
13 Timestamp :Paketlerin iki nokta arasındaki gidiş geliş süreleri için.

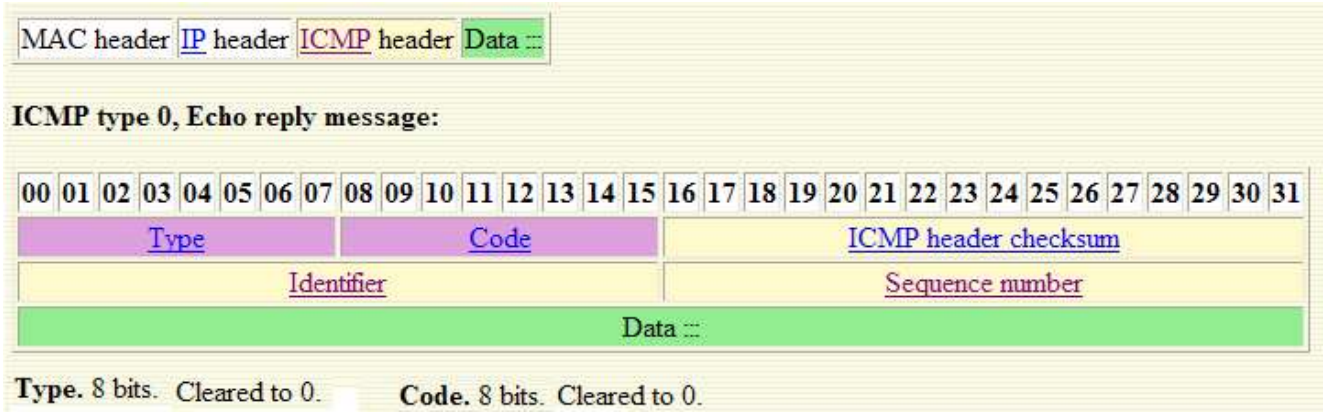
14 Timestamp Reply:

15 Information Request

16 Information Reply

En çok kullanılan mesaj türü (Echo 0 - 8) . “Yanıt-istek-yanıt” mesajları olarak bilinir. Ping komutunun kullandığı mesaj’dır.
Ping ile sorgulanan bilgisayara echo istek (8) ile bir miktar bilgi gönderilir. Hedef bilgisayardan ise kendisinin gönderdiği verinin aynısını içeren yankı yanıt (echo reply 0) ICMP mesajını göndermesini ister. Bu bildirim yapılmış ise iki nokta arasında iletişimin yapılabilir olduğu anlaşılır.





MAC header	IP header	ICMP header	Data

ICMP type 13, Timestamp request message:

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type	Code	ICMP header checksum
Identifier		Sequence number
Originate timestamp		
Receive timestamp		
Transmit timestamp		

Type. 8 bits. Set to 13.

Code. 8 bits. Always cleared to 0.

MAC header	IP header	ICMP message 14	Data

Message format:

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type	Code	ICMP header checksum
Identifier		Sequence number
Originate timestamp		
Receive timestamp		
Transmit timestamp		

Type. 8 bits. Set to 14.

Code. 8 bits. Always cleared to 0.

kında bilgilendirmek için kullanılır

ICMP type 4, Source quench message:

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">ICMP header checksum</td></tr>
<tr><td colspan="32">unused</td></tr>
<tr><td colspan="32">IP header + the first 64 bits of the original datagram's data.</td></tr>
</table>

Type. 8 bits. Set to 4. **Code.** 8 bits. Always cleared to 0. **unused.** 32 bits. Cleared to 0.

- **Parametre sorunu:** Bilgisayar veya router, başlık üzerinde IP datagramın iletilmesine mani bir durum olduğunu tespit ederse, datagramı yok edip karşıya bildirmesi içinir.

MAC header	IP header	ICMP header	Data :::

ICMP type 12, Parameter problem message:

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">ICMP header checksum</td></tr>
<tr><td colspan="8">Pointer</td><td colspan="24">unused</td></tr>
<tr><td colspan="32">IP header + the first 8 bytes of the original datagram's data.</td></tr>
</table>

Type. 8 bits. Set to 12.

Code. 8 bits. Specifies the reason for the error.

