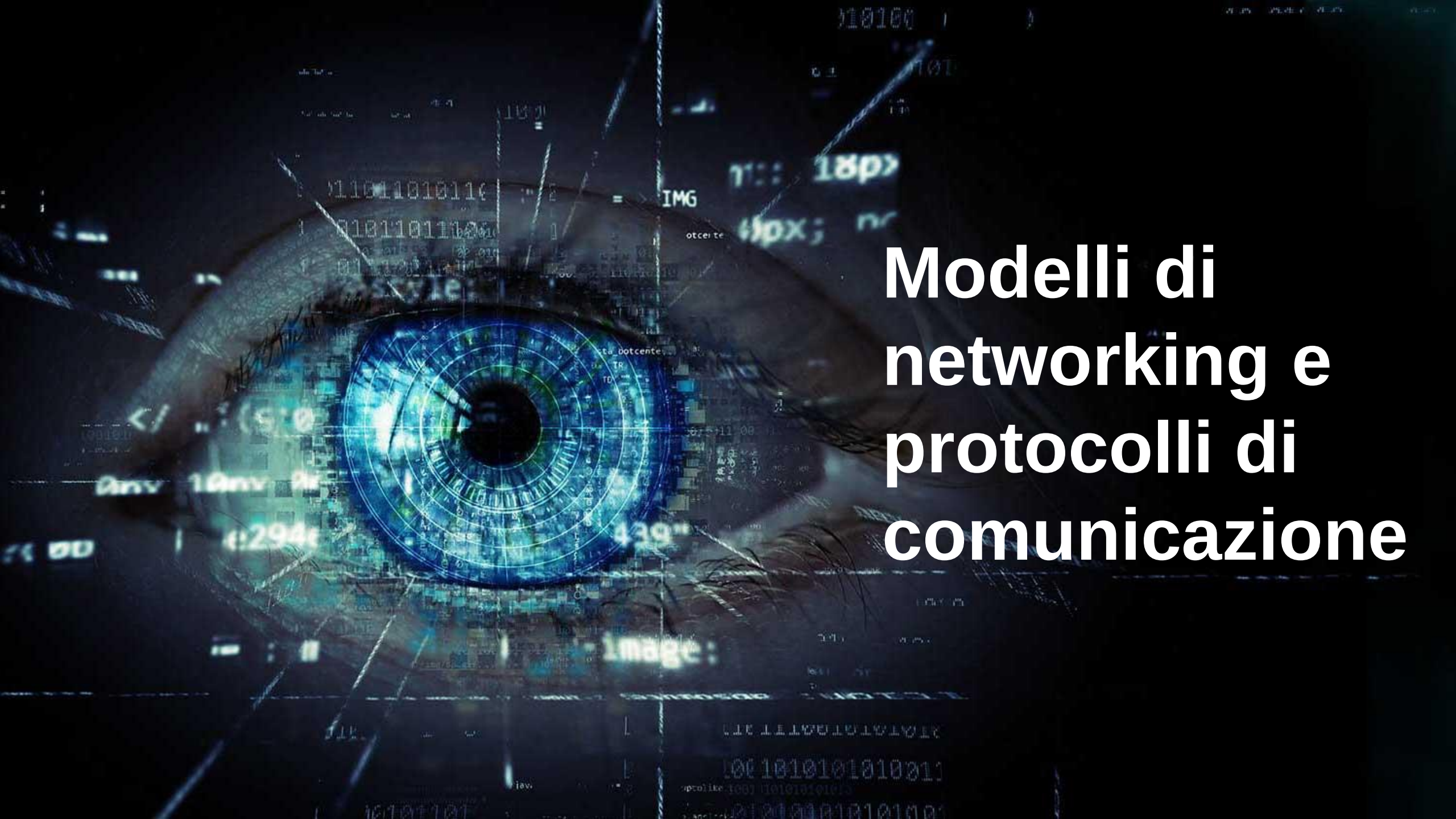
Corso di Cybersecurity

Ing. Giulio Magnanini



Modelli di networking e protocolli di comunicazione

IP

- **IP è un protocollo a livello di rete («Internet» nel modello TCP/IP) che ha l’obiettivo di gestire l’instradamento (route addressing) dei vari pacchetti**
- **Come UDP è un protocollo connectionless (Non stabilisce la sessione con handshake)**
- **Nella prossima slide vediamo come è composto un datagramma IP**

