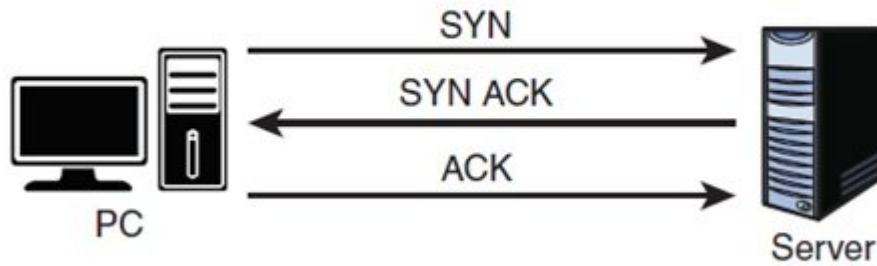
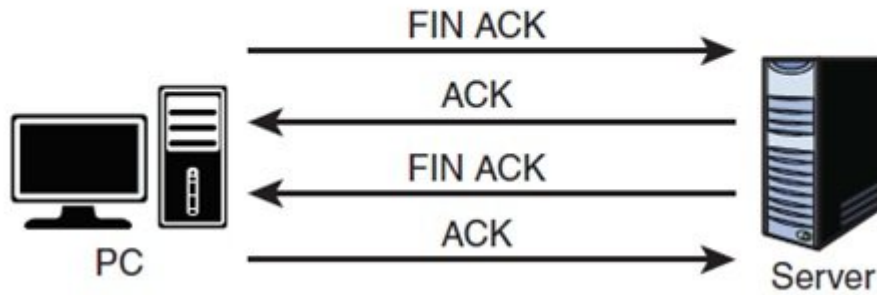




### Three-Step Startup



### Four-Step Shutdown



TCP는 1 단계에서 SYN을 보내고, 2 단계에서 SYN ACK을 받고, 3 단계에서 ACK을 보냅니다. 4 단계에서는 FIN을 보내고, 5 단계에서 ACK을 받습니다. 6 단계에서는 FIN ACK을 보내고, 7 단계에서 ACK을 받습니다. Nmap은 SYN을 보내고, SYN ACK을 받으면 포트가 열려 있다고 판단합니다.

Source Port		Destination Port						
Sequence Number								
Acknowledgment Number								
Data Offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window
Checksum				Urgent Pointer				
Options						Padding		
Data								

(Destination) (Source)

ACK sequence acknowledgment sequence  
 . . . . .  
 ACK Push RST SYN FIN  
 . . . . .  
 ACK SYN  
 . . . . .  
 FIN RST  
 . . . . .  
 RST  
 . . . . .  
 checksum  
 . . . . .  
 checksum TCP  
 . . . . .  
 URG  
 . . . . .  
 NULL

: . . . . .  
 PSH SYN URG XMAS  
 . . . . .  
 CEH  
 . . . . .  
 TCP  
 . . . . .  
 NULL  
 . . . . .  
 TCP  
 . . . . .  
 FIN CWR ECE URG ACK PSH RST SYN

(User Datagram Protocol) . . . . .

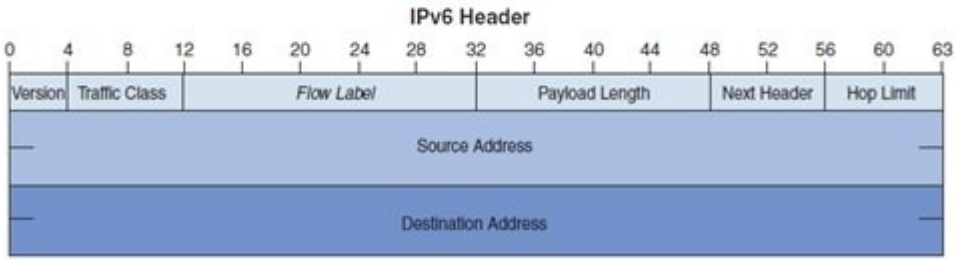
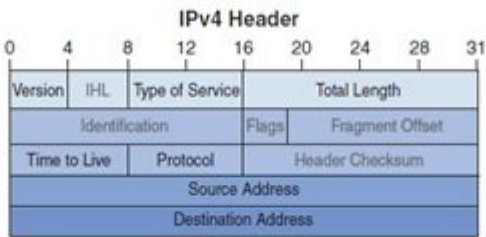
. . . . .  
 TCP . . . . .  
 UDP  
 . . . . .  
 UDP . . . . .  
 . . . . .  
 DNS (DHCP) . . . . .  
 . . . . .  
 UDP TCP . . . . .  
 . . . . .  
 UDP . . . . .

Source Port	Destination Port
Length	Optional Checksum

**(Internet)** . . . . .

4/6 (IP) . . . . .  
 . . . . .  
 IP . . . . .  
 (ICMP)  
 . . . . .  
 IP . . . . .  
 . . . . .  
 . . . . .  
 RFC 791 . . . . .  
 . . . . .  
 IP UDP TCP . . . . .

IPv4 header structure and fields. The Total Length field indicates the total length of the packet in bytes.