Code	Description
0	Invalid IP header.
1	A required option is missing.

ICMP mesajlarını kullanan programlar

Ping ve *traceroute* uygulamaları ICMP protokolunu kullanır.

- ***Ping:*** En çok kullanılan ağ analiz programlarından birisidir. Ping, hedef bilgisayara **"yankı istek (echo request) -** Type 8" mesajı gönderir. Eğer hedef bilgisayardan süresi içerisinde **"yankı cevap (echo reply)-** Type 0 **"** yanıtı gelirse, Ağ üzerinde erişilebilir olduğu anlaşılır.
- Ping her gönderdiği mesaj üzerine gönderilme zamanını ekler. Alınan yanıtı kullanarak (kaynak-hedef-kaynak dönüş süresi) paket iletimi için geçen zamanı bulabilir. Ping isteğine cevap için bir süre belirlenmiştir (time out- ping request time out -yaklaşık 2 sn).

* Hedef IP'ye Ping request'tan sonra time out kadar zaman içinde cevap (reply) gelmezse ping time-out hatası verir. Bu süreden sonra host dinlemeyi keser.

- Ping atılacak IP adresi için ARP tablosunda veya ARP sorgusunda IP-MAC eşleşmesi oluşturulamıyorsa ping request mesajı bile gönderilmez ve 'destination host unreachable – Hedef bilgisayar erişilemez ' hatası verir.

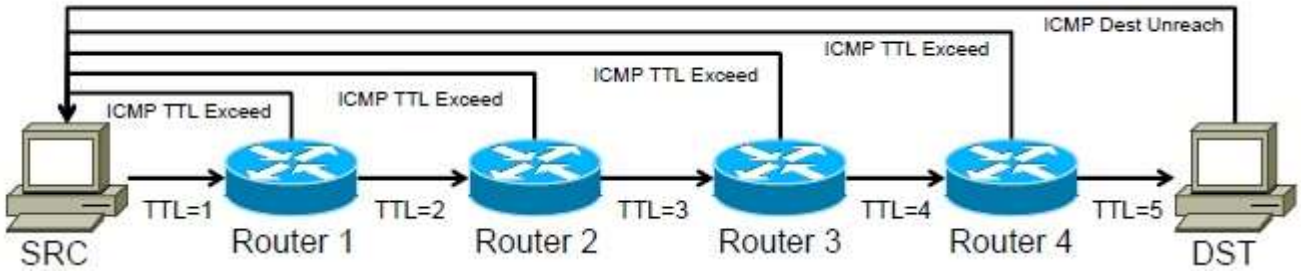
ping 192.15.36.44

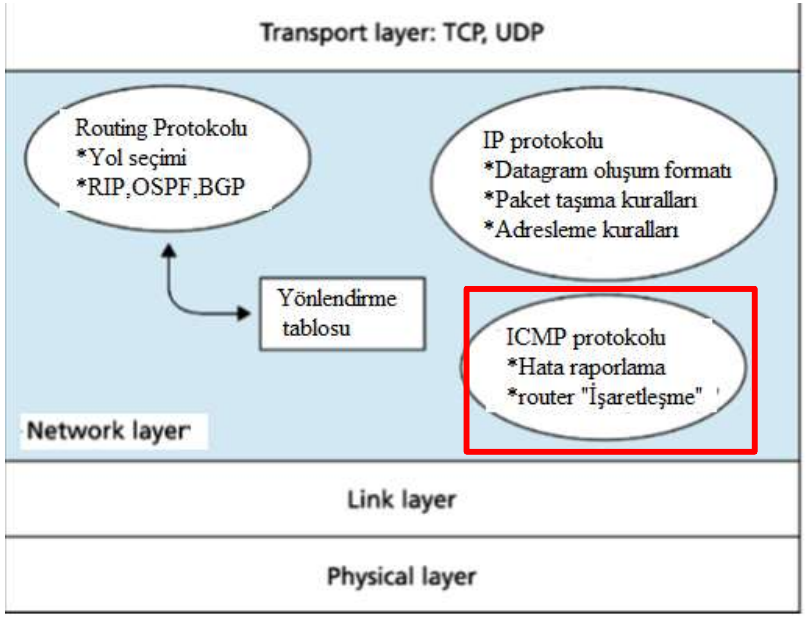
Gidiş dönüş başarıyla tamamlanmadıysa, ping aracı çeşitli hata mesajları görüntüler. Ping mesajında alınan hata mesajları aşağıdaki bilgileri içerir:

- **Geçiş Süresinde TTL Süresi Doldu:** Bir IP paketi hedefine ulaşmamışsa, önce ağ üzerinde yaşayabileceği maksimum süreyi belirler. Bu hatayı gidermek için, ping -i anahtarını kullanarak TTL değerini artırılabilir.
- **Hedef Ana Bilgisayar Ulaşılamaz:** Hedef pasiftir veya ağda yoktur. Hedef ana bilgisayar için yerel veya uzak bir rota bulunmaması nedeniyle oluşabilir. Bu hatayı gidermek için yerel rota tablosunu değiştirilmesi veya düğümü aktif edilmesi.
- **İstek Zaman Aşımına Uğradı:** Ping komutunun zaman aşımına uğradığını gösterir. Ağ trafiği, Adres Çözümleme Protokolü (ARP) istek paketi filtreleme hatası veya yönlendirici hatası nedeniyle yankı mesajı alınmadığını gösterir. Ping-w seçeneğinden bekleme süresini artırmak, bu sorunu çözebilir.
- **Bilinmeyen Ana Bilgisayar:** IP adresinin veya ana bilgisayar adının ağda bulunmadığını veya hedef ana bilgisayar adının çözülemediğini belirtir. Bu sorunu gidermek için, etki alanı adı sistemi (DNS) sunucularının adını ve kullanılabilirliğini doğrulayın.

Traceroute

- **Traceroute:** Datagramların hedeflerine ulaşıncaya kadar izledikleri rotanın belirlenmesi için kullanılan bir analiz programı (komutu)dır. Kaynak; paketin geçtiği yollarda karşılaştığı ağ elemanlarını öğrenmek için önce TTL değerini 1 yaptığı paketi gönderir. İlk ağ elemanı bu paketi alır almaz ICMP Type 11 (Time Exceeded) mesajını kaynağa gönderecektir. Traceroute bu mesajdan ilgili ağ elemanını tespit eder. Daha sonra TTL = 2 vererek paketi tekrar gönderir. Bu kez paket ilk elemanı aşarak ikinci elemandan ICMP Time Exceeded alır ve bunu da kaydeder. Bu şekilde hedef sunucuya kadar TTL değeri artırılarak bütün ağ elemanları tespit edilmiş olur.
- Time Exceeded mesajları da iç ağlar hakkında dış dünyaya bilgi vermemek üzere güvenlik gerekçesi ile devre dışı bırakılabilir.





ICMP Protokolu zayıflıkları

*ICMP kimlik doğrulaması sunmaz.
*IP protokolunun içerisindedir. IP'nin Kontrol ve hata mesaj protokoludur.

ICMP protokolu Saldırıları

* ICMP, ağdaki cihazları tarama ve istismar etmek için kullanılabilir.
*ICMP kullanımı ile, backdoor, port scan, redirect trafik, echo gibi DoS atakları düzenlenebilir

Genel ICMP Echo Atakları

- Ping (ICMP ile gerçekleşir) bombardımanı saldılarının amacı, büyük miktarda ICMP yankı istek paketlerini ağa yollayarak bant genişliğini kullanıp ağ kaynaklarını tüketmektir.

- Alınan her ICMP yankı istek (request) paketine karşılık, ICMP yankı cevap paketinin de yayınlandığına dikkat ediniz.

- Özellikle bant genişliği düşük olan ağlarda bu ataklar önemlidir.