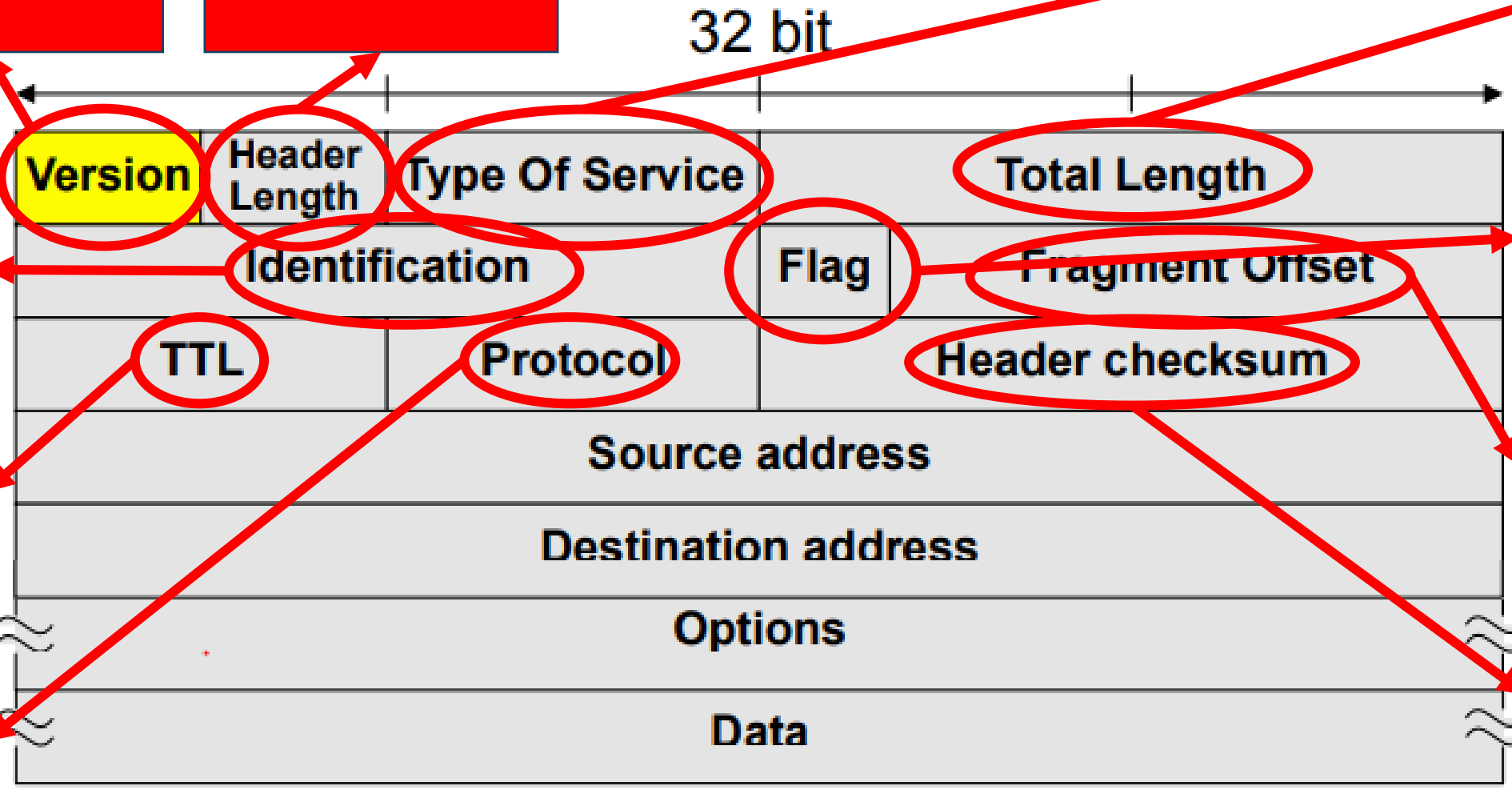
IP

Indica la versione del protocollo IP utilizzato (IPv4, IPv6)

Lunghezza, in multipli di 4 bit, dell'header del datagramma

bit D - Utilizzare il path con delay minimo
bit T - Utilizzare il path con throughput massimo
bit R - Utilizzare il path con massima affidabilità
bit C – Utilizzare il path con costo economico minimo

Lunghezza totale del datagramma in byte



Identificazione univoca del datagramma

Time to live: numero di secondi per cui il pacchetto resta in rete

Protocollo (TCP, UDP) utilizzato a livello di trasporto per il datagramma

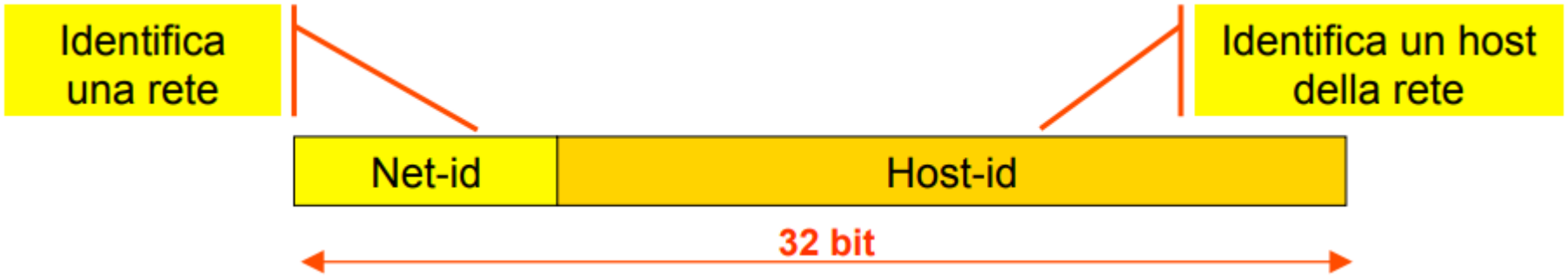
Not Used; DF=Don't Fragment; **MF**=More Fragment

Numero del frammento

Checksum per il controllo degli errori

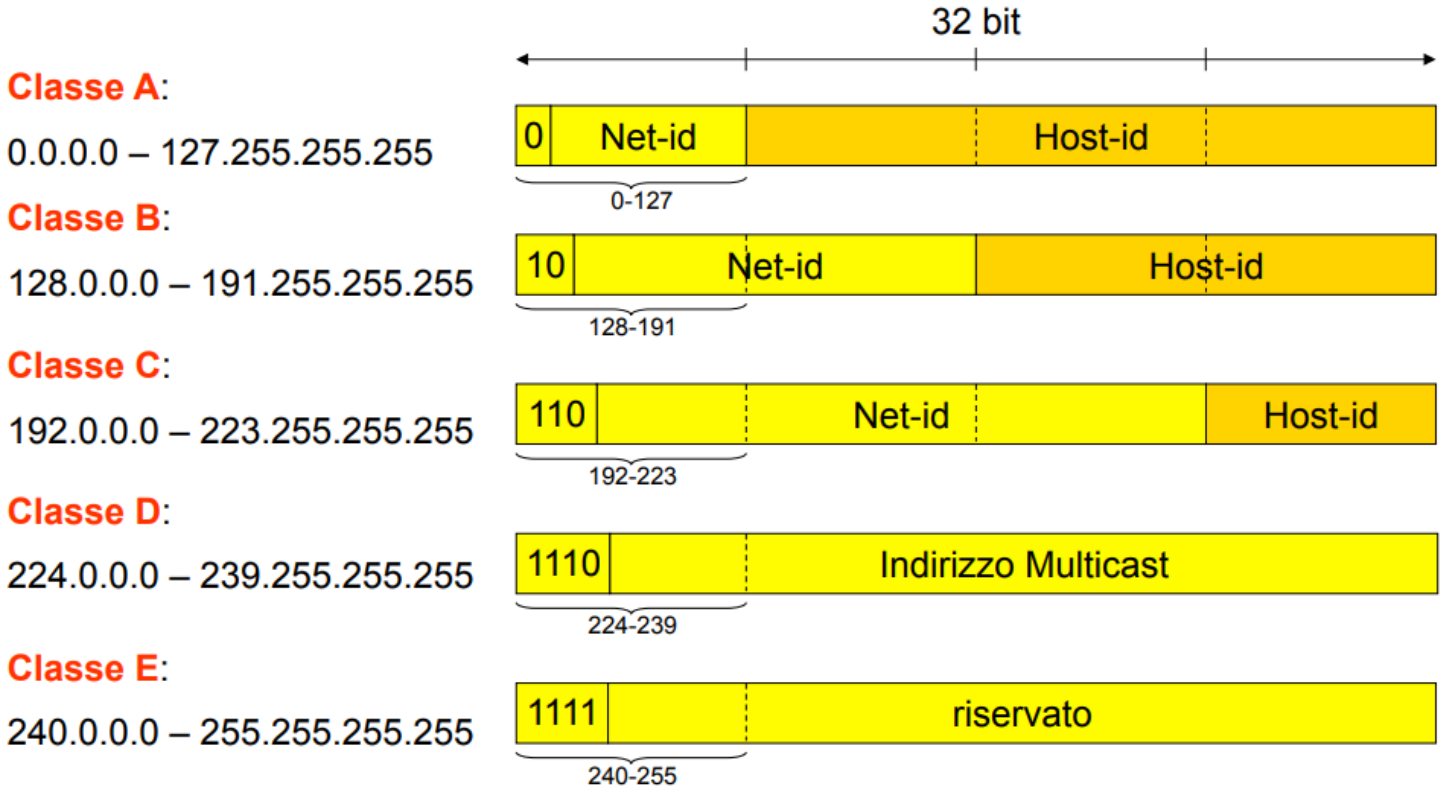
Indirizzi IP

- **IP utilizza e definisce degli indirizzi per i vari host su una rete, di formato ben preciso.**
- **Questi indirizzi sono a 32 bit e si esprimono in forma decimale puntata (193.204.49.40)**
- **L'assegnazione degli indirizzi è compito dell' Internet Assigned Number Authority (IANA) gestita dall'ICANN (Interne Corporation for Assigned Names and Numbers)**
- **Ogni indirizzo IP è così composto:**



