FlashStart+MikroTik

Internet Protection with DNS Filtering

About the Trainer

Marco Boschini

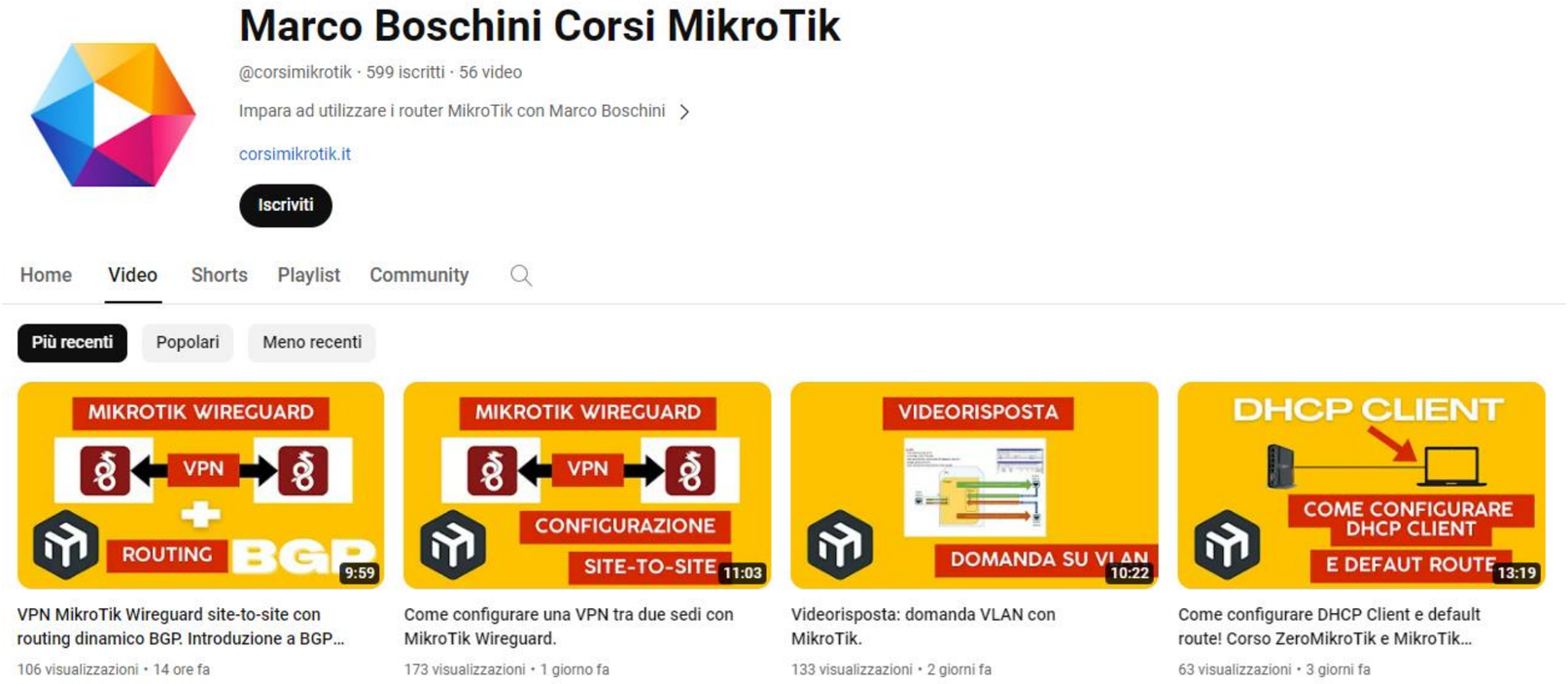
- MikroTik Certified Trainer
- MTCNA, MTCRE, MTCINE, MTCWE, MTCTCE, MTCUME, MTCIPv6, MTCSE, MTCSWE, MTCEWE
- Founder CorsiMikroTik.it
- marco@corsimikrotik.it
- https://www.linkedin.com/in/marco-boschini/

SCAN ME

YouTube

Marco Boschini Corsi MikroTik

https://www.youtube.com/corsimikrotik



Telegram

Corsi MikroTik

t.me/corsimikrotik

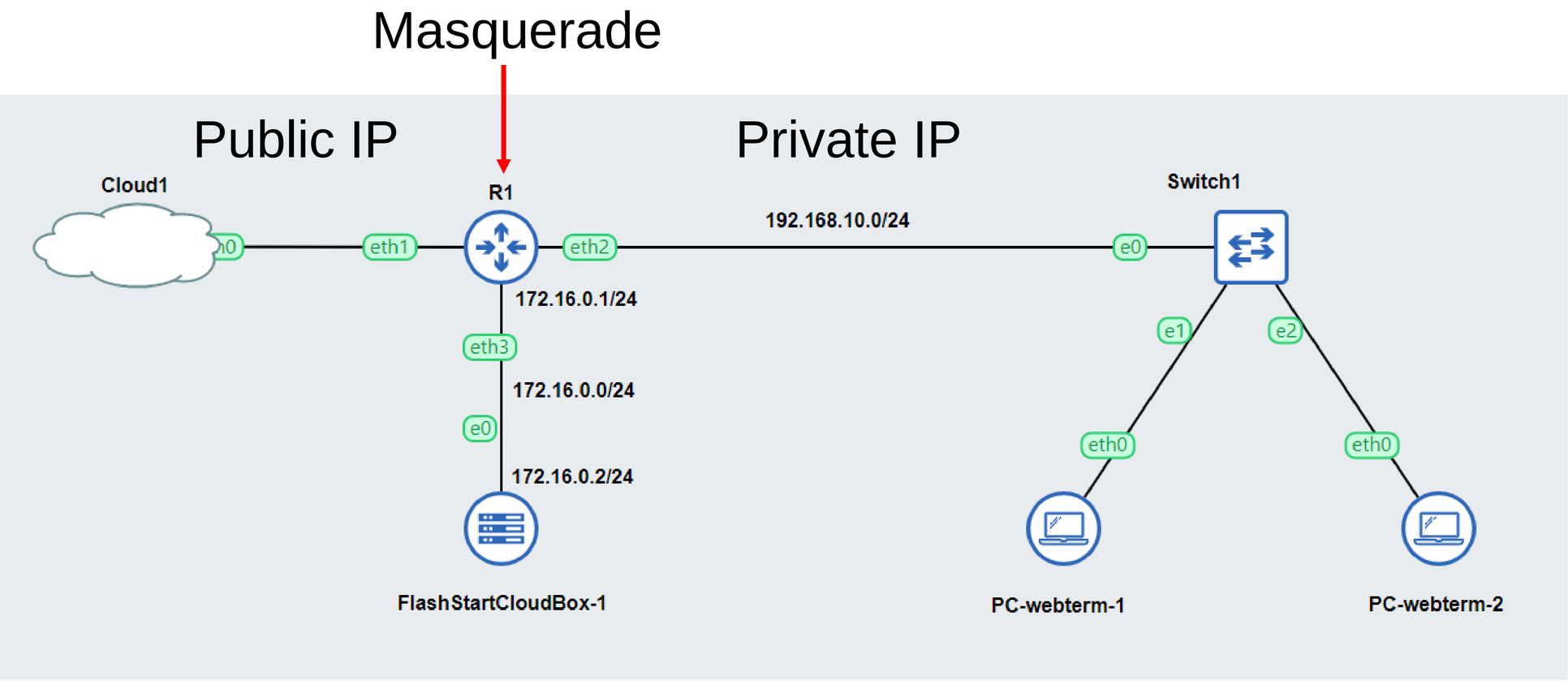
Canale Corsi MikroTik

SCAN ME

Obiettivi

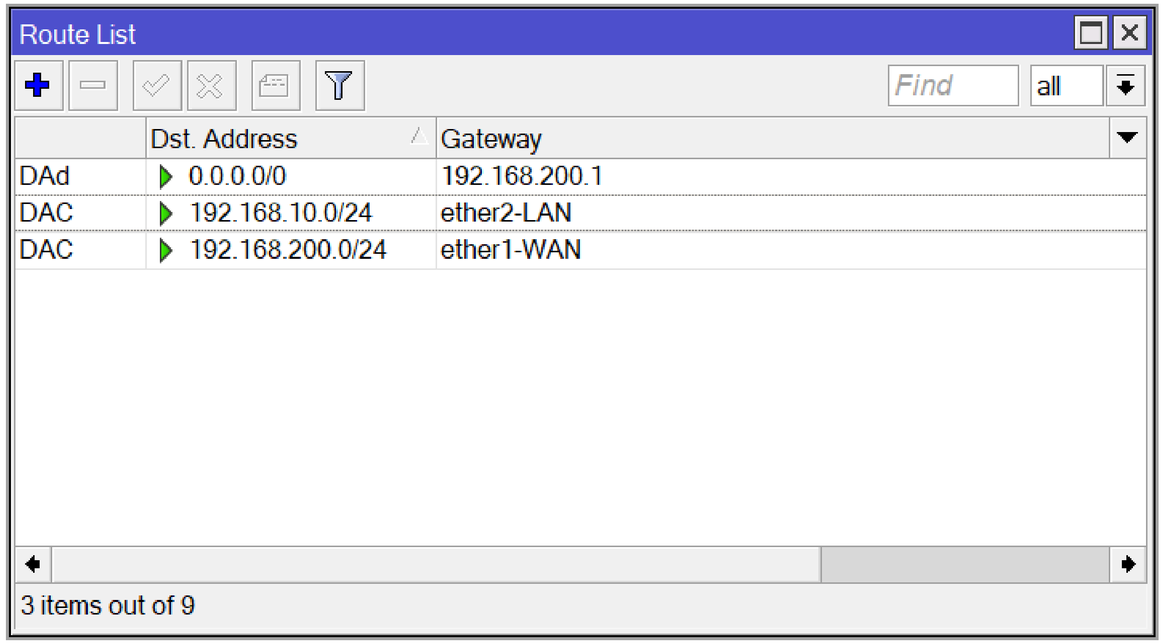
- Comprendere come funziona un router
- Comprendere come come un PC può comunicare con internet
- Comprendere a cosa serve il DNS
- Comprendere come funziona un DHCP Server
- Comprendere come catturare le richieste DNS dalla tua LAN