Footprinting (Ping taraması)

- Hedef ağa saldırıdaki ilk adım, ağ hakkında bilgi toplamaktır. Buna 'ağın ayak izi‘ belirlemesi denir. ICMP bunun için uygundur. Bir ping taraması (sweep) ağa doğrudan bir saldırı değildir, ancak kesin bir tehditdir.
- Ping Taraması: Tanımlanmış bir IP aralığı için ağda hangi bilgisayarların canlı olduğunu bulmak için kullanılabilecek bir tekniktir. ICMP'ye izin veren ağ yöneticileri, ICMP tabanlı saldırılara karşı savunmasızdır.
- Birçok ağ yöneticisi, bu tür ayak izlerini önlemek için ICMP'yi tamamen engeller. Bu, sorun gidermeyi ve izlemeyi biraz zorlaştırdığından, bazı olumsuz yanları da vardır.
- Ping sweep için nmap, sing, ICMPscan v.b birçok araç mevcuttur. Bunlardan en çok kullanılanı nmap aracıdır. Windows tabanlı bir makinada;

```
$ nmap -sP -PI 192.168.0.0/24

Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-04-01 20:
Host 192.168.0.0 seems to be a subnet broadcast address (2 extra pings
Host 192.168.0.1 appears to be up.
Host 192.168.0.25 appears to be up.
Host 192.168.0.32 appears to be up.
Host 192.168.0.50 appears to be up.
Host 192.168.0.65 appears to be up.
Host 192.168.0.102 appears to be up.
Host 192.168.0.110 appears to be up.
Host 192.168.0.155 appears to be up.
Host 192.168.0.255 seems to be a subnet broadcast address (2 extra pir
Nmap finished: 256 IP addresses (8 hosts up) scanned in 17.329 seconds
```

Port Scanning

- ICMP, “hangi portların açık olduğunu keşfetmek için”, saldırganlar tarafından büyük oranda kullanılır. Çünkü TCP protokolu gibi bağlantılı bir protokol olmadığından saldırganlar için paha biçilmez bir araçtır.
- İlgili bilgisayardaki bir port’a bir UDP paket gönderilmesi ile portun açık olup olmadığını bildiren bir ICMP yanıtı alırsınız.
  - Eğer port açık ise; bir cevap gelmeyecektir.
  - Eğer port kapalı ise; **ICMP *tip3* *code3* olan bir ICMP reply mesajı alınacaktır. (Hedef ulaşılamaz, Port ulaşılamaz)**.