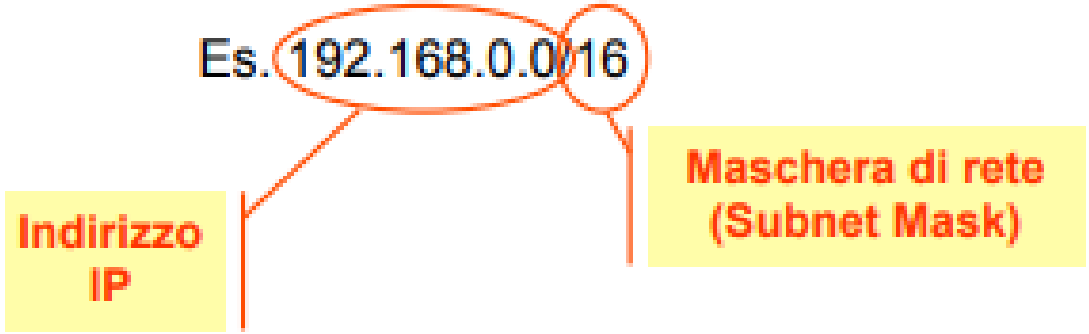
Indirizzamento IP classful

- **L'indirizzamento classico introduce 5 classi di indirizzi IP: A, B, C, D, E**
- **La classe A supporta 16.777.214 hosts, la B 65.534 hosts, la C 254 Hosts, le altre due sono usate una per il multicast e l'altra per sviluppi futuri**



Indirizzamento IP classless

- **CIDR (Classless InterDomain Routing): indirizzamento più usato, non considera le classi ma direttamente gli IP**
- **Il formato dell'indirizzo è di tipo a.b.c.d/x dove x è la maschera di rete che indica il numero di bit più significativi ed identifica la rete.**

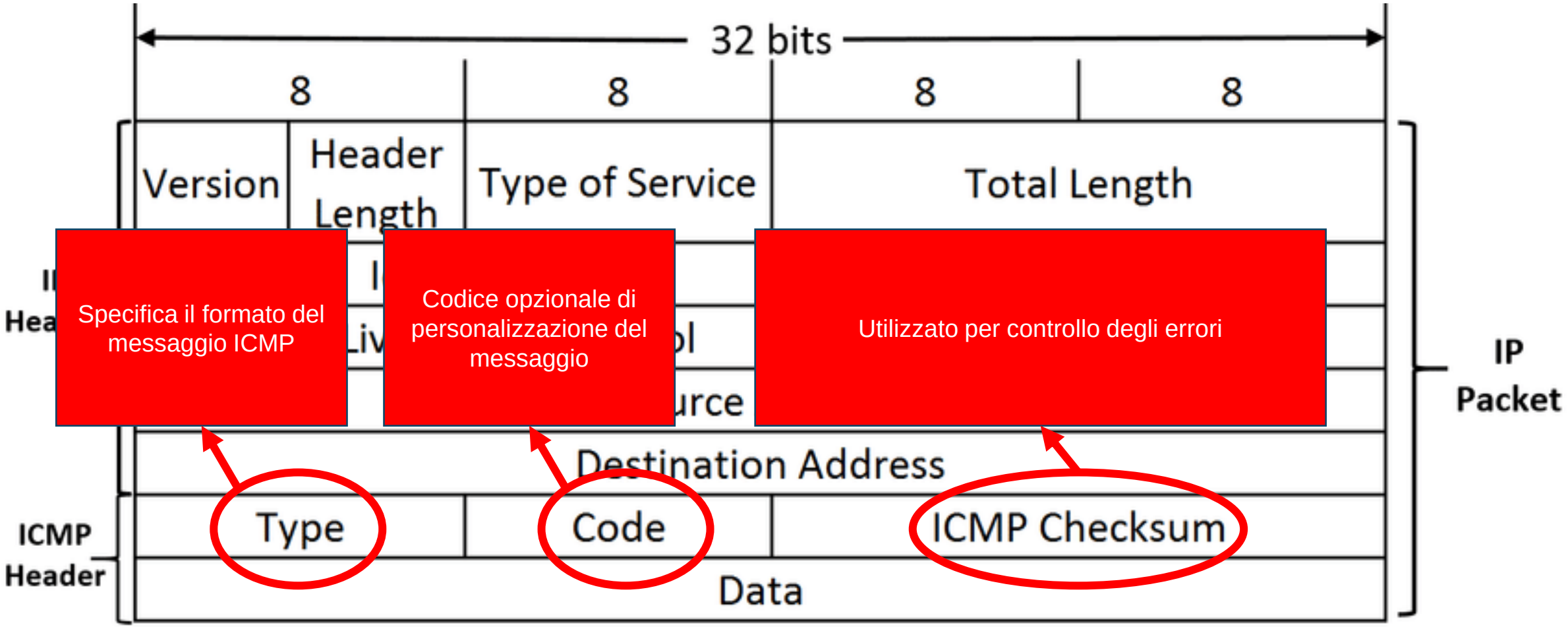


CIDR	Subnet Mask
/1	128.0.0.0
/2	192.0.0.0
/3	224.0.0.0
/4	240.0.0.0
/5	248.0.0.0
/6	252.0.0.0
/7	254.0.0.0
/8	255.0.0.0
/9	255.128.0.0
/10	255.192.0.0
/11	255.224.0.0
/12	255.240.0.0
/13	255.248.0.0
/14	255.252.0.0
/15	255.254.0.0
/16	255.255.0.0
/17	255.255.128.0
/18	255.255.192.0
/19	255.255.224.0
/20	255.255.240.0
/21	255.255.248.0
/22	255.255.252.0
/23	255.255.254.0
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252
/31	255.255.255.254
/32	255.255.255.255

ICMP

- **ICMP (Internet Control Message Protocol) è un protocollo a livello di rete («Internet» nel modello TCP/IP) che ha l'obiettivo di controllare la salute di una rete**
- **Lavora spesso unito al protocollo IP**
- **ICMP è famoso per essere usato per *ping, traceroute* ed altri tool di scansione di una rete**
- **ICMP è anche usato per causare diversi exploit quali DoS sulla banda, *ping of death, smurf attack, e ping flood***