Come funziona un router

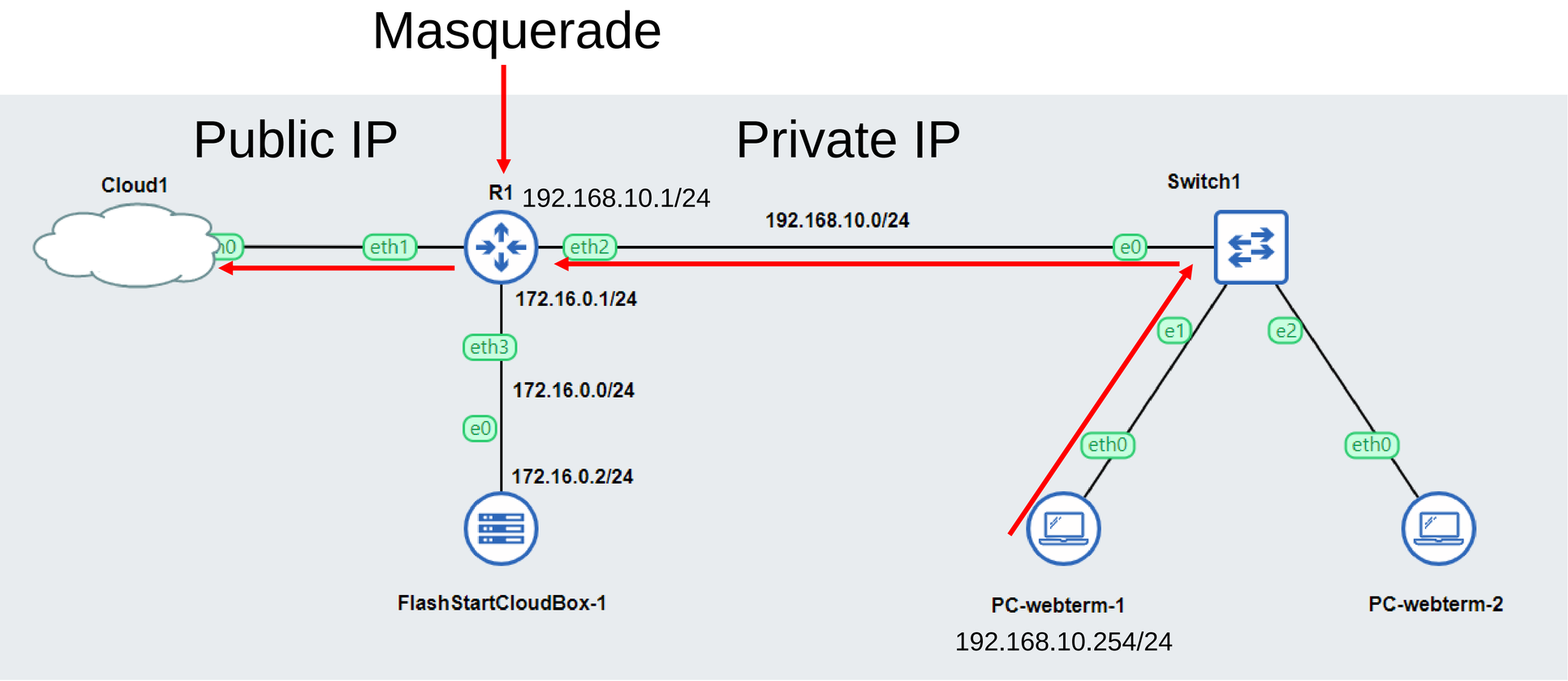


Routing

- Routing utilizza indirizzi IP, non utilizza i nomi di site (es. google.com)