IPv6 features and protocols:
 

- Fixed 128-bit address length.
- Flow Label field for traffic differentiation.
- Optional extension headers (Options).
- IPsec for security.
- NAT-64 for IPv4 compatibility.
- Neighbor Discovery Protocol (NDP) replaces ARP.
- Routing protocols: RIPng, OSPFv3, EIGRPv6, IS-IS, and BGP.

IPv4 address range: 0 to 255.



IPID = 043C Length = 3,600 Offset = 0

More = 1  
Len = 1,000  
Offset = 0

More = 1  
Len = 1,000  
Offset = 1,000

More = 1  
Len = 1,000  
Offset = 2,000

More = 0  
Len = 600  
Offset = 3,000

00000000 0 0000 1000 0000 0000 0000 0000 .000000 000000 00 999-0 00000000 0 0000 0 0000 000 0000  
0 000000 000000 00 2999-20000 00000 0 0000 20000 0000 000000 000 00000 .000000 000000 00 1999-1000  
000 00000 00 00 00000 00 .000000 000000 00 399-3000 00000000 0 0000 3000 0000 000000 00000  
0 000000 00 More 0000 00 000000 00000000 00000000 00000 00 000 0000000 1 00 000000 More 00000 000000  
000000 00000000000 00000000 00000000 0000 00000 .00000000 00000000 0000 00000 00 00 00000 00000 000000  
000000000 00000000 00000000 0000 00000 00000000 0000 0000 .00000 0000 0000000 00 00 00000000 0000 00000  
.0000000 TCP / IP 00 0000000 00000000 00000 00 0 00000 00000000 00 00000000 00 0000000 00000 00 0000000  
0000000 00 0000 000000000 00000000 0 0000 00000 "TCP/IP Illustrated, Volume 1: The Protocols" 00000  
0000 0000000 0000 00 0000

00000 00 0000 00000 00 0000000 00000000 0000 0000000 0 00000000 0000000 00000 00000000 00 :00000  
000000 00000 00000 00 00 00000 000000000 00 00000 0000000 00 0000000 0000000 0000000 00 00 000000000  
.00000000

0000 00000 0000 00 00000000 00000000 00000 00000000 00000 00000000 00000 00000000 0000000 00000 00000  
000000 000000000 00000000 00 00000000 000000 00000 0000000000 00000000000000000000 0000000 000000 00 00000  
00 00 00000000 00000000000 0000000000 00 .0000 0000 00000 00000 00000 00 00 00000 00000 00 00000000  
00000 00 0000000 0000 0000 0000 .0000 00000 00 00000 0000 000000000 00 00 00000 000000000 00000  
.0000000

More = 1  
Len = 1,000  
Offset = 0

More = 1  
Len = 1,000  
Offset = 500

More = 0  
Len = 1,000  
Offset = 1,500

ICMP Echo Request (ping) packets are sent to the destination. The destination host responds with an ICMP Echo Reply. The More flag indicates if there are more fragments. The Len field indicates the length of the data. The Offset field indicates the starting position of the data.

Teardrop attack: A Teardrop attack is a type of Denial of Service (DoS) attack. It involves sending a large number of fragmented packets to a target system. The target system's buffer becomes full, and it cannot process any more packets, leading to a denial of service.

ICMP Echo Reply (ping response) packets are sent back to the source. The code field indicates the reason for the error. The type field indicates the type of ICMP message. The code field is used to further identify the error.

Type	Code	Function
0/8	0	Echo response/request (ping)
3	0-15	Destination unreachable
4	0	Source quench
5	0-3	Redirect
11	0-1	Time exceeded
12	0	Parameter fault
13/14	0	Time stamp request/response
17/18	0	Subnet mask request/response

ICMP Echo Request (ping) packets are sent to the destination. The destination host responds with an ICMP Echo Reply. The code field is used to further identify the error.

ICMP ping 3 type codes. Ping of Death, crafted Smurf attack, netmask, DoS, type 3 codes.

Some Common Type 3 Codes

Code	Function
0	Net unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed and Don't Fragment was set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network administratively prohibited
10	Communication with destination host administratively prohibited
11	Destination network unreachable for type of service
12	Destination host unreachable for type of service
13	Communication administratively prohibited

ICMP type 3 codes. CEH, RFC 792, DoS, netmask, type 3 codes.

ICMP type 3 codes.

CEH type 3 codes.

[CEH type 3 codes](#)

ICMP type 3 codes

ICMP type 3 codes

ICMP type 3 codes

ICMP type 3 codes

ICMP type 3 codes

11:30 - 10/12/1398

ICMP type 3 codes

ICMP type 3 codes - CEH v10 type 3 codes - CEH type 3 codes - CEH type 3 codes - CEH type 3 codes



معماری

<https://www.shabakeh-mag.com/security/16602/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-c:معماری-eh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D8%A2%D9%86%D8%A7%D8%AA%D9%88%D9%85%DB%8C-%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-tcp-ip-%D9%88-%D8%B6%D8%B9%D9%81%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A2%D9%86-%D8%A8%D8%AE%D8%B4-2>