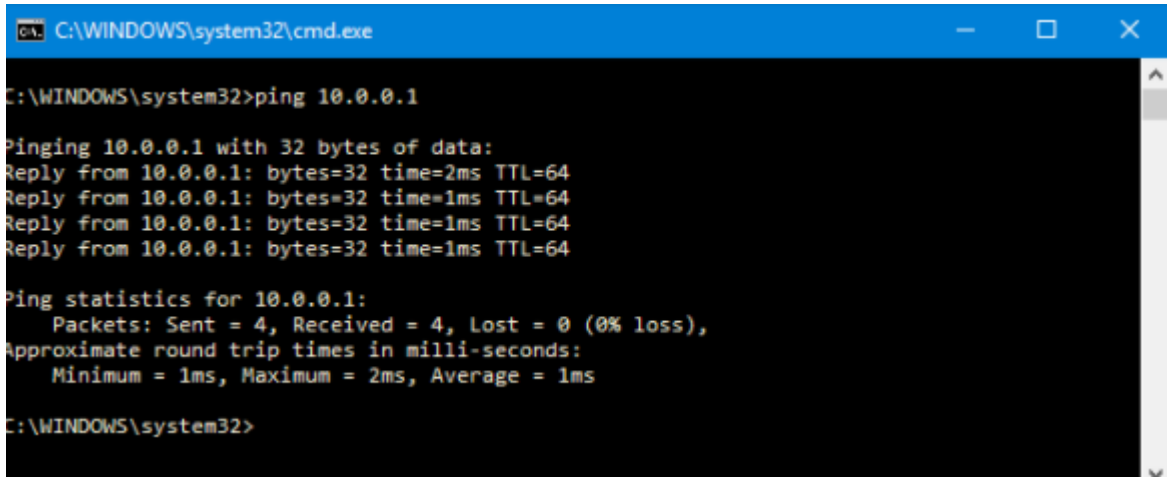
ICMP

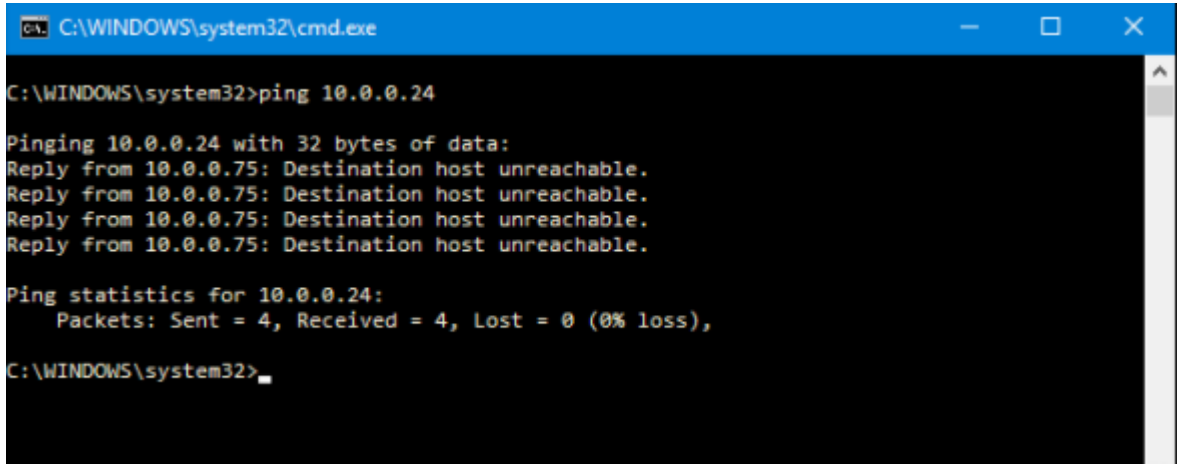

32 bits
8
8
8
8
Version
Header Length
Type of Service
Total Length
Destination Address
Type
Code
ICMP Checksum
Data
ICMP Header
IP Packet
Specifica il formato del messaggio ICMP
Codice opzionale di personalizzazione del messaggio
Utilizzato per controllo degli errori

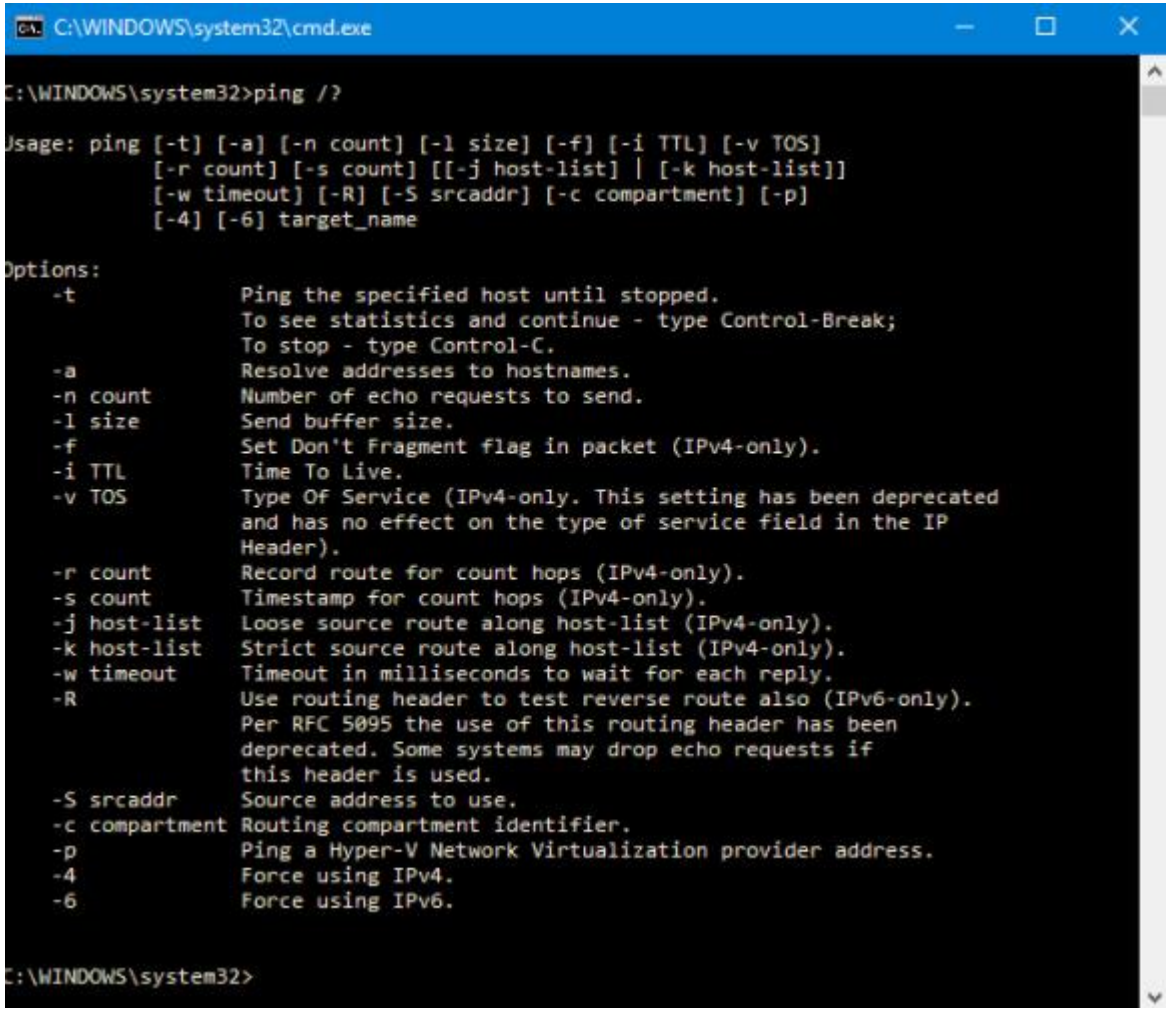
ICMP

ICMP Type	Code	Description
0	0	eco reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	7	destination host unknown
8	0	eco request
10	0	router discovery
11	0	TTL expired