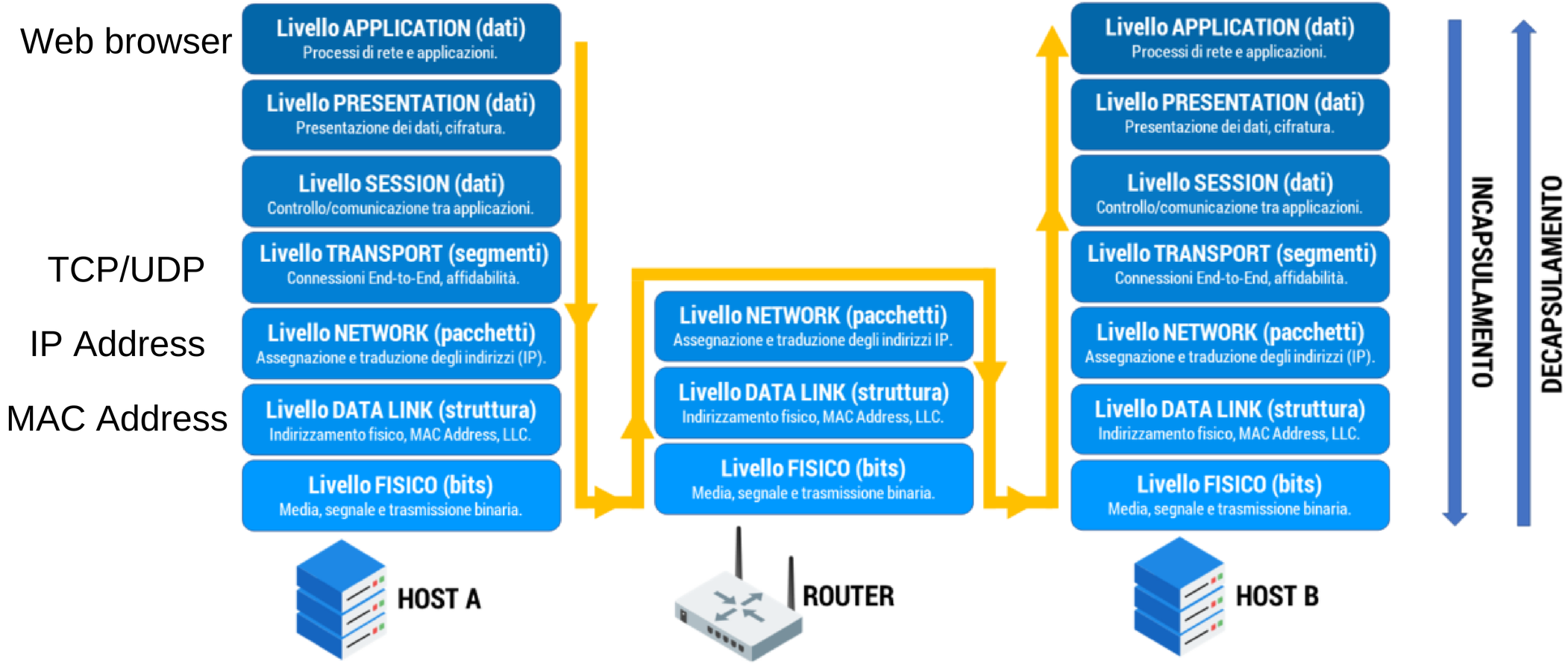


Come comunica su internet un PC



Default route 0.0.0.0/0
gateway=192.168.10.1

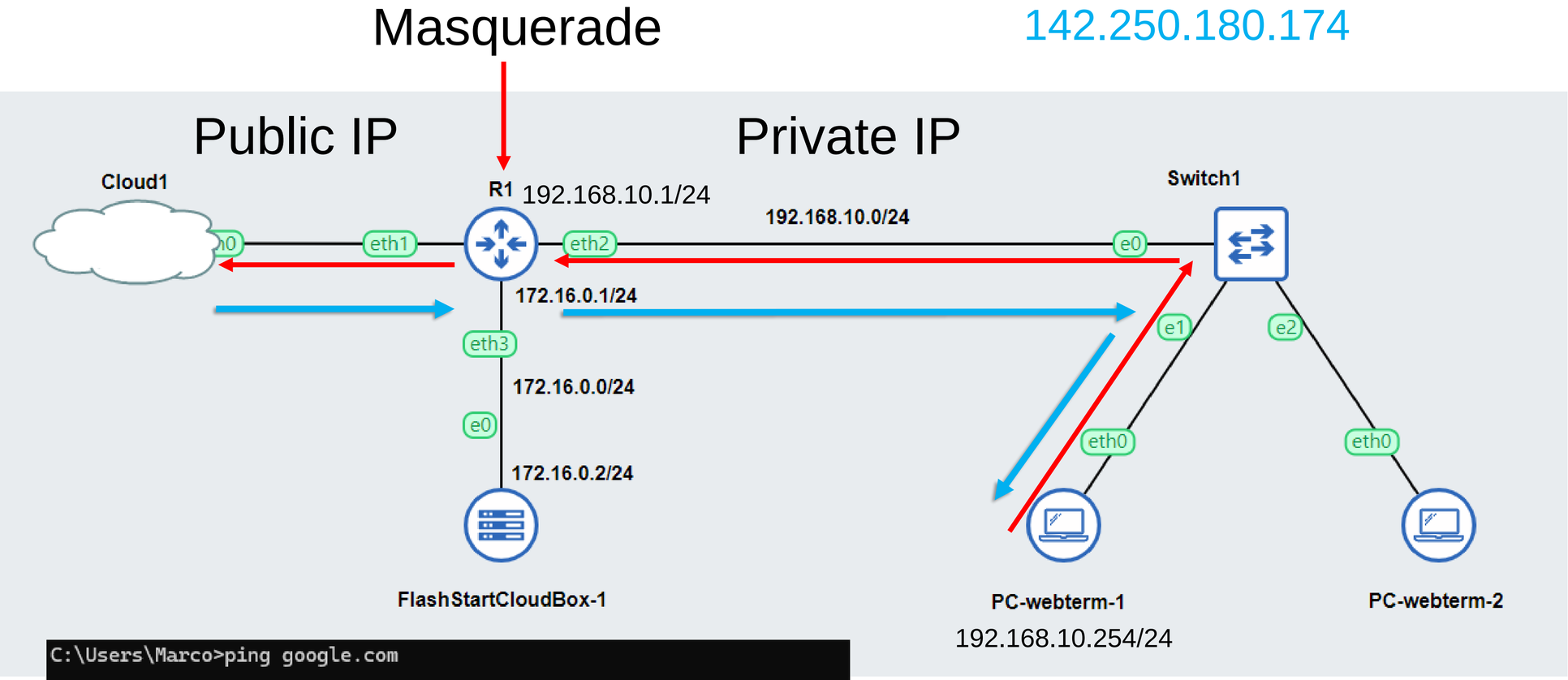
Routing


Web browser
TCP/UDP
IP Address
MAC Address
Livello APPLICATION (dati)
Processi di rete e applicazioni.
Livello PRESENTATION (dati)
Presentazione dei dati, cifratura.
Livello SESSION (dati)
Controllo/comunicazione tra applicazioni.
Livello TRANSPORT (segmenti)
Connessioni End-to-End, affidabilità.
Livello NETWORK (pacchetti)
Assegnazione e traduzione degli indirizzi (IP).
Livello DATA LINK (struttura)
Indirizzamento fisico, MAC Address, LLC.
Livello FISICO (bits)
Media, segnale e trasmissione binaria.
HOST A
Livello NETWORK (pacchetti)
Assegnazione e traduzione degli indirizzi IP.
Livello DATA LINK (struttura)
Indirizzamento fisico, MAC Address, LLC.
Livello FISICO (bits)
Media, segnale e trasmissione binaria.
ROUTER
Livello APPLICATION (dati)
Processi di rete e applicazioni.
Livello PRESENTATION (dati)
Presentazione dei dati, cifratura.
Livello SESSION (dati)
Controllo/comunicazione tra applicazioni.
Livello TRANSPORT (segmenti)
Connessioni End-to-End, affidabilità.
Livello NETWORK (pacchetti)
Assegnazione e traduzione degli indirizzi (IP).
Livello DATA LINK (struttura)
Indirizzamento fisico, MAC Address, LLC.
Livello FISICO (bits)
Media, segnale e trasmissione binaria.
HOST B
INCAPSULAMENTO
DECAPSULAMENTO

DNS

PC: Qual è l'indirizzo IP di www.google.com?

DNS: L' indirizzo IP è 142.250.180.174



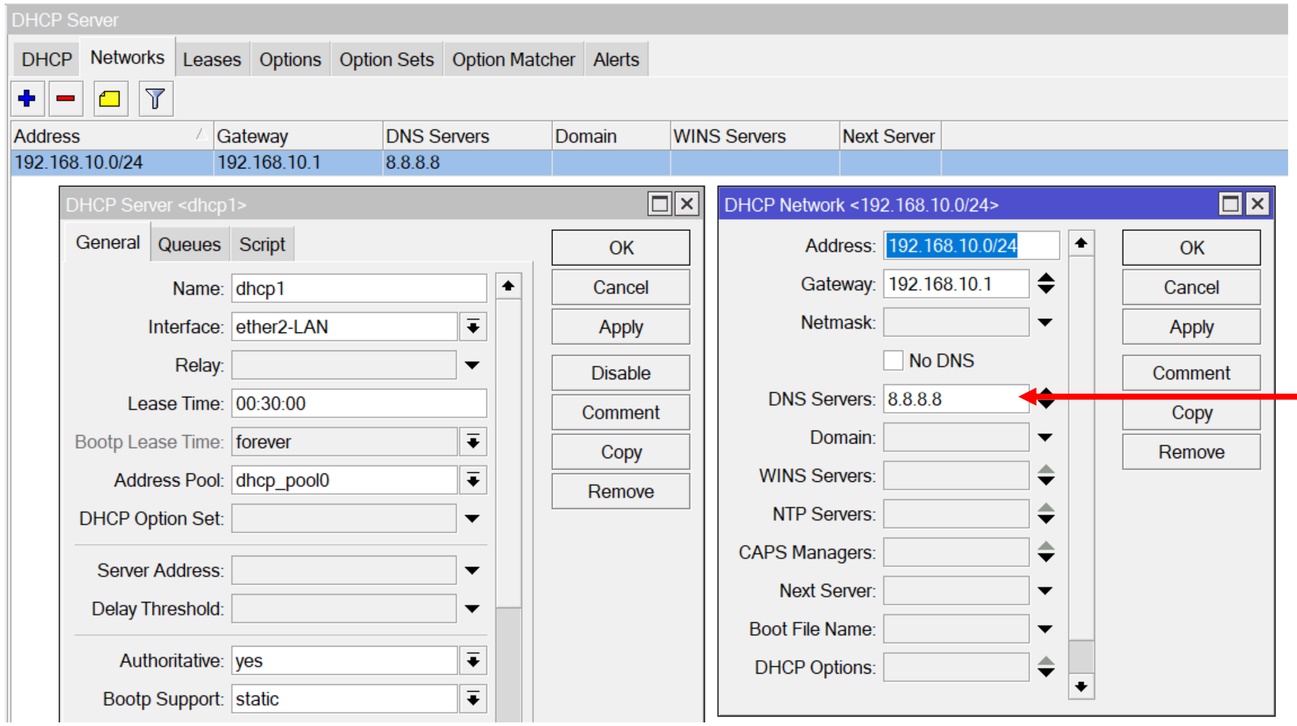

```
C:\Users\Marco>ping google.com

Esecuzione di Ping google.com [142.250.180.174] con 32 byte di dati:
Risposta da 142.250.180.174: byte=32 durata=4ms TTL=118
Risposta da 142.250.180.174: byte=32 durata=4ms TTL=118
```

Default route 0.0.0.0/0
gateway=192.168.10.1

Come funziona il DHCP Server

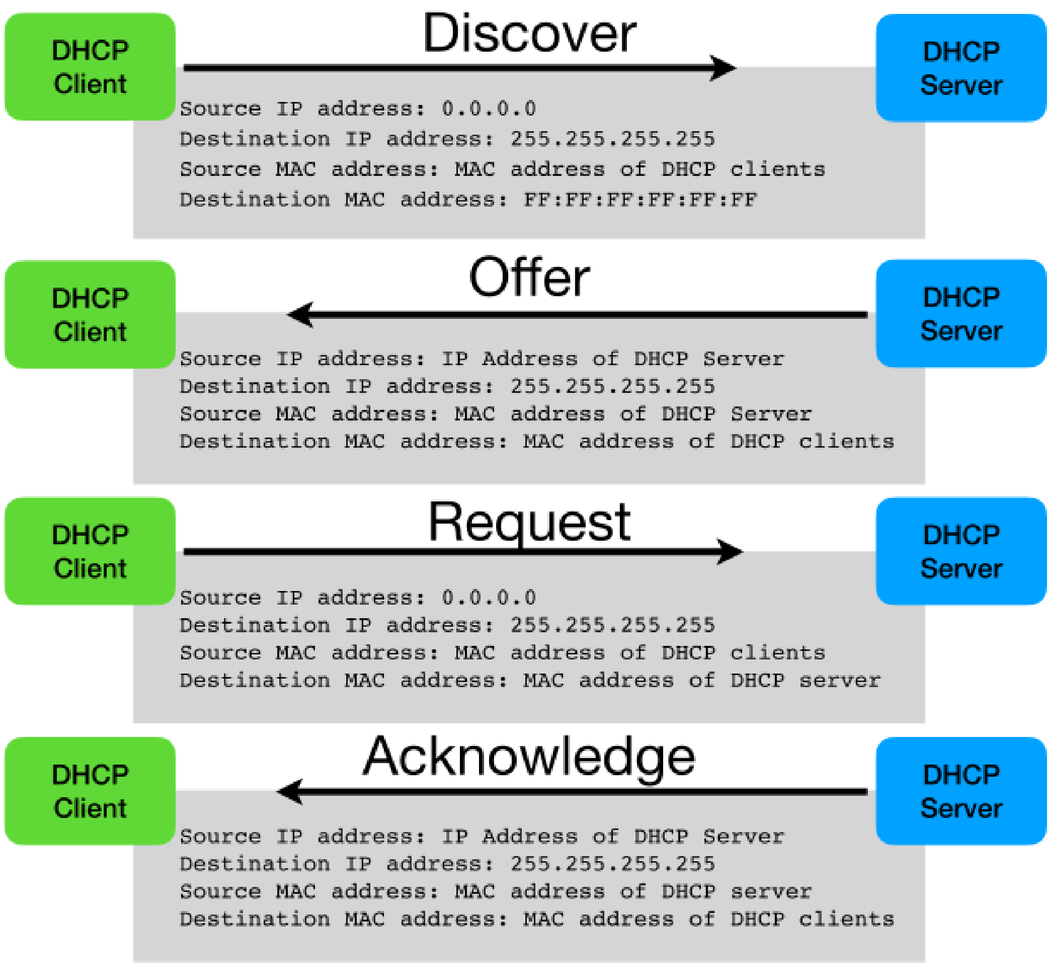
- I dispositivi di una rete LAN possono ricevere i parametri IP address, subnet mask, gateway e DNS dal DHCP Server



