

FlashStart+MikroTik

Internet Protection with DNS Filtering

FlashStart®
INTERNET PROTECTION



About the Trainer

Marco Boschini

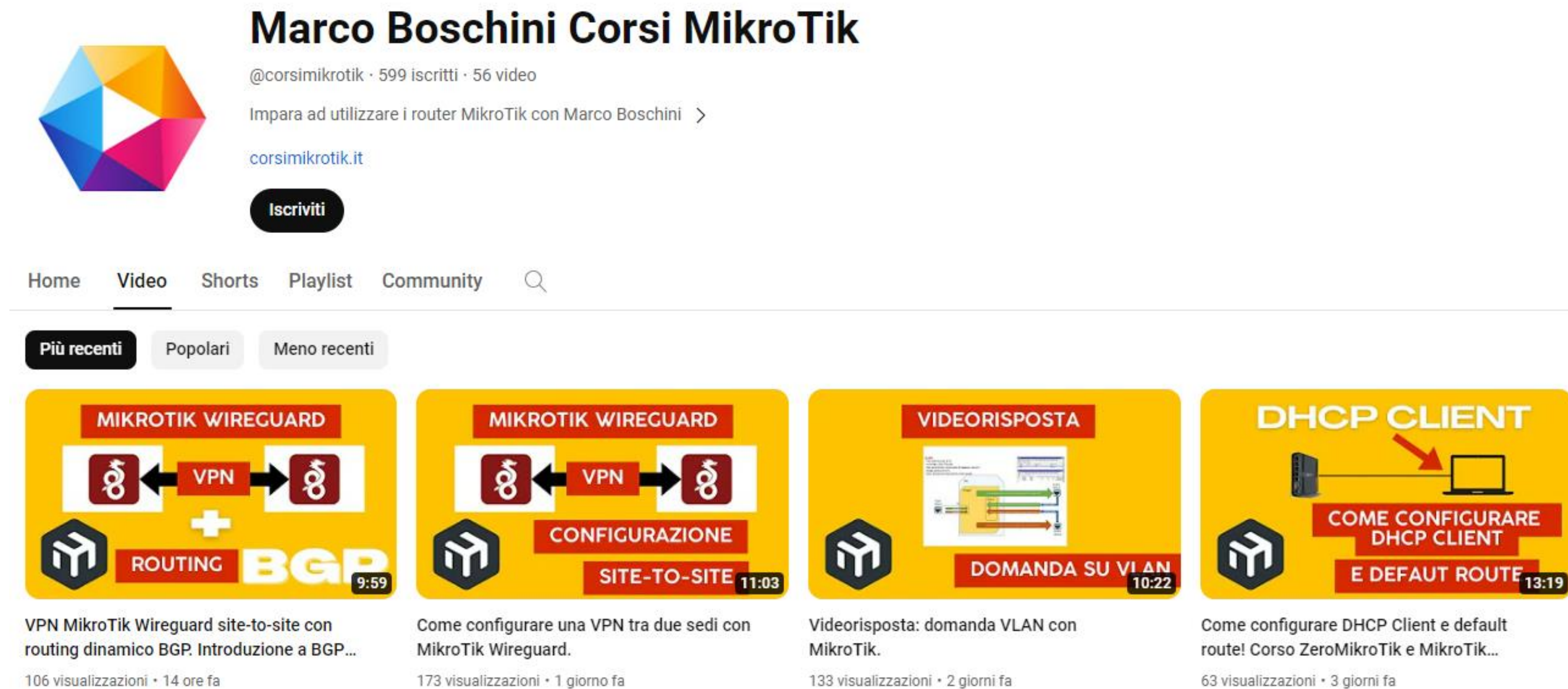
- MikroTik Certified Trainer
- MTCNA, MTCRE, MTCINE, MTCWE, MTCTCE, MTCUME, MTCIPv6, MTCSE, MTCWE, MTCEWE
- Founder [CorsiMikroTik.it](https://www.corsimikrotik.it)
-  marco@corsimikrotik.it
-  <https://www.linkedin.com/in/marco-boschini/>