Ping


C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=2ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Ping statistics for 10.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\WINDOWS\system32>


C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping 10.0.0.24
Pinging 10.0.0.24 with 32 bytes of data:
Reply from 10.0.0.75: Destination host unreachable.
Reply from 10.0.0.75: Destination host unreachable.
Reply from 10.0.0.75: Destination host unreachable.
Reply from 10.0.0.75: Destination host unreachable.
Ping statistics for 10.0.0.24:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\WINDOWS\system32>

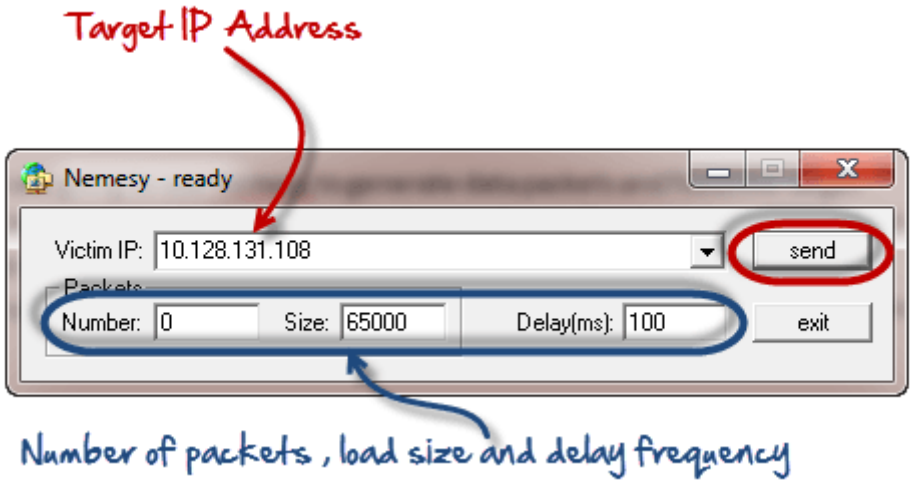

C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping /?
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
[-4] [-6] target_name
Options:
-t Ping the specified host until stopped.
To see statistics and continue - type Control-Break;
To stop - type Control-C.
-a Resolve addresses to hostnames.
-n count Number of echo requests to send.
-l size Send buffer size.
-f Set Don't Fragment flag in packet (IPv4-only).
-i TTL Time To Live.
-v TOS Type Of Service (IPv4-only. This setting has been deprecated
and has no effect on the type of service field in the IP
Header).
-r count Record route for count hops (IPv4-only).
-s count Timestamp for count hops (IPv4-only).
-j host-list Loose source route along host-list (IPv4-only).
-k host-list Strict source route along host-list (IPv4-only).
-w timeout Timeout in milliseconds to wait for each reply.
-R Use routing header to test reverse route also (IPv6-only).
Per RFC 5095 the use of this routing header has been
deprecated. Some systems may drop echo requests if
this header is used.
-S srcaddr Source address to use.
-c compartment Routing compartment identifier.
-p Ping a Hyper-V Network Virtualization provider address.
-4 Force using IPv4.
-6 Force using IPv6.
C:\WINDOWS\system32>

Ping of death e Smurf Attack

- **Ping of death: Attacco nel quale vengono inviati pacchetti ICMP di tipo ping malformati che mandano in tilt il sistema attaccato**
- **Smurf Attack: Attacco nel quale vengono mandati innumerevoli pacchetti ping di tipo Echo Request ad un indirizzo di broadcast di una rete in modo da ottenere in risposta gli ip degli host facenti parte della rete attaccata**

Ping Flood

- **Ping flood: Attacco nel quale vengono mandati innumerevoli pacchetti ping di tipo Echo Request che sommergono di richieste il sistema attaccato. Per fare questo tipo di attacco (Qui solo per motivi di ricerca e studio!) si può usare Nemesy**