Puoi inviare la configurazione di uno specifico IP DNS ai DHCP Clients

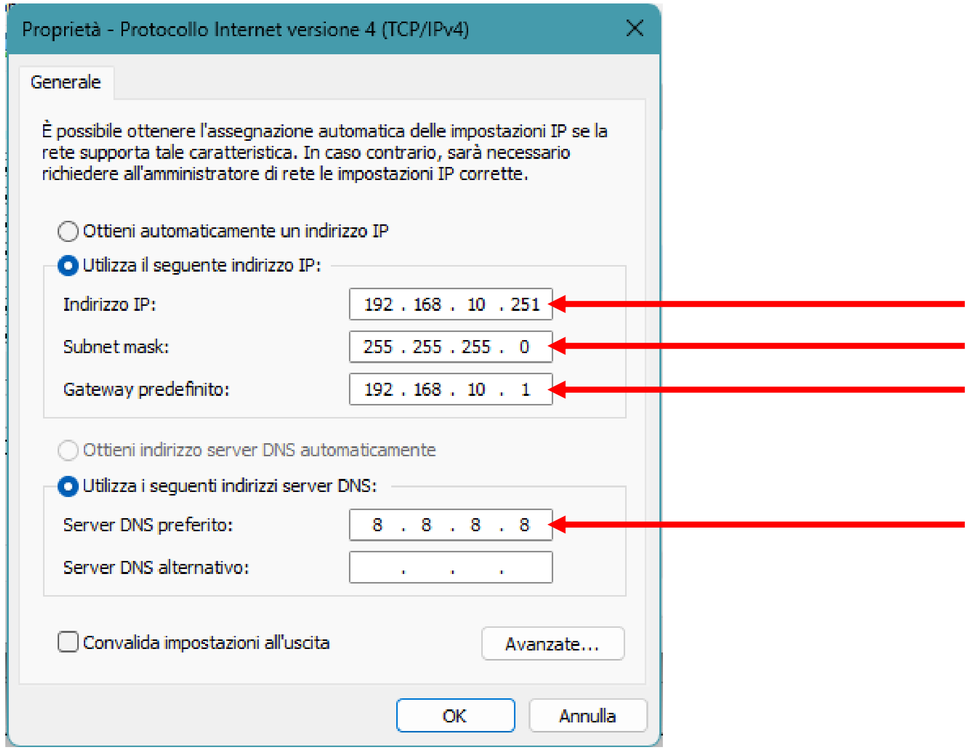
Come funziona il DHCP Server

- DORA Process
- **D**iscover
- **O**ffer
- **R**equest
- **A**cknowledge



Parametri di rete manuali

- A device in a LAN can set parameters manually



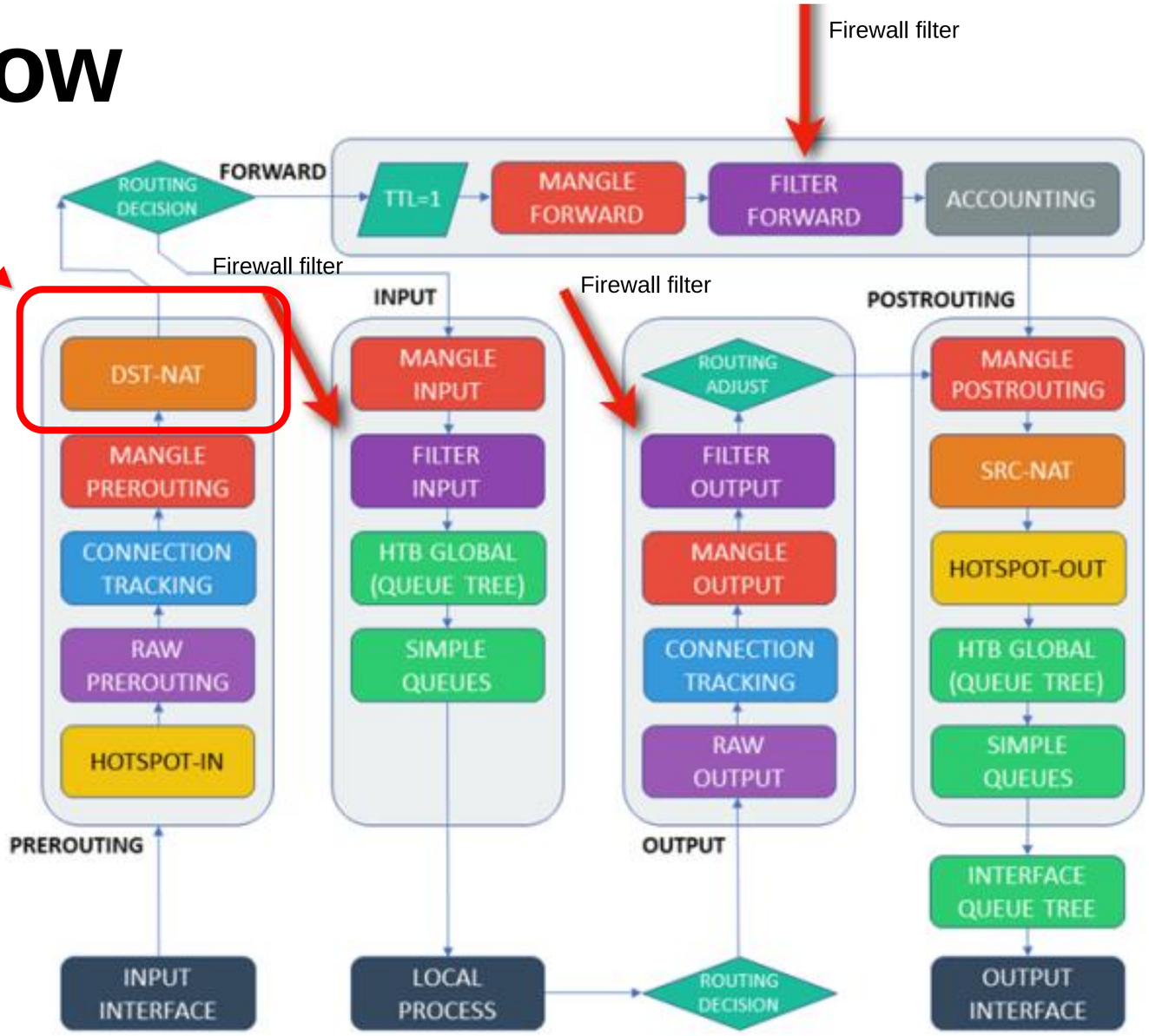
Come catturare le richieste DNS dalla rete LAN

- DNS requests sono trasmesse usando il protocollo UDP porta 53, e con protocollo TCP porta 53 se la richiesta eccede la dimensione di 512 bytes.
- Puoi cambiare l'indirizzo IP di destinazione di un pacchetto e inviare la richiesta DNS al server DNS FlashStart (e.g. 185.236.104.104).
- FlashStart risponderà con l'indirizzo IP corretto solo per le richieste permesse (connessioni verso siti sicuri e autorizzati).
- FlashStart risponderà con un indirizzo IP di "blocco" se la richiesta è destinate ad un sito proibito o malevolo (non considerate sicuro o bloccato)

Packet Flow

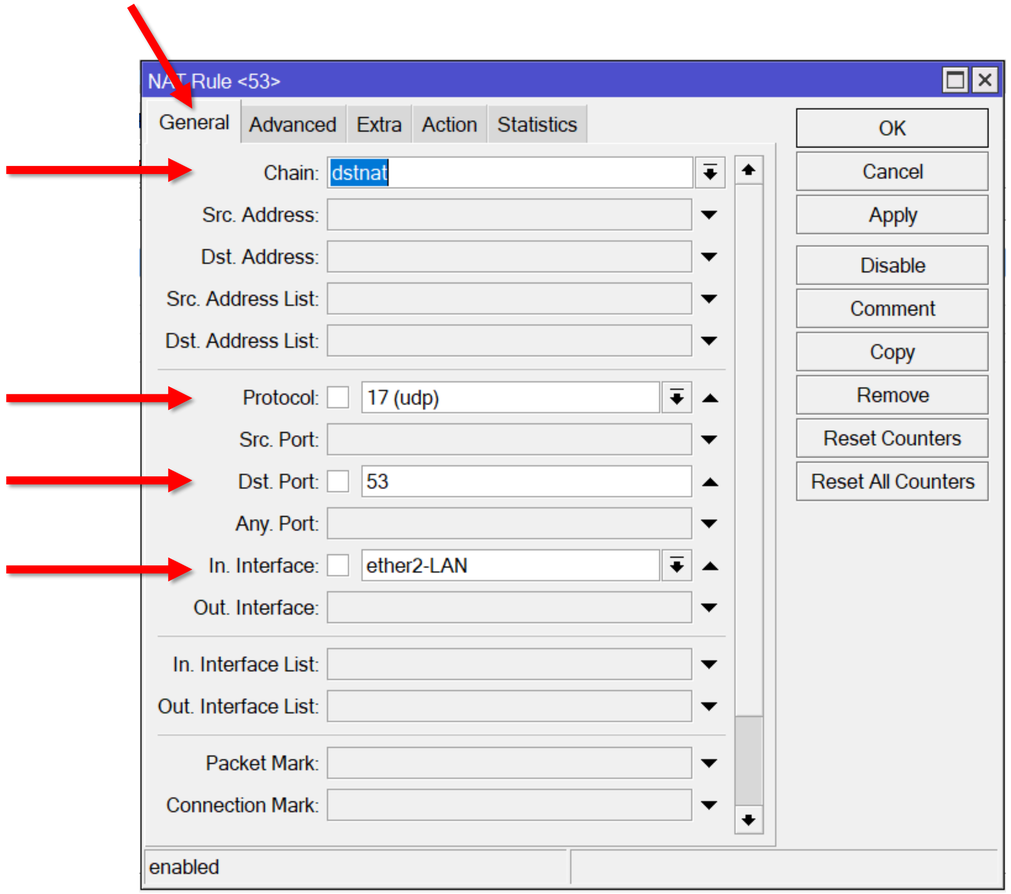
Qui puoi cambiare l'indirizzo IP di destinazione