YouTube

Marco Boschini Corsi MikroTik

<https://www.youtube.com/corsimikrotik>



The screenshot shows the YouTube channel page for Marco Boschini Corsi MikroTik. The channel name is "Marco Boschini Corsi MikroTik" with the handle "@corsimikrotik", 599 subscribers, and 56 videos. The bio states "Impara ad utilizzare i router MikroTik con Marco Boschini" and includes the website "corsimikrotik.it". There is an "Iscriviti" (Subscribe) button. The navigation tabs are Home, Video, Shorts, Playlist, and Community. The video filter is set to "Più recenti" (Most recent). Four video thumbnails are displayed:

- MIKROTIK WIREGUARD**: VPN MikroTik Wireguard site-to-site con routing dinamico BGP. Introduzione a BGP... (9:59, 106 visualizzazioni • 14 ore fa)
- MIKROTIK WIREGUARD**: Come configurare una VPN tra due sedi con MikroTik Wireguard. (11:03, 173 visualizzazioni • 1 giorno fa)
- VIDEORISPOSTA**: Videorisposta: domanda VLAN con MikroTik. (10:22, 133 visualizzazioni • 2 giorni fa)
- DHCP CLIENT**: Come configurare DHCP Client e default route! Corso ZeroMikroTik e MikroTik... (13:19, 63 visualizzazioni • 3 giorni fa)