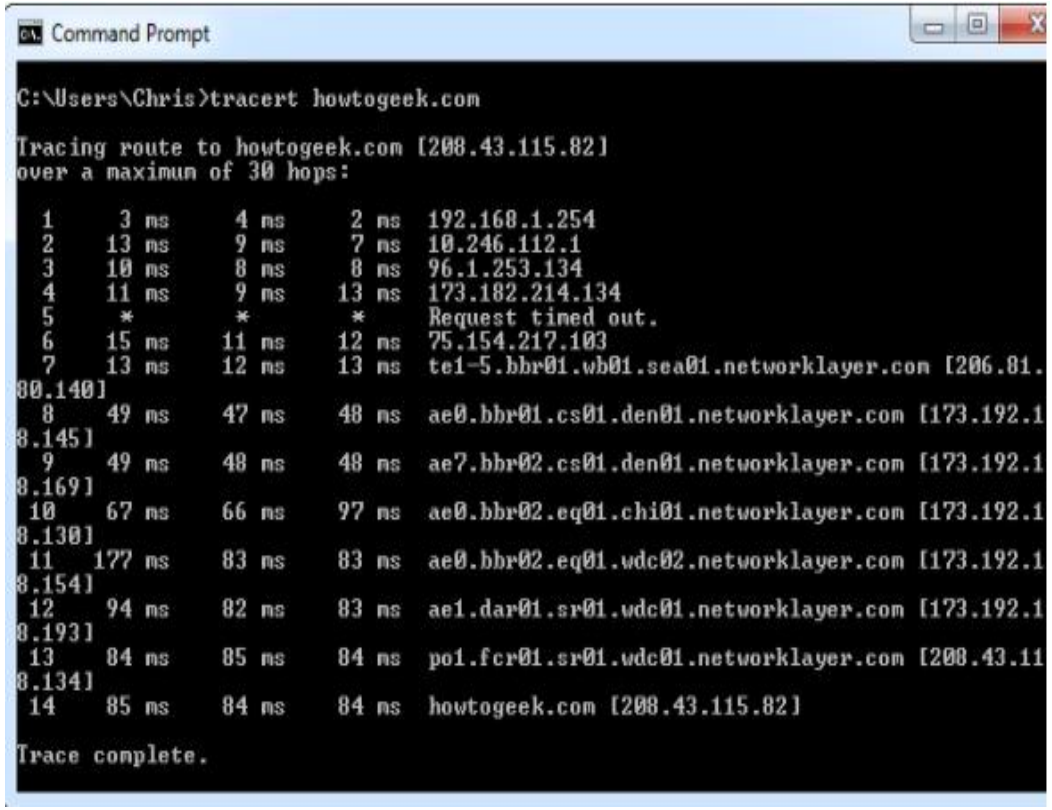


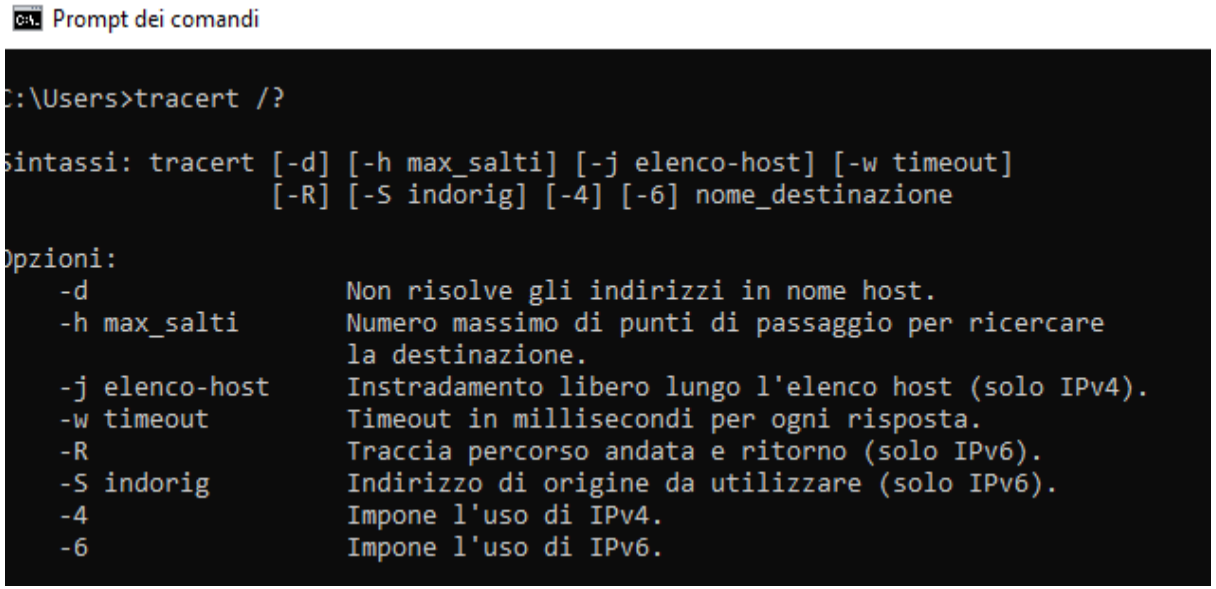
- **0 = identifica un numero di pacchetti infinito (si mandano infiniti ping) da inviare alla vittima**
- **Size = identifica quanto grandi saranno i pacchetti da inviare alla vittima**
- **Delay = identifica l'intervallo di tempo in millisecondi per ogni invio**

Contromisure a questi attacchi

- **Utilizzare firewall che filtrano il numero di pacchetti ICMP**
- **Utilizzare sonde per il controllo del traffico interno ed esterno (inbound ed outbound) delle varie reti**
- **Utilizzare SIEM che inviano alert in caso di pattern ripetuti di pacchetti uguali nella rete**

Traceroute

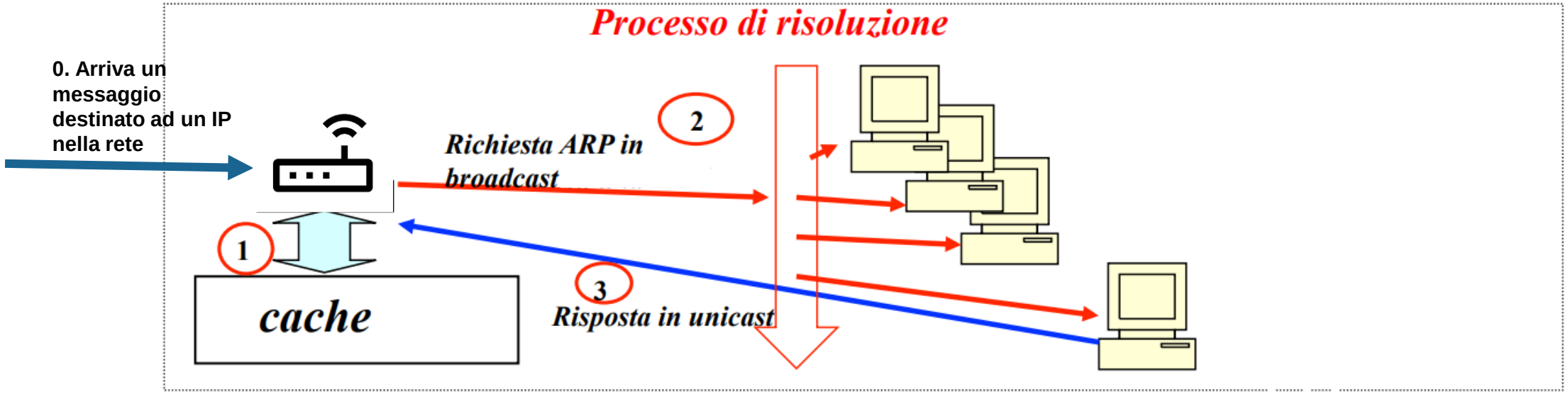

Command Prompt
C:\Users\Chris>tracert howtogeek.com
Tracing route to howtogeek.com [208.43.115.82]
over a maximun of 30 hops:
1 3 ms 4 ms 2 ms 192.168.1.254
2 13 ms 9 ms 7 ms 10.246.112.1
3 10 ms 8 ms 8 ms 96.1.253.134
4 11 ms 9 ms 13 ms 173.182.214.134
5 * * * Request timed out.
6 15 ms 11 ms 12 ms 75.154.217.103
7 13 ms 12 ms 13 ms te1-5.bbr01.wb01.sea01.networklayer.con [206.81.
80.140]
8 49 ms 47 ms 48 ms ae0.bbr01.cs01.den01.networklayer.com [173.192.1
8.145]
9 49 ms 48 ms 48 ms ae7.bbr02.cs01.den01.networklayer.com [173.192.1
8.169]
10 67 ms 66 ms 97 ms ae0.bbr02.eq01.chi01.networklayer.com [173.192.1
8.130]
11 177 ms 83 ms 83 ms ae0.bbr02.eq01.wdc02.networklayer.com [173.192.1
8.154]
12 94 ms 82 ms 83 ms ae1.dar01.sr01.wdc01.networklayer.com [173.192.1
8.193]
13 84 ms 85 ms 84 ms po1.fcr01.sr01.wdc01.networklayer.com [208.43.11
8.134]
14 85 ms 84 ms 84 ms howtogeek.com [208.43.115.82]
Trace complete.


Prompt dei comandi
:\Users>tracert /?
intassi: tracert [-d] [-h max_salti] [-j elenco-host] [-w timeout]
[-R] [-S indorig] [-4] [-6] nome_destinazione
pzioni:
-d Non risolve gli indirizzi in nome host.
-h max_salti Numero massimo di punti di passaggio per ricercare
la destinazione.
-j elenco-host Instradamento libero lungo l'elenco host (solo IPv4).
-w timeout Timeout in millisecondi per ogni risposta.
-R Traccia percorso andata e ritorno (solo IPv6).
-S indorig Indirizzo di origine da utilizzare (solo IPv6).
-4 Impone l'uso di IPv4.
-6 Impone l'uso di IPv6.