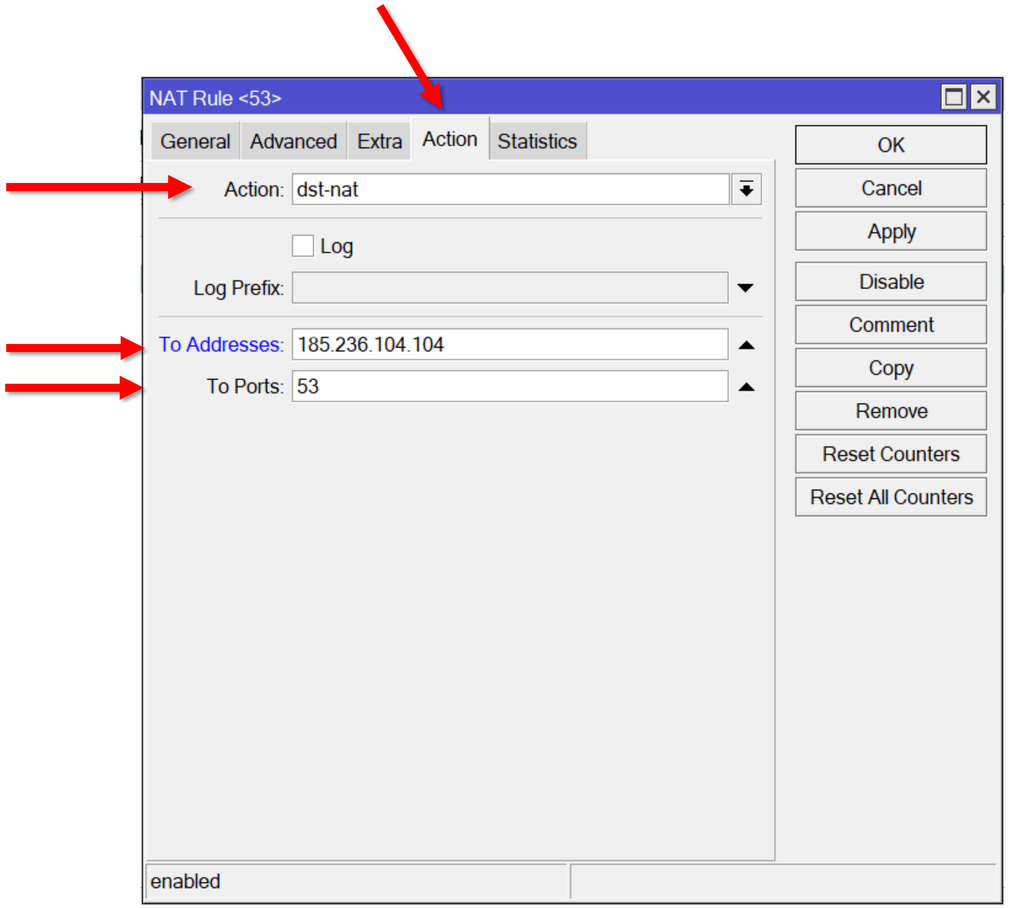
Src 192.168.88.254
Dst ~~8.8.8.8~~
Dst 185.236.104.104



Src 192.168.88.254
Dst 8.8.8.8

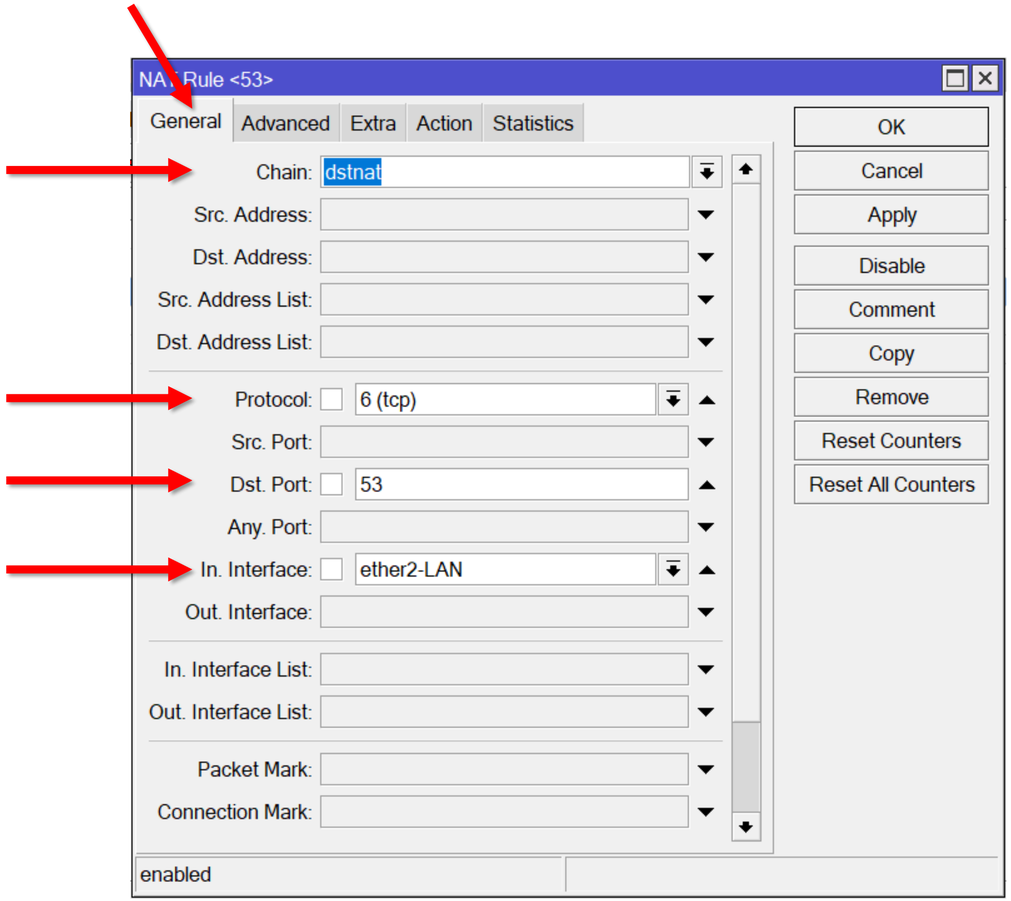
Come cambiare l'IP di destinazione ad una richiesta DNS



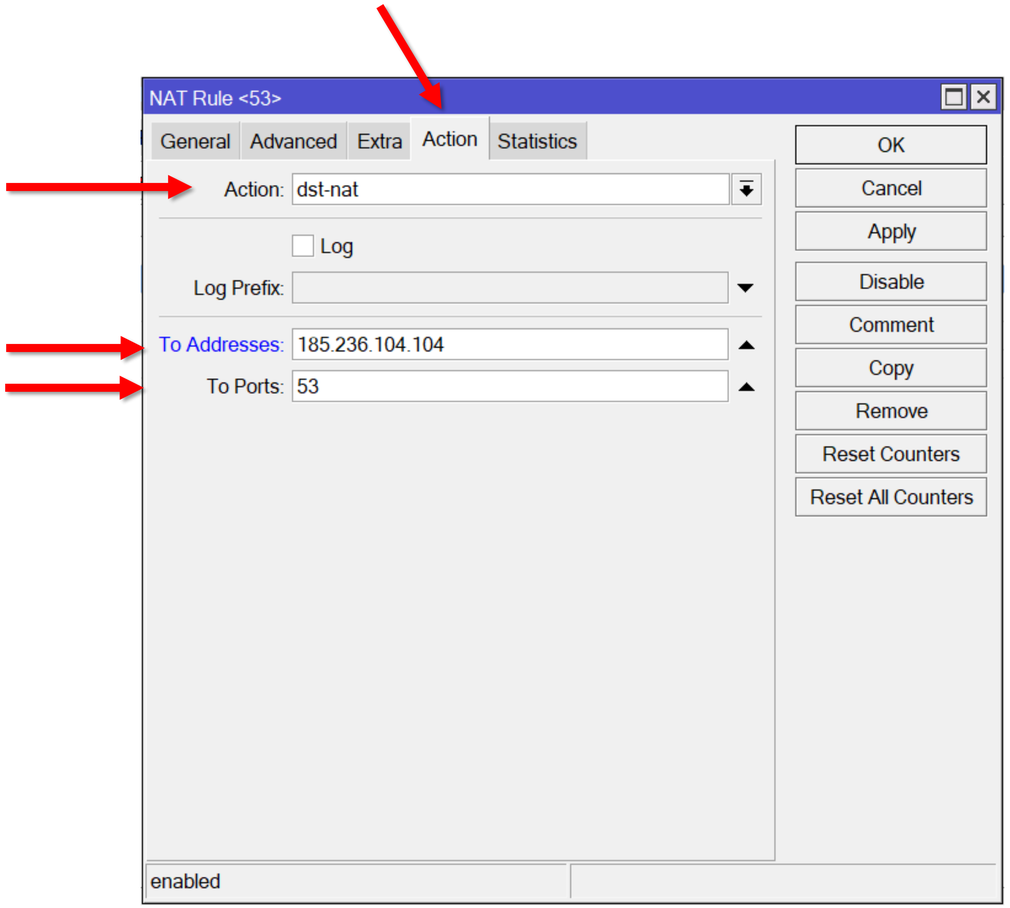


IP > Firewall > NAT > Add (+)