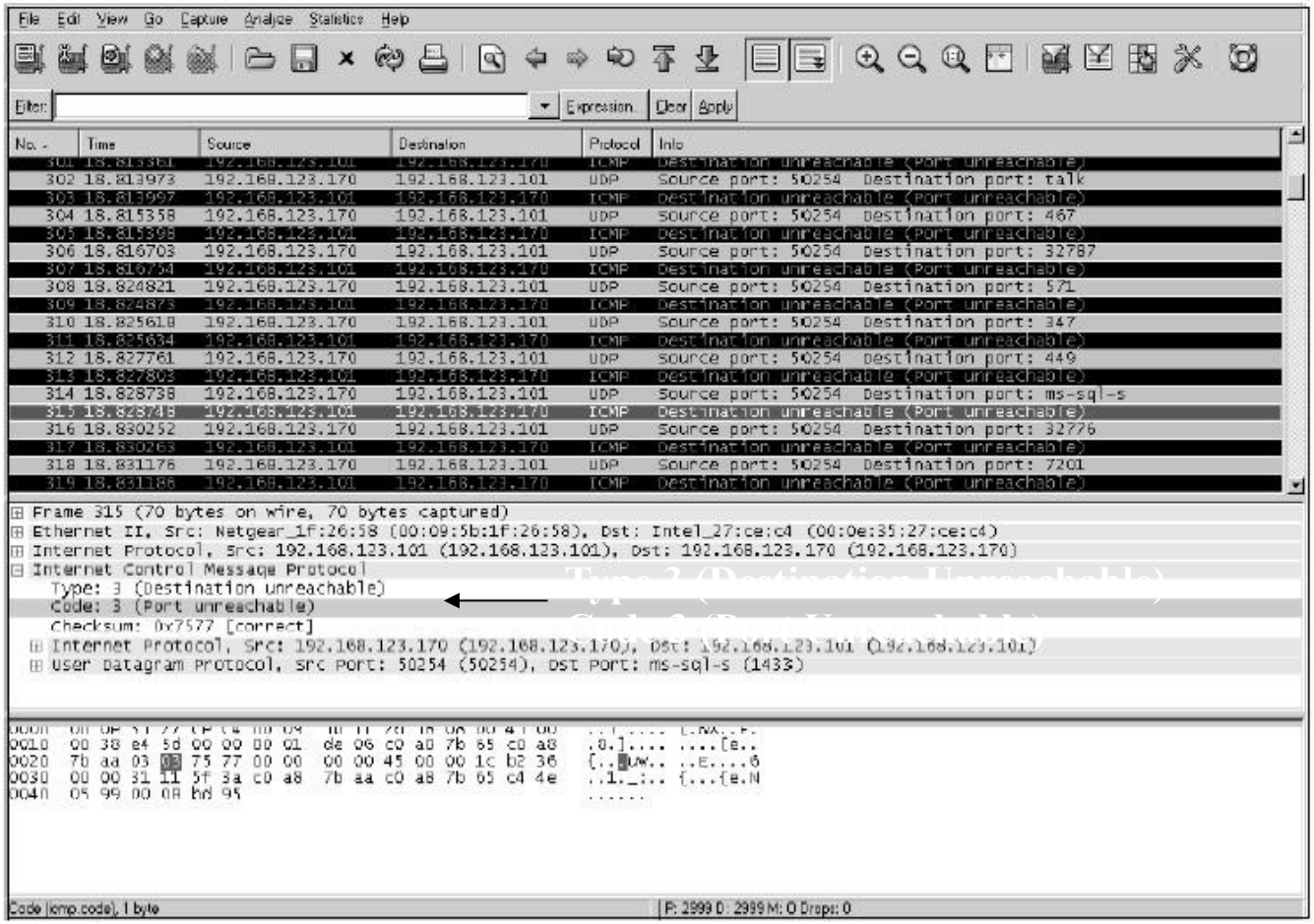
Hping2 tool’unu kullanarak 192.168.5.5 IP’sinin 50.portuna bir UDP paketi gönderilsin;

```
[root@stan /root]# hping2 -2 192.168.5.5 -p 50 -c 1
default routing not present
HPING 192.168.5.5 (eth0 192.168.5.5): udp mode set, 28 headers + 0 data
bytes
ICMP Port Unreachable from 192.168.5.5  (kenny.sys-security.com)

--- 192.168.5.5 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Port Scanning (cont.)

Figure 4.19 Port Scan

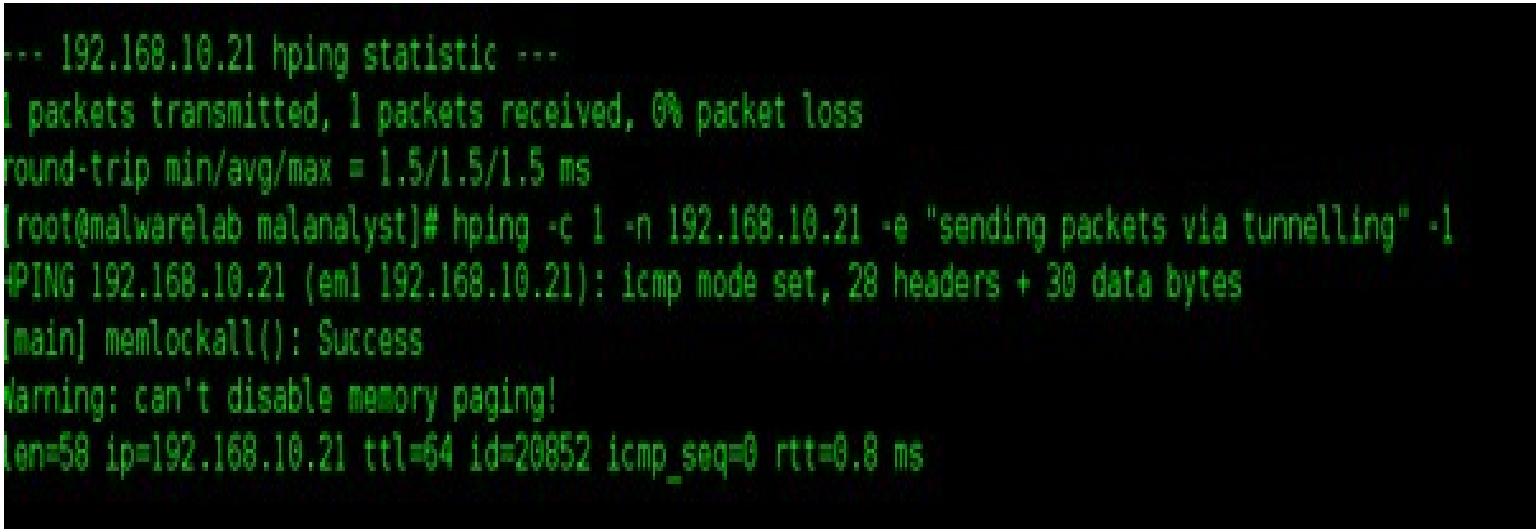


ICMP Tünelleme

ICMP tünelleri, bilgi akışının herhangi bir güvenlik mekanizması tarafından kontrol edilmediği, oluşturulmuş gizli bir kanal şeklidir. ICMP tünelleme kullanılarak, bir eko paketine isteğe bağlı veriler enjekte edilebilir ve uzaktaki bir bilgisayara gönderilebilir. Uzak bilgisayar başka bir ICMP paketine bir cevap enjekte eder ve geri gönderir. Bu tür iletişim trafiği, proxy tabanlı bir güvenlik duvarı (firewall) için, kaynak ve hedef IP adreslerine daha fazla odaklandıkları için tespit edilemez bir durumdur. Bu mekanizmalar, gerçek trafiğin gizlenmesi yoluyla güvenlik duvarlarının kurallarını atlamak için kullanılabilir. Uygulama tabanlı güvenlik duvarları, tüm paket üzerinde derin bir paket incelemesi yaptıkları için, yalnızca böyle bir trafik türünü algılayabilir. Bu nedenle, ağ yöneticisi veya güvenlik yöneticileri, derin paket incelemesi gerçekleştirilmedikçe bu şifreli iletişimi tespit edemez.