Telegram

Corsi MikroTik

t.me/corsimikrotik



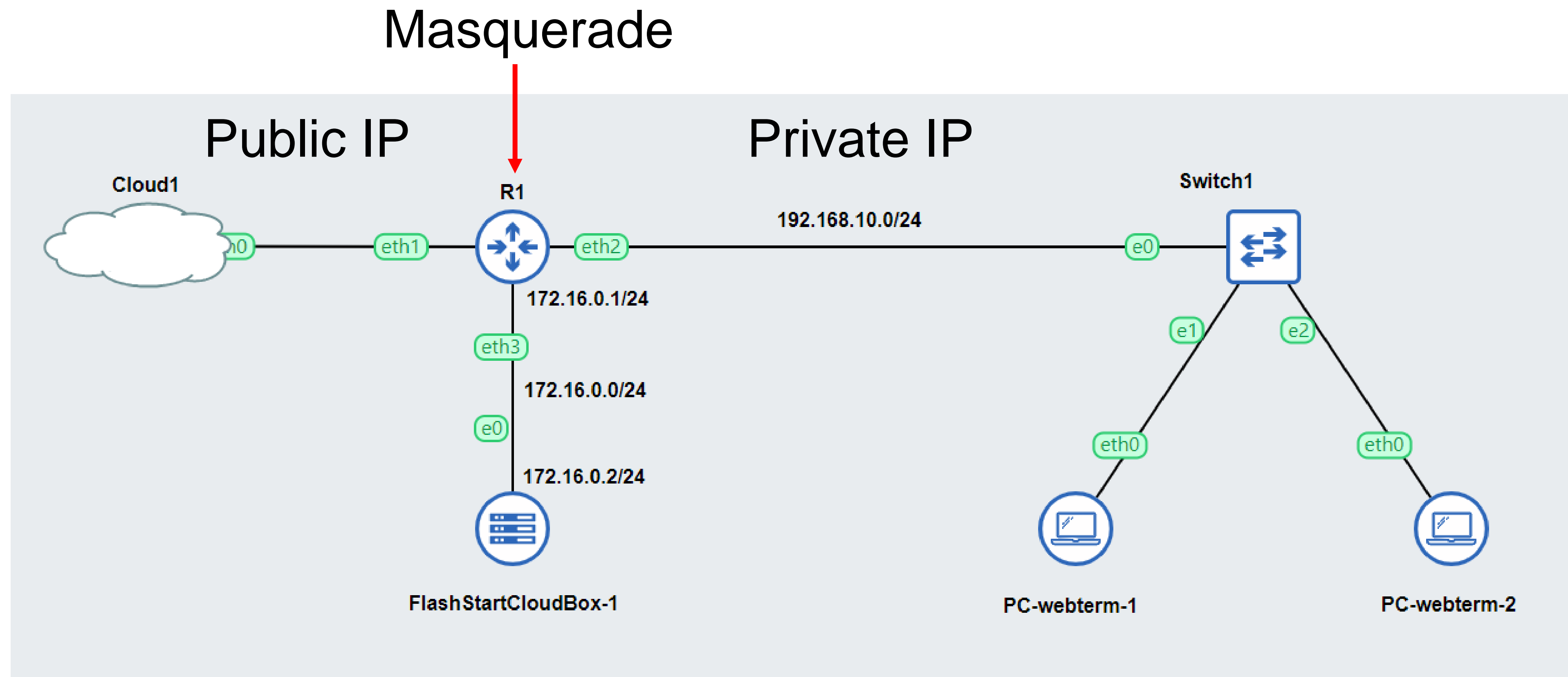
Canale Corsi MikroTik



Obiettivi

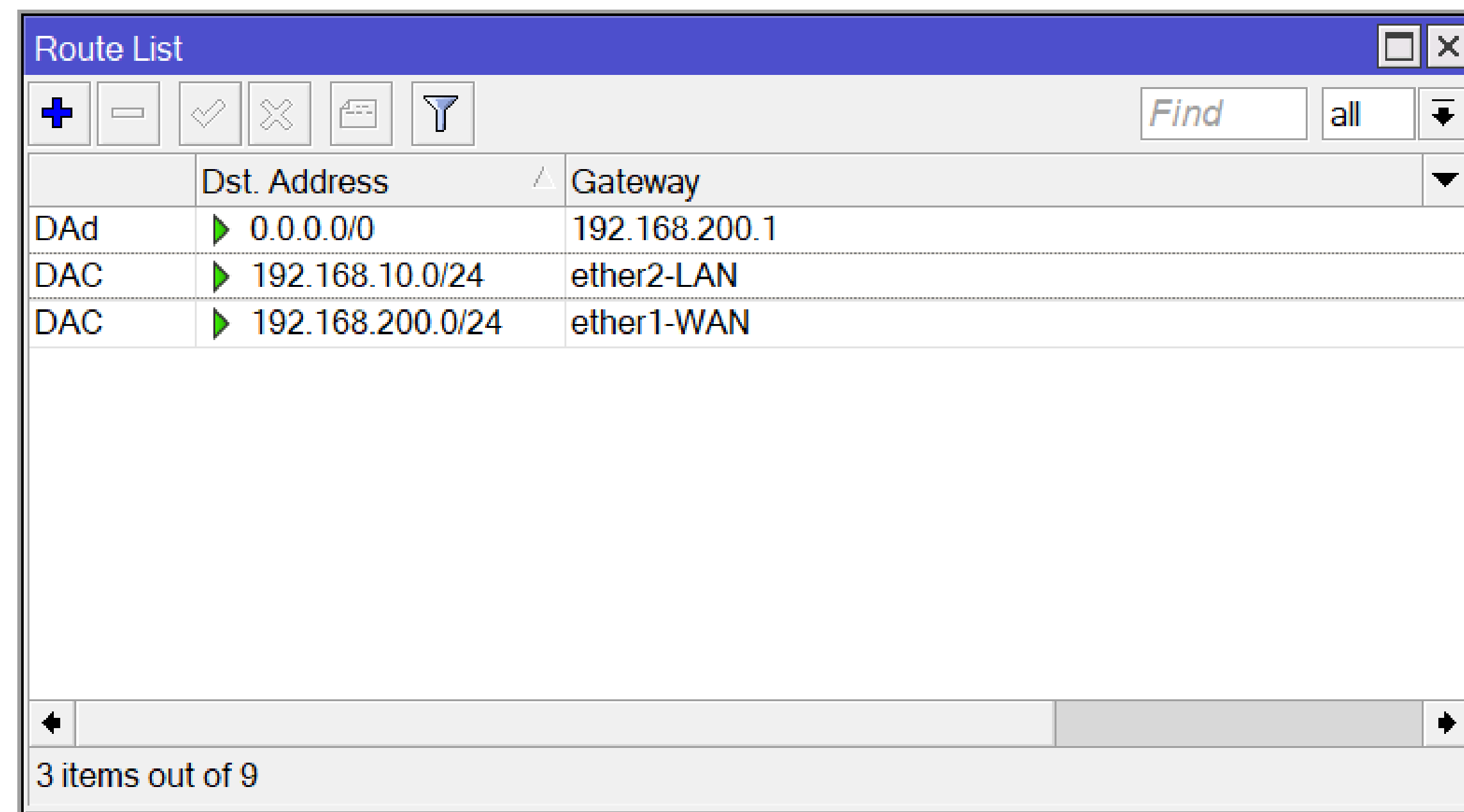
- Comprendere come funziona un router
- Comprendere come come un PC può comunicare con internet
- Comprendere a cosa serve il DNS
- Comprendere come funziona un DHCP Server
- Comprendere come catturare le richieste DNS dalla tua LAN