Come cambiare l'IP di destinazione di una richiesta DNS



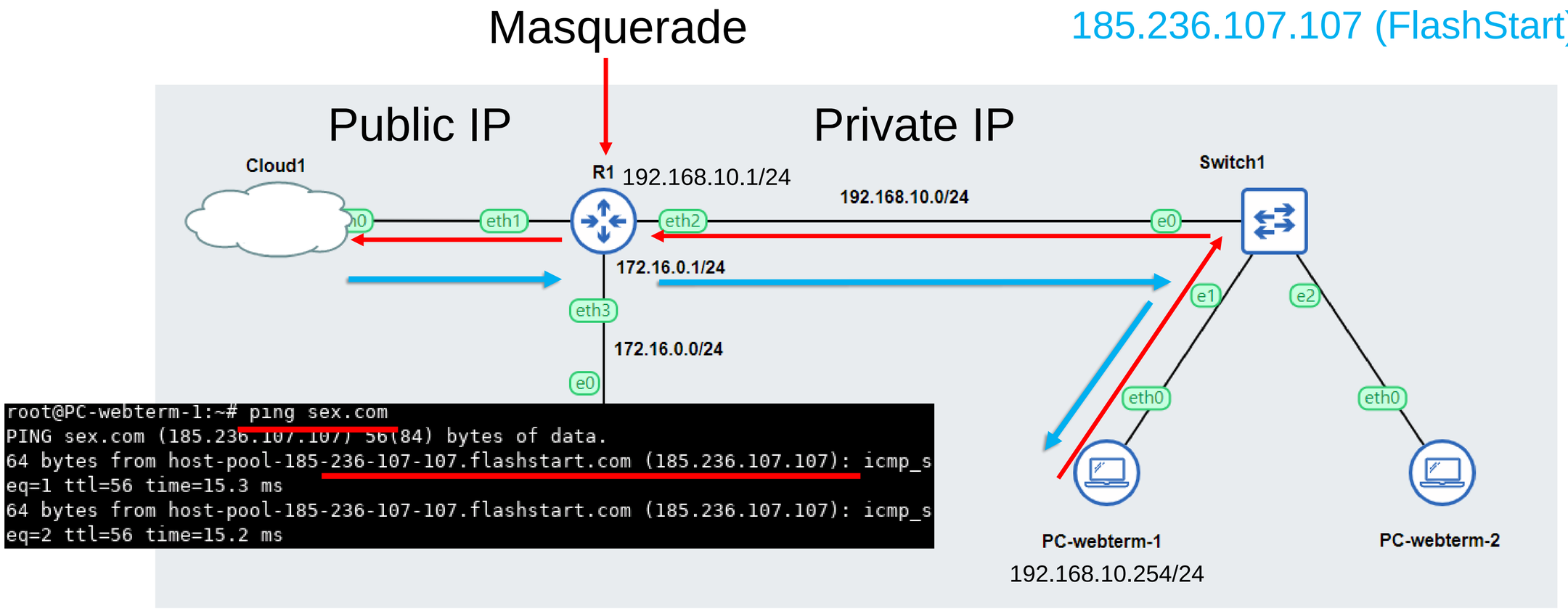
IP > Firewall > NAT > Add (+)



FlashStart

PC: Qual è l'indirizzo IP di www.sex.com?

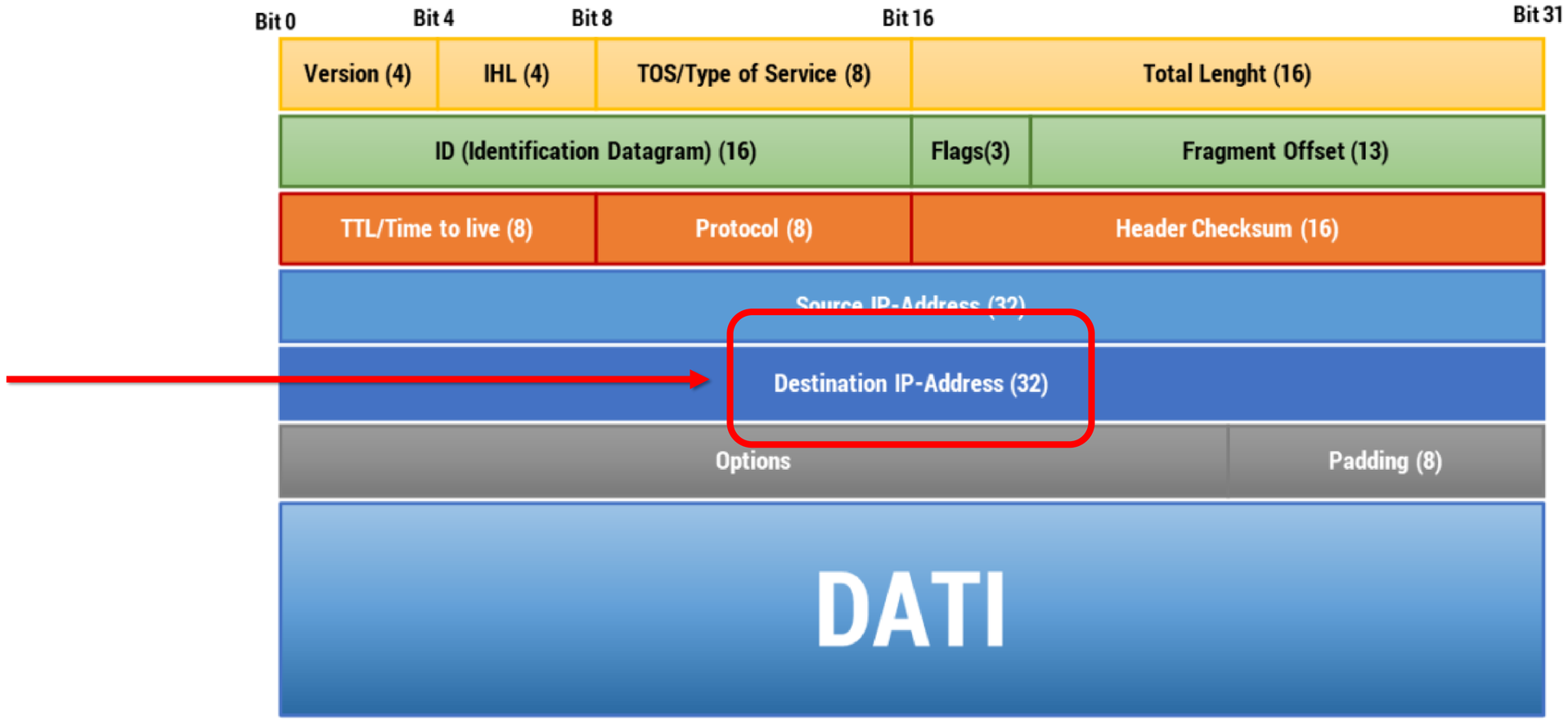
FlashStart: l'indirizzo IP è 185.236.107.107 (FlashStart)




```
root@PC-webterm-1:~# ping sex.com
PING sex.com (185.236.107.107) 56(84) bytes of data.
64 bytes from host-pool-185-236-107-107.flashstart.com (185.236.107.107): icmp_s
eq=1 ttl=56 time=15.3 ms
64 bytes from host-pool-185-236-107-107.flashstart.com (185.236.107.107): icmp_s
eq=2 ttl=56 time=15.2 ms
```

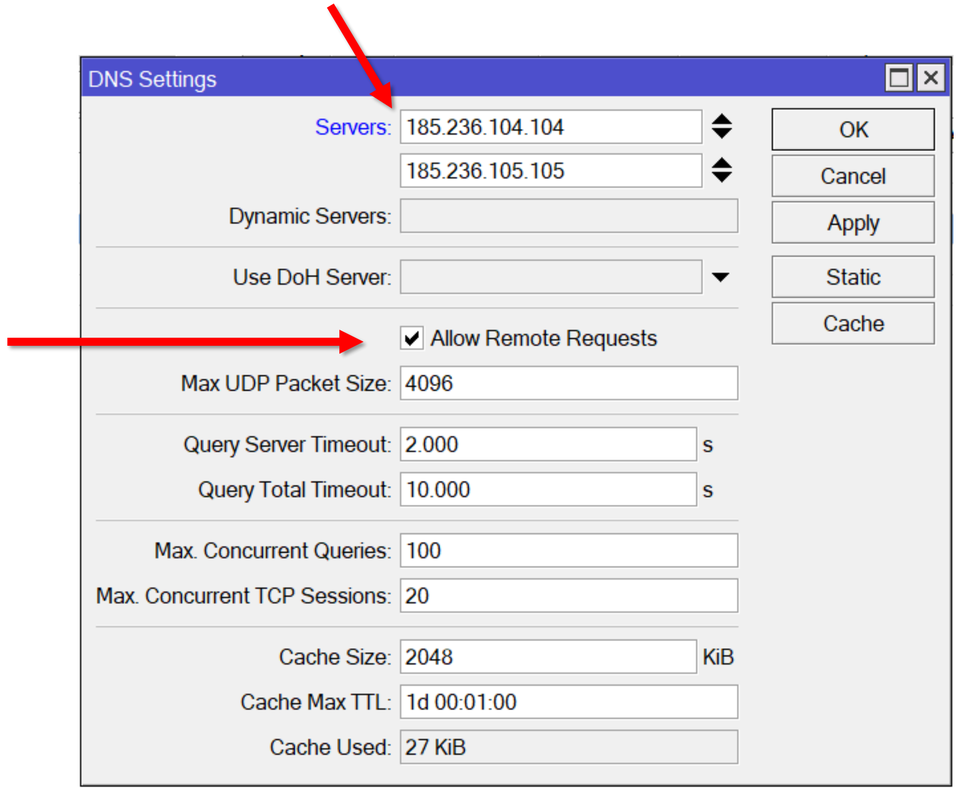
Default route 0.0.0.0/0
gateway=192.168.10.1