Hping, bir cihaza test veya saldırı yapmak için kullanılan bir paket hazırlama aracıdır. Komut istemini kullanarak gönderdiğimiz normal bir ping mesajı için dört paket veri gönderir.

Aşağıdaki komutu yazarak ping mesajı ile “tünelden paket gönderme” işlemi gerçekleştirilir.

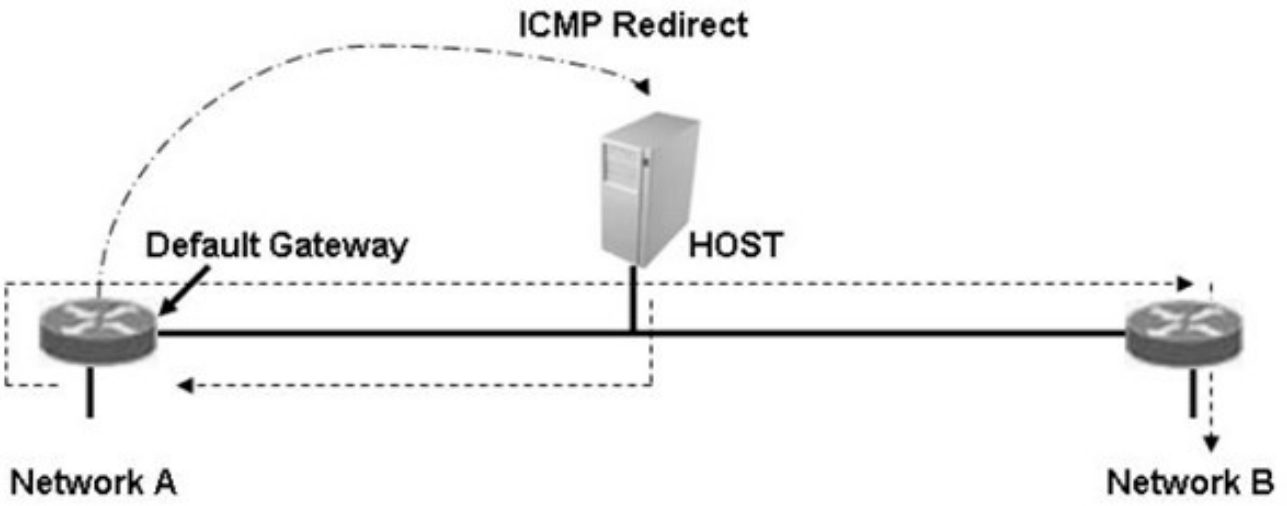


ICMP Nuke Atakları

- Bilgisayarlar çoğu zaman aralarındaki bağlantının sağlamlığını birbirlerine ICMP paketleri göndererek anlarlar.
- **ICMP Nuke Atağı;** Sahte adresler (spoof edilmiş) kullanarak, bir saldırgan; iki host arasındaki düzgün iletişimi "**Time Exceeded**" (Type 11) veya "**Destination Unreachable**" (ICMP Type 3) mesajlarını her iki hosta'da göndererek, sanki hata varmış gibi gösterebilir, bozabilir.
- Bu bir DOS atağıdır. Eski bir atak türüdür.
- ICMP Types and Codes 'lar konusuna bir gözat.

ICMP Redirect Attack
(ICMP yeniden yönlendirme atağı)

- Bir saldırgan; ICMP "**redirect**" mesajları göndererek, bir hedef router'a yönlendirilmiş mesajları, IP adresi saldırganın adresi olan bir host'a forward eder.



ICMP Redirect Ataklarını Önleme

- Linux işletim sisteminde, kernel'de değişiklik yaparak redirect mesajlarının kabul edilmemesini sağlayabiliriz.