ARP

- **ARP (Address Resolution Protocol) è un protocollo a livello data-link del modello OSI**
- **Il protocollo ARP (Address Resolution Protocol) serve per conoscere il MAC address, una volta noto l'indirizzo IP di destinazione. Si occupa di fare la mappatura tra indirizzi IP e MAC**
- **Una tabella di arp offre una corrispondenza di indirizzi IP e indirizzi MAC nella cache degli apparati di rete (es. Router, pc connessi in una rete….)**

ARP



1. **Il MAC del destinatario** viene cercato nella cache.
2. **Se il MAC** non è nella cache, si cerca il destinatario con un messaggio ARP con **l'indirizzo IP del destinatario** in ***broadcast*** sulla rete.
3. **Il destinatario** riceve la richiesta ARP con il **proprio indirizzo IP** e restituisce ***in unicast*** al router **(del quale conosce l'IP ed il MAC)** il proprio indirizzo MAC.
4. Il router memorizza nella propria cache una tabella ARP con le associazioni IP-MAC che conosce
5. Se l'indirizzo IP del destinatario è su un'altra rete, il processo si ripete considerando mittente e ricevente i router (o i **proxy ARP**) delle rispettive reti.

ARP table

```
C:\Users>arp -a

Interfaccia: 192.168.1.150 --- 0x6
  Indirizzo Internet     Indirizzo fisico      Tipo
  192.168.1.1            20-b0-01-ac-ea-e8     dinamico
  192.168.1.98           34-23-87-4c-da-90     dinamico
  192.168.1.255          ff-ff-ff-ff-ff-ff     statico
  224.0.0.2              01-00-5e-00-00-02     statico
  224.0.0.22             01-00-5e-00-00-16     statico
  224.0.0.251            01-00-5e-00-00-fb     statico
  224.0.0.252            01-00-5e-00-00-fc     statico
  239.255.255.250        01-00-5e-7f-ff-fa     statico
  255.255.255.255        ff-ff-ff-ff-ff-ff     statico
```

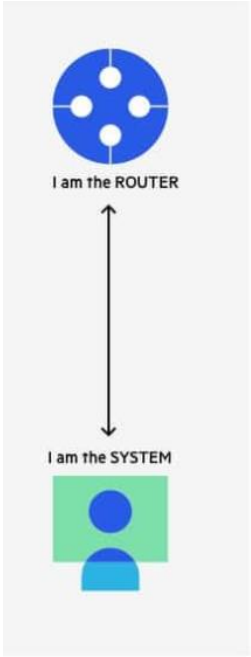
Prompt dei comandi

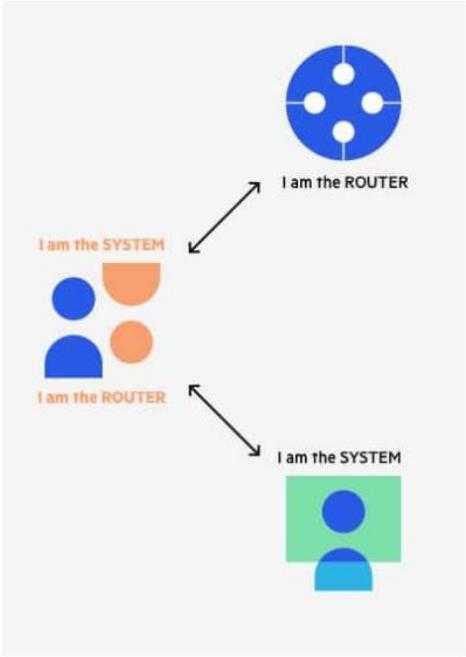
```
C:\Users>arp /?

Consente di visualizzare e modificare le tabelle di conversione da indirizzi IP
a indirizzi fisici utilizzate dal protocollo ARP (Address Resolution Protocol).

ARP -s ind_inet ind_eth [ind_if]
ARP -d ind_inet [ind_if]
ARP -a [ind_inet] [-N ind_if] [-v]

  -a            Visualizza le voci ARP correnti ottenendole dai dati del
                protocollo. Se è specificato ind_inet, verranno visualizzati
                solo gli indirizzi IP e fisico del computer specificato. Se
                sono presenti più interfacce di rete che utilizzano ARP,
                verranno visualizzate le voci di ogni tabella ARP.
  -g            Analogo a -a.
  -v            Visualizza le voci ARP correnti in modalità dettagliata.
                Vengono visualizzate anche tutte le voci non valide e le
                voci relative all'interfaccia loopback.
  ind_inet      Specifica un indirizzo Internet.
  -N ind_if     Visualizza le voci ARP per l'interfaccia di rete specificata
                da ind_if.
  -d            Elimina l'host specificato da ind_inet. In ind_inet è
                possibile utilizzare il carattere jolly asterisco (*) per
                eliminare tutti gli host.
  -s            Aggiunge l'host e associa l'indirizzo Internet ind_inet
                all'indirizzo fisico ind_eth. L'indirizzo fisico è un numero
                esadecimale di 6 byte separati da trattini.
                La voce è permanente.
  ind_eth       Specifica un indirizzo fisico.
  ind_if        Se presente, specifica l'indirizzo Internet dell'interfaccia
                di cui si desidera modificare la tabella di conversione degli
                indirizzi. Se non è presente, verrà utilizzata la prima
                interfaccia utilizzabile.
Esempio:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  ....Aggiunge una voce statica.
  > arp -a                                    ....Visualizza la tabella ARP.
```

ARP Spoofing

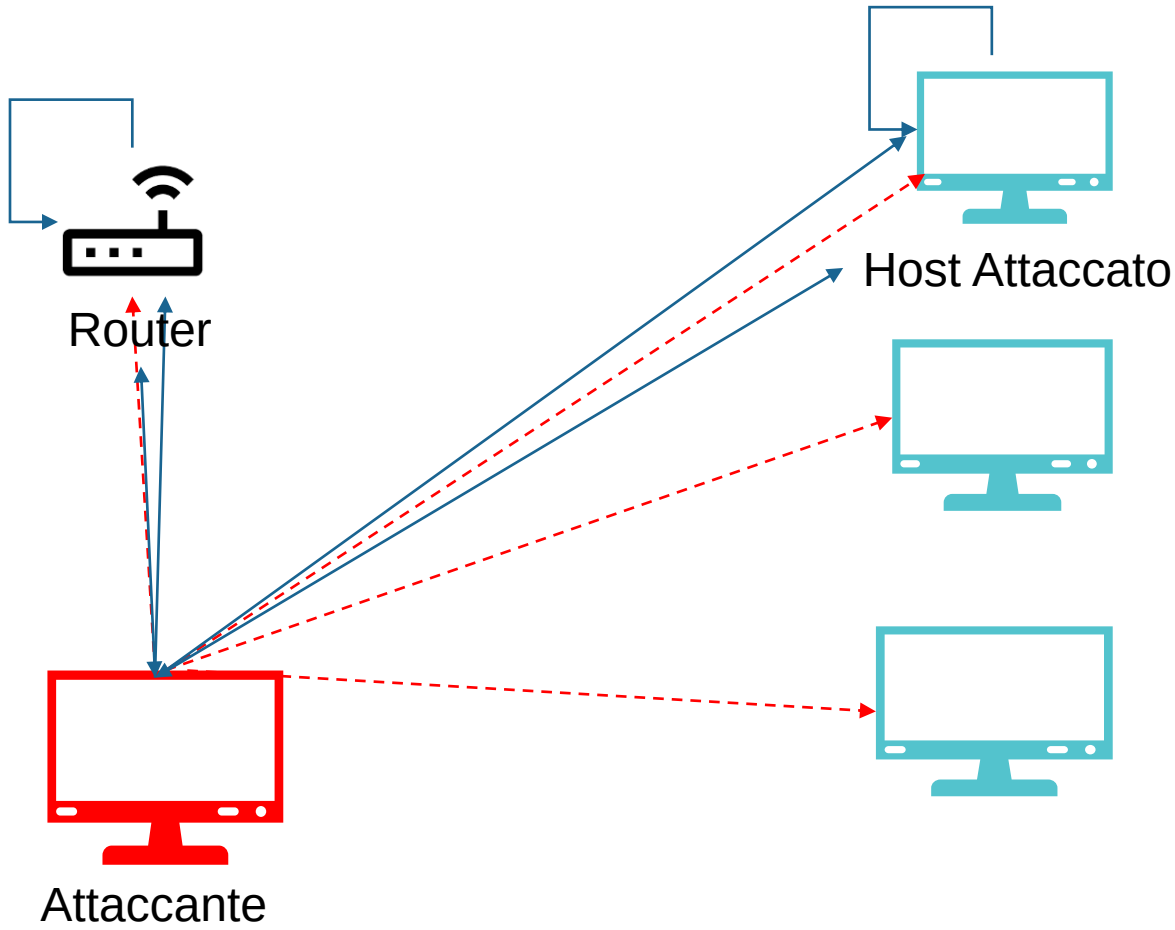
- **L'ARP Spoofing (Arp Poisoning) è un attacco che consente l'invio di pacchetti ARP reply contraffatti, in cui il computer che riceve questi pacchetti ARP reply crede di spedire i frame ethernet al legittimo destinatario della connessione, invece li spedisce al computer che si è intromesso nella comunicazione.**