IP Packet


Bit 0
Bit 4
Bit 8
Bit 16
Bit 31
Version (4)
IHL (4)
TOS/Type of Service (8)
Total Lenght (16)
ID (Identification Datagram) (16)
Flags(3)
Fragment Offset (13)
TTL/Time to live (8)
Protocol (8)
Header Checksum (16)
Source IP-Address (32)
Destination IP-Address (32)
Options
Padding (8)
DATI

MikroTik DNS Relay

- Puoi usare un router MikroTik come DNS Relay
- RouterOS richiede al server DNSla risoluzione del nome se non è presente nella sua cache locale
- RouterOS risponde direttamente alla richiesta DNS se è presente nella sua cache (miglioramento di velocità)

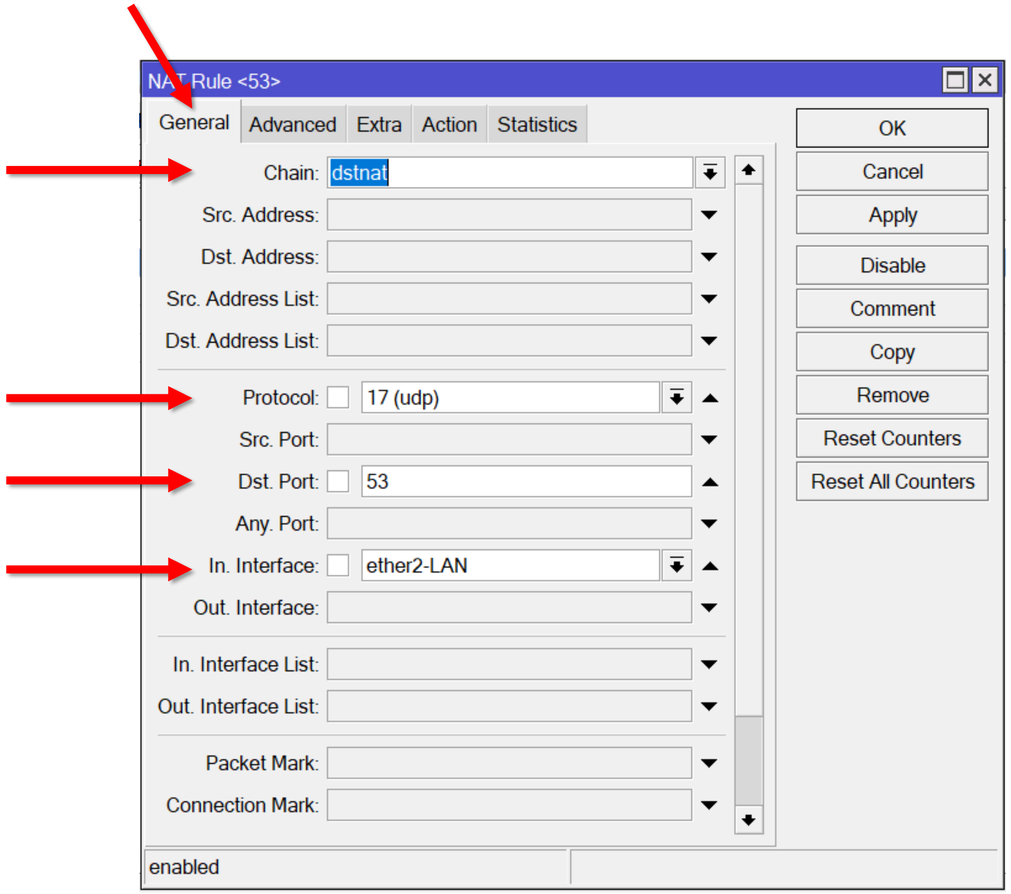


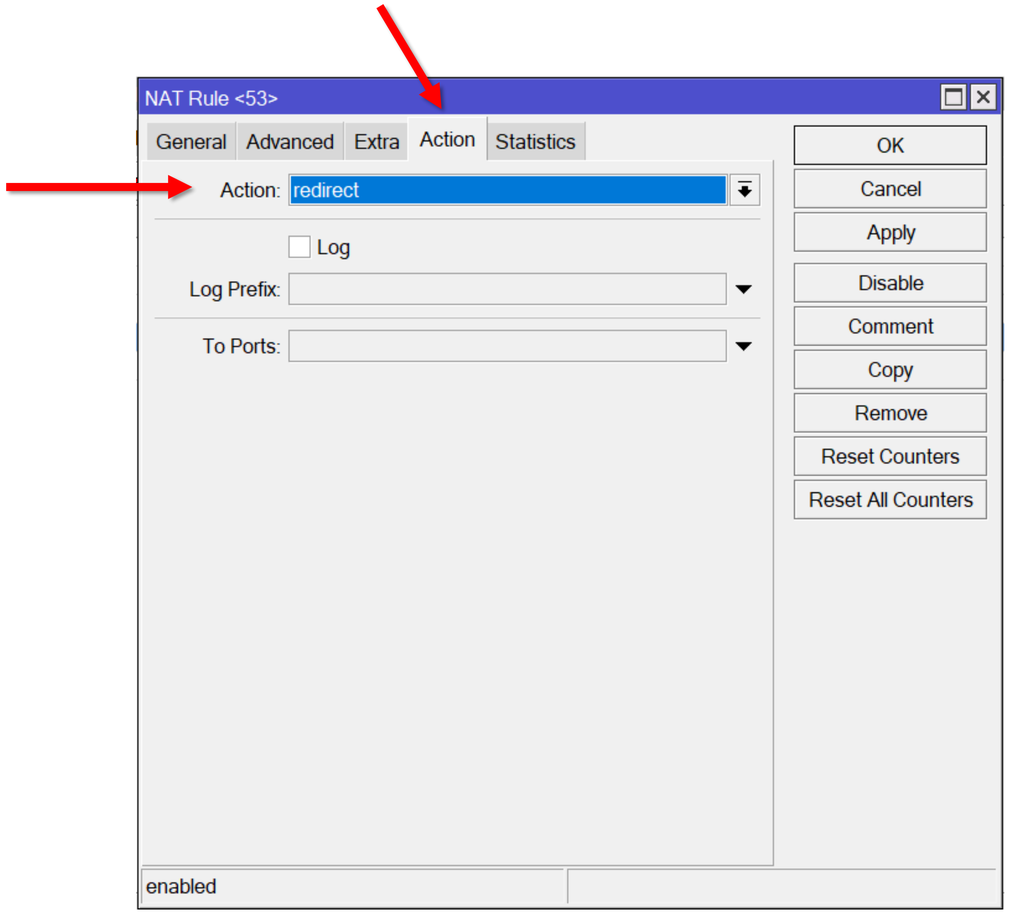
IP > DNS

Redirect

- Speciale tipo di DST-NAT
- Redirige i pacchetti al router stesso

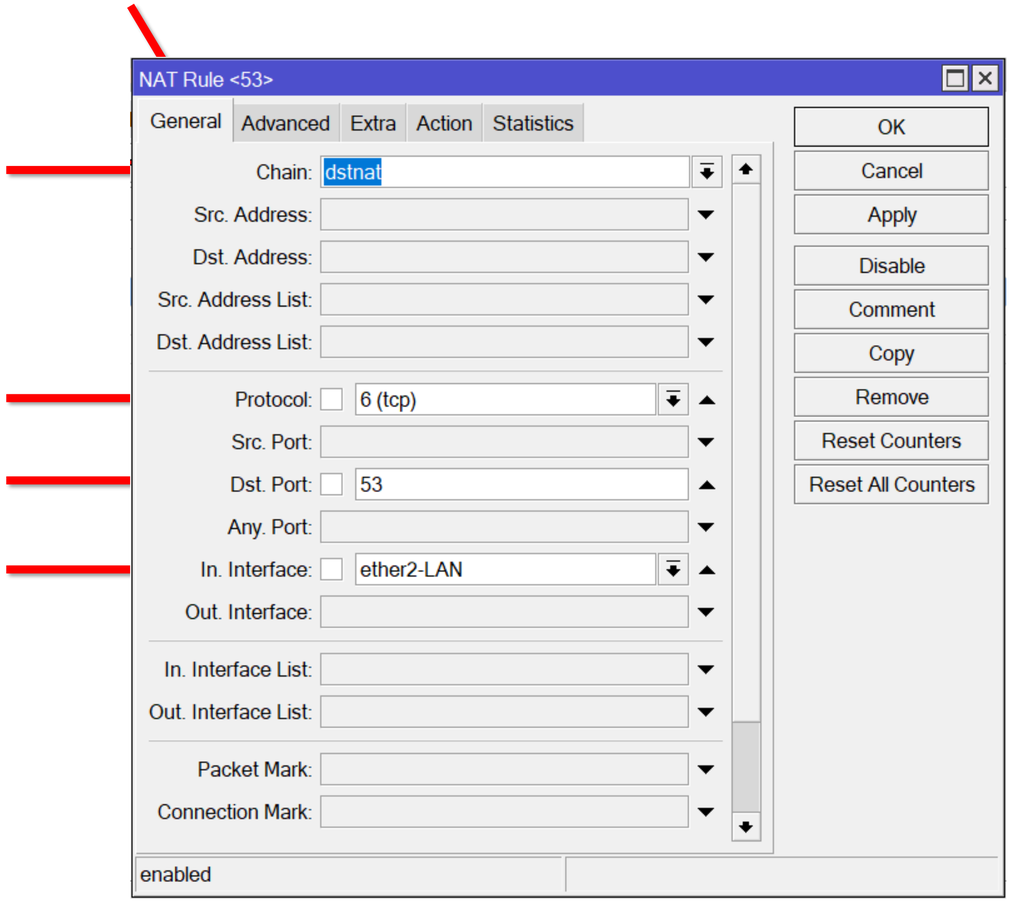
Redirect