```
root@router# echo 0 >
  /proc/sys/net/ipv4/conf/eth0/accept_redirects
```

```
[root@localhost eth0]# pwd
/proc/sys/net/ipv4/conf/eth0
[root@localhost eth0]# ls
accept_redirects     bootp_relay         mc_forwarding        send_redirects
accept_source_route  disable_policy      medium_id            shared_media
arp_accept           disable_xfrm        promote_secondaries  tag
arp_announce         force_igmp_version  proxy_arp
arp_filter           forwarding          rp_filter
arp_ignore           log_martians        secure_redirects
[root@localhost eth0]#
```

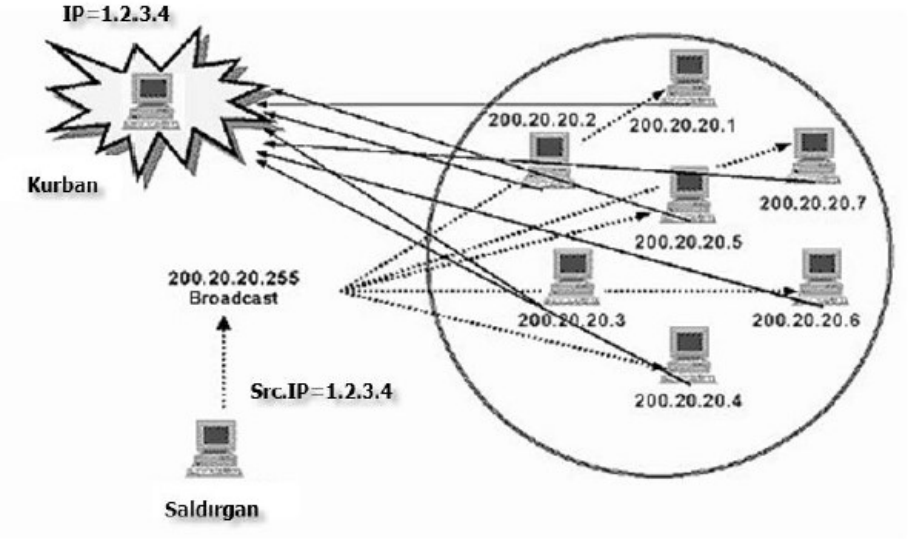
ICMP Flood (ICMP Taşkını-Sel basması Bombardımanı)

- Ping Flood, bir ping (ICMP üzerinden yapılır) broadcast fırtınası yaratarak hedef sistemi bunaltabilir. Bu bir DoS saldırısıdır.
- Linux'ta, ping –f kullanılarak herhangibir host'a bir taşkın oluşturulabilir.