- **È un tipico esempio di Man-In-The Middle:**





ARP Spoofing



1: L’attaccante, che ha accesso alla rete, fa lo scan della rete ed ottiene l’IP del router e di un altro host

2: L’attaccante invia delle richieste ARP maligne facendo credere all’host di cui ha rubato l’IP al punto 1 di essere il router (utilizzando l’IP del router che conosce) ed al router di essere l’host di cui ha ottenuto l’IP al punto 1

3: Il router e l’host aggiornano le loro arp table con l’indirizzo IP dell’attaccante associato al MAC del router facendolo risultare così nel mezzo della comunicazione

Come si rileva un ARP Spoofing?

```
arp -a
```

```
Internet Address      Physical Address

192.168.5.1           00-14-22-01-23-45
192.168.5.201         40-d4-48-cr-55-b8
192.168.5.202         00-14-22-01-23-45
```

- **Se nella tabella ARP esistono due MAC uguali con IP diversi, allora qualcuno sta provando ad intromettersi nella rete**
- **In questo caso, l'IP .1 è il router, dunque l'attaccante avrà IP 192.168.5.202**

Protocolli a livello applicazione (Accenno)

- **Telnet (TCP, porta 23): protocollo che emula un terminale su rete per le connettività in remoto, non permette trasferimento di file**
- **FTP (TCP, porta 20): uguale al precedente, ma permette il trasferimento di file**
- **SMTP (TCP, porta 25): protocollo usato per trasmettere messaggi email da un client verso un server email e viceversa**
- **POP3 (TCP, porta 110): stesso uso del precedente**
- **DHCP (UDP porte 67 e 68): usato per il controllo centralizzato degli indirizzi di rete**
- **HTTP (TCP, porta 80): usato per trasmettere gli elementi da un web server ad un web browser**
- **SSL (TCP, porta 443): utilizzato per rendere sicure le comunicazioni tramite https o altri protocolli di comunicazione a livello applicazione**

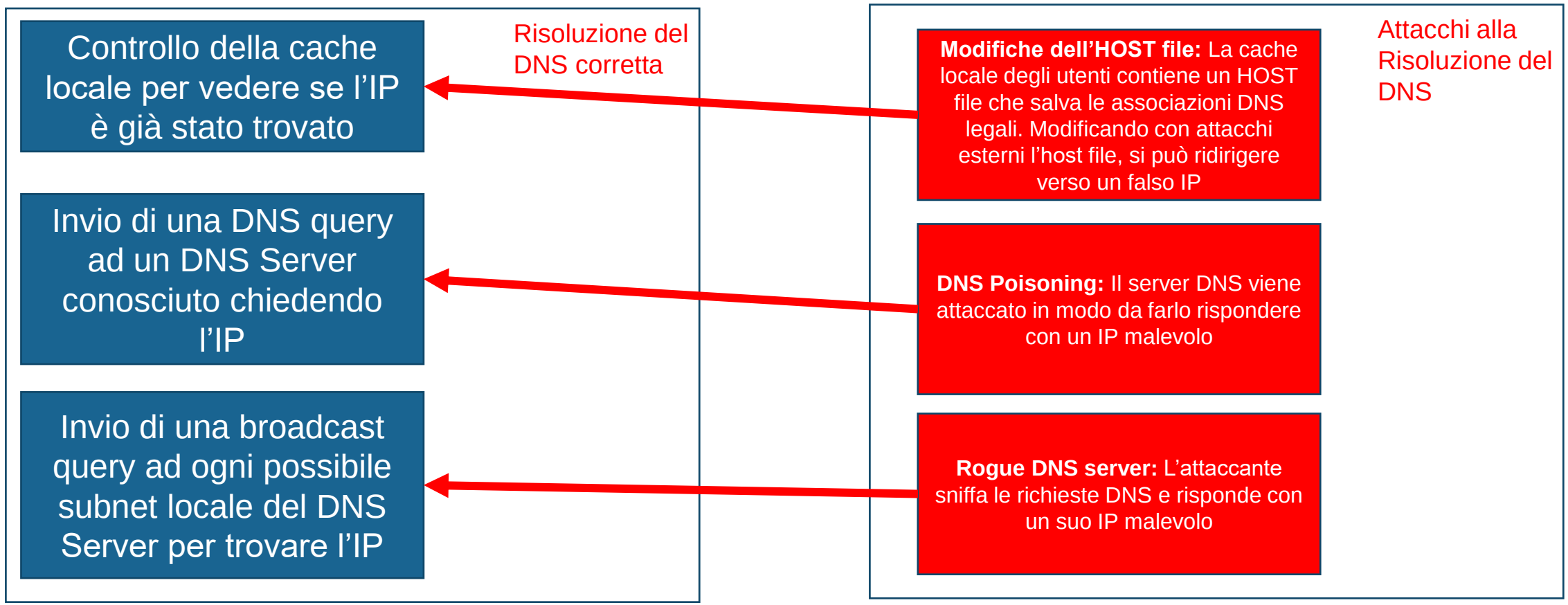
DNS – Domain Name System

- **Il livello applicazione ha l'obiettivo di interfacciarsi con gli utenti, dunque bisogna cercare di rendere le cose facili**
- **E' molto più semplice ricordare www.google.com piuttosto che 64.233.187.99**
- **Questo è il motivo per cui è stata sviluppata la traduzione degli indirizzi. Il Domain Name System (DNS)**

Domain Name	www.google.com
IP address	64.233.187.99
MAC address	Aa:bb:cc:ff:11

Attacchi al DNS

- **Attacco che crea una falsificazione del DNS in modo da ridirigere un client verso un IP non desiderato.**




Grazie per l’attenzione