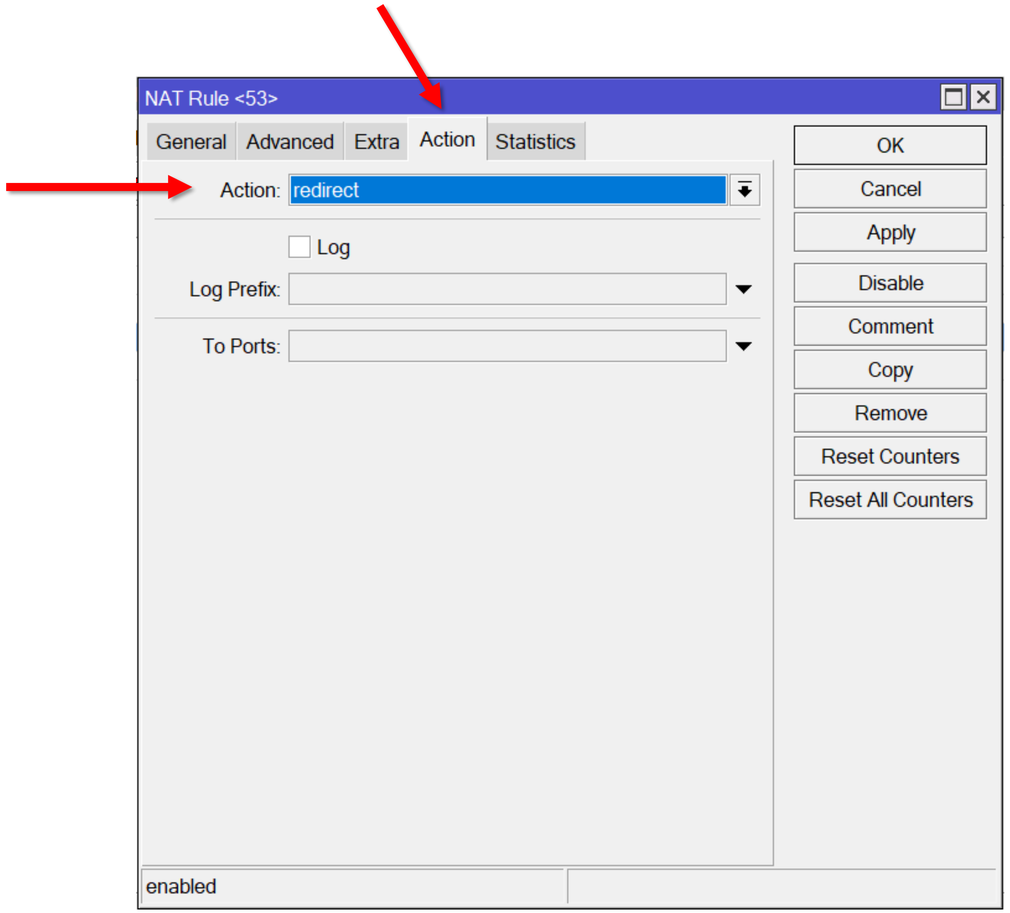


IP > Firewall > NAT > Add (+)

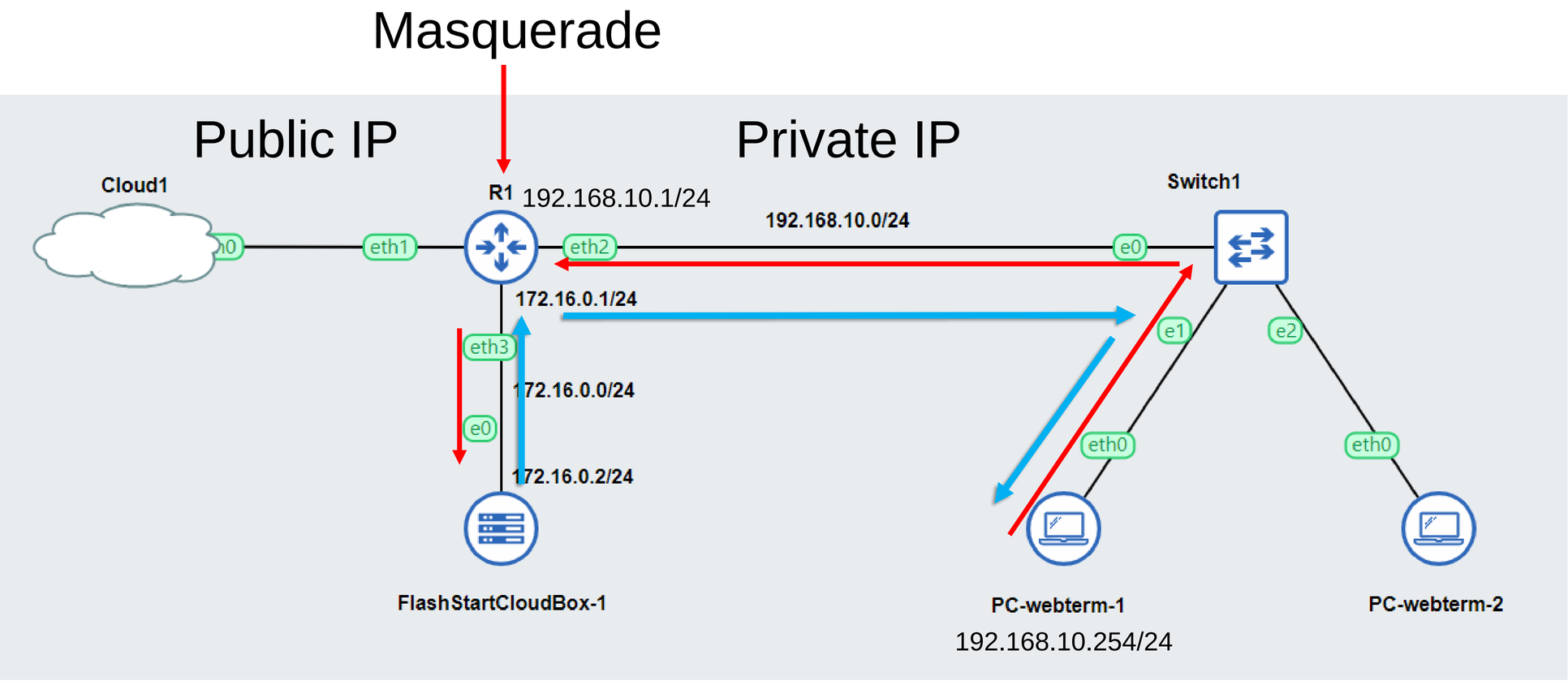
Redirect



IP > Firewall > NAT > Add (+)



CloudBOX


Masquerade
Public IP
Private IP
Cloud1
R1
192.168.10.1/24
eth1
eth2
192.168.10.0/24
e0
Switch1
172.16.0.1/24
eth3
e1
e2
172.16.0.0/24
e0
eth0
eth0
172.16.0.2/24
FlashStartCloudBox-1
PC-webterm-1
192.168.10.254/24
PC-webterm-2

CloudBOX

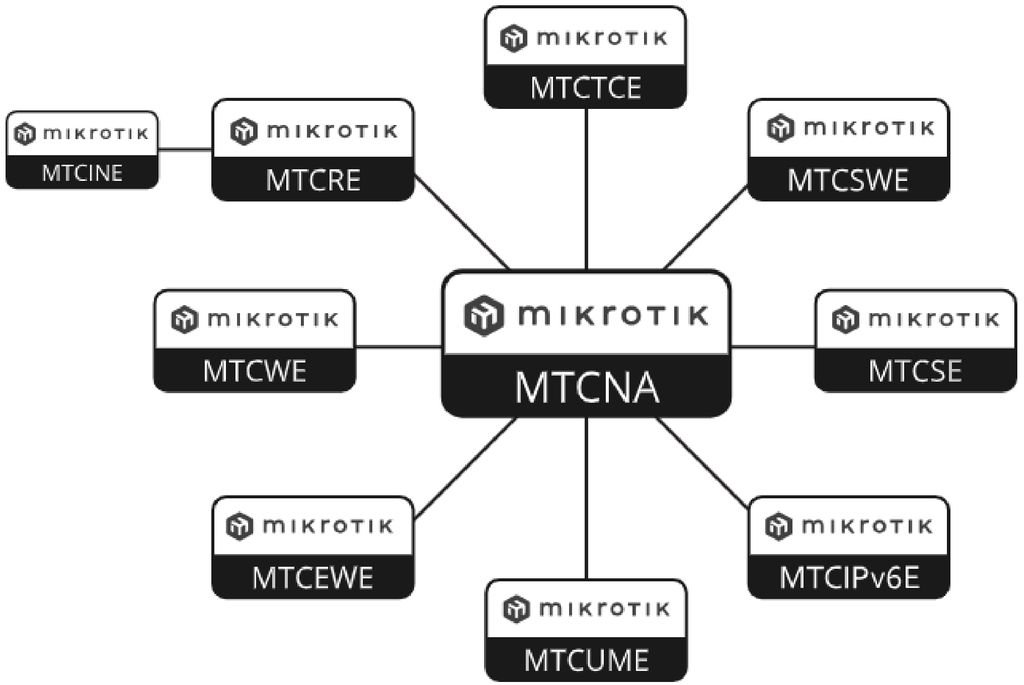
- Virtual Machine (VMWare, Proxmox, Hyper-V)
- Local DNS Cache
- Profili multipli
- Data export

MikroTik Training

Corsi MikroTik

- Corsi per nuove certificazioni
- Rinnovi di certificazione (anche online)
- https://corsimikrotik.it/contatti

SCAN ME



Q&A?

- Sito Web corsimikrotik.it
- YouTube https://youtube.com/corsimikrotik
- Canale telegram https://t.me/corsimikrotik