```
root@router# ping -f 10.10.10.12 -c 1000
```

ile 10.10.10.12 IP'li host'a 1,000 paket gönderilir.

IP ping paketinin işleyişinden yararlanan "***Smurf saldırıları***" da ICMP FLOOD'un özel bir halidir. Çok sayıda reply paketi ile hedefin gerçek trafiği alması engellenir. Smurf ataklarında; kurban bilgisayarın IP adresinden network'ün broadcast adresine Internet (ICMP) isteği (ping) gönderilir ve network üzerindeki bütün bilgisayarlardan kurban bilgisayara yanıt göndermesi sağlanır.



Ping Flood'dan korunma

- Ping flood, IPTable 'ın konfigirasyonu ile "ICMP echo-request messages" larının sayısını sınırlayarak durudurulabilir.

```
root@router# iptables –A FORWARD –p icmp –icmp-
  type echo-request -m limit –limit 10/s –j
  ACCEPT
(saniyede 10 tane  gelen icmp echo request paketlerini kabul et)

root@router# iptables –A FORWARD –p icmp –icmp-
  type echo-request –j DROP
(Icmp echo-request paketlerini düşür)
```

Not:iptables, Linux veya Unıx'te NAT'lama veya paket filtreleme için bir araçtır.

Ping of Death

- Ping of Death, IP paketlerine gömülü olarak ICMP ile gönderilen “echo request” mesajları ile yapılır. Bu mesajlar 65.535 bayt’tan daha büyük mesajlar halinde sürekli olarak gönerilirse Buffer kapasitesi küçük olan makinalarda buffer taşmasına sebep olarak makinanın çökmesine sebep olur. Ping of death bir DoS atağı çeşididir.

Windows komut satırından:

```
ping -1 65550 192.168.1.X
```

Linux komut satırından:

```
ping -s 65550 192.168.1.X
```

SMURF Atağı

Daha önce tartıştığımız gibi, ne zaman bir tip 8 gönderilirse, bir tip 0 geri gönderilir veya bir yankı isteği gönderildiğinde bir ICMP yankı yanıtı gönderilir. Bir smurf saldırısında, saldırgan ICMP paketinin kaynak adresini bozar ve bu ağdaki tüm bilgisayarlara bir yayın gönderir. Ağ aygıtları bu trafiği filtrelemezse, ağdaki tüm bilgisayarlara yayınlanır. Mağdurun ağı, bu kadar fazla trafikten etkilenir ve bu da tüm ağın verimliliğini düşürür.

Adres sahtekarlığını önlemek için yönlendiricilere ve güvenlik duvarına filtreler yerleştirin. Bir LAN segmentine bir IP adresi atanmalı ve kaynak makinenin IP adresi segmente atanmış IP adresi aralığında değilse, trafik kesilmelidir.

ICMP Router keşfi

ICMP router bulma protokolü, komşu yönlendiricilerin IP adresini bulur. Yönlendirici bulma mesajı, Ana bilgisayarların komşu bir yönlendiricinin varlığını keşfetmesine olanak tanır, ancak hangi yönlendiricinin belirli bir hedefe ulaşmak için en iyisi değildir. Yönlendirici reklam mesajı (hello mesaji v.b) bir ICMP mesajıdır (tip 9, kod 0). ICMP yönlendirici bulma protokolü için temel zorluk, herhangi bir kimlik doğrulama biçiminin bulunmamasıdır, bu nedenle son ana makinelerin aldıkları bilgilerin geçerli olup olmadığını söylemeleri imkansızdır.

Yukarıdaki sorun nedeniyle, saldırgan, saldırganın kaynağından uç noktaya kadar olan tüm iletişim için orta saldırgan olarak hareket edeceği man in the middle gerçekleştirebilir. Saldırganlar ayrıca ICMP yönlendirici bulma mesajlarını taklit edebilir ve kurbanın yönlendirme tablosuna uzaktan kötü rota girişleri ekleyebilir. Bu tür saldırılar DOS saldırısına yol açabilir ve oldukça şiddetli olabilir.

ICMP rota keşiflerini önlemek için kullanılan bir önlem, dijital imzaları kullanmak ve tüm tip 9 ve 10 ICMP paketlerini engellemektir

Genel bakış

- IP, ICMP, and Routing protokolları önemlidir.
- IP bağlantısız bir protokol olduğu için DOS saldırılarına açıktır.

- Saldırganlar tarafından IP protokoluna saldırılar için ICMP kullanılabilir.

- Routing protokolları data yığınlarına maruz kalırlar.