Come funziona un router



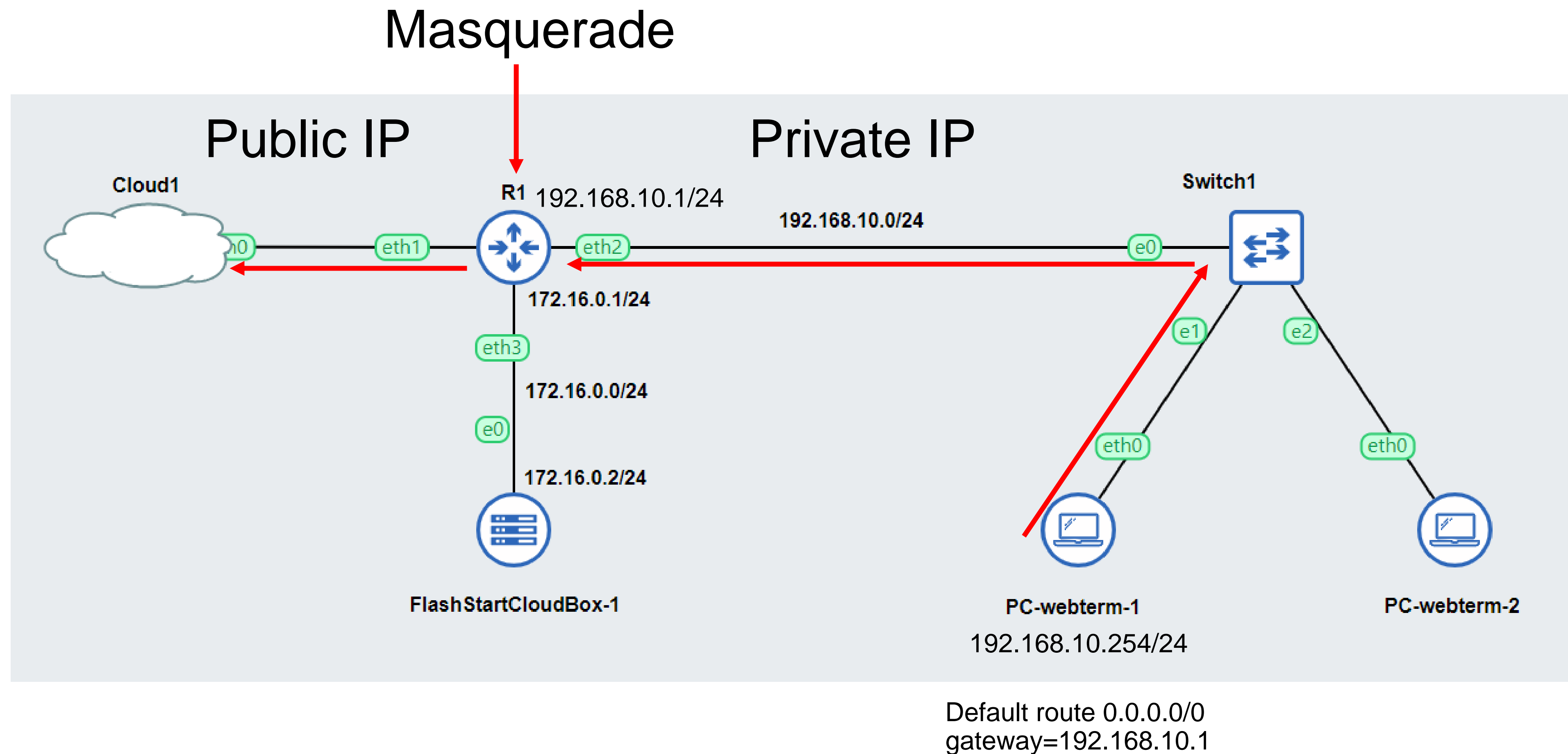
Routing

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

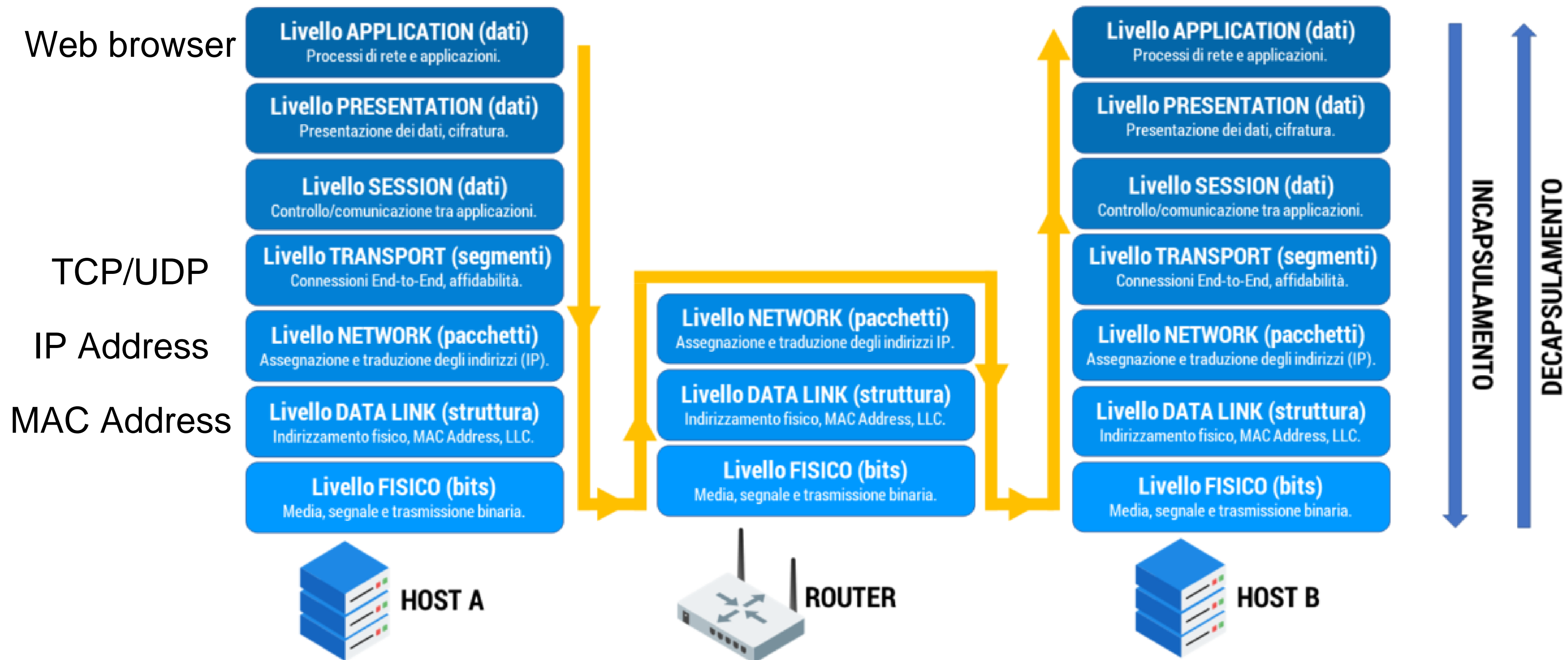


	Dst. Address	Gateway
DAd	0.0.0.0/0	192.168.200.1
DAC	192.168.10.0/24	ether2-LAN
DAC	192.168.200.0/24	ether1-WAN

Come comunica su internet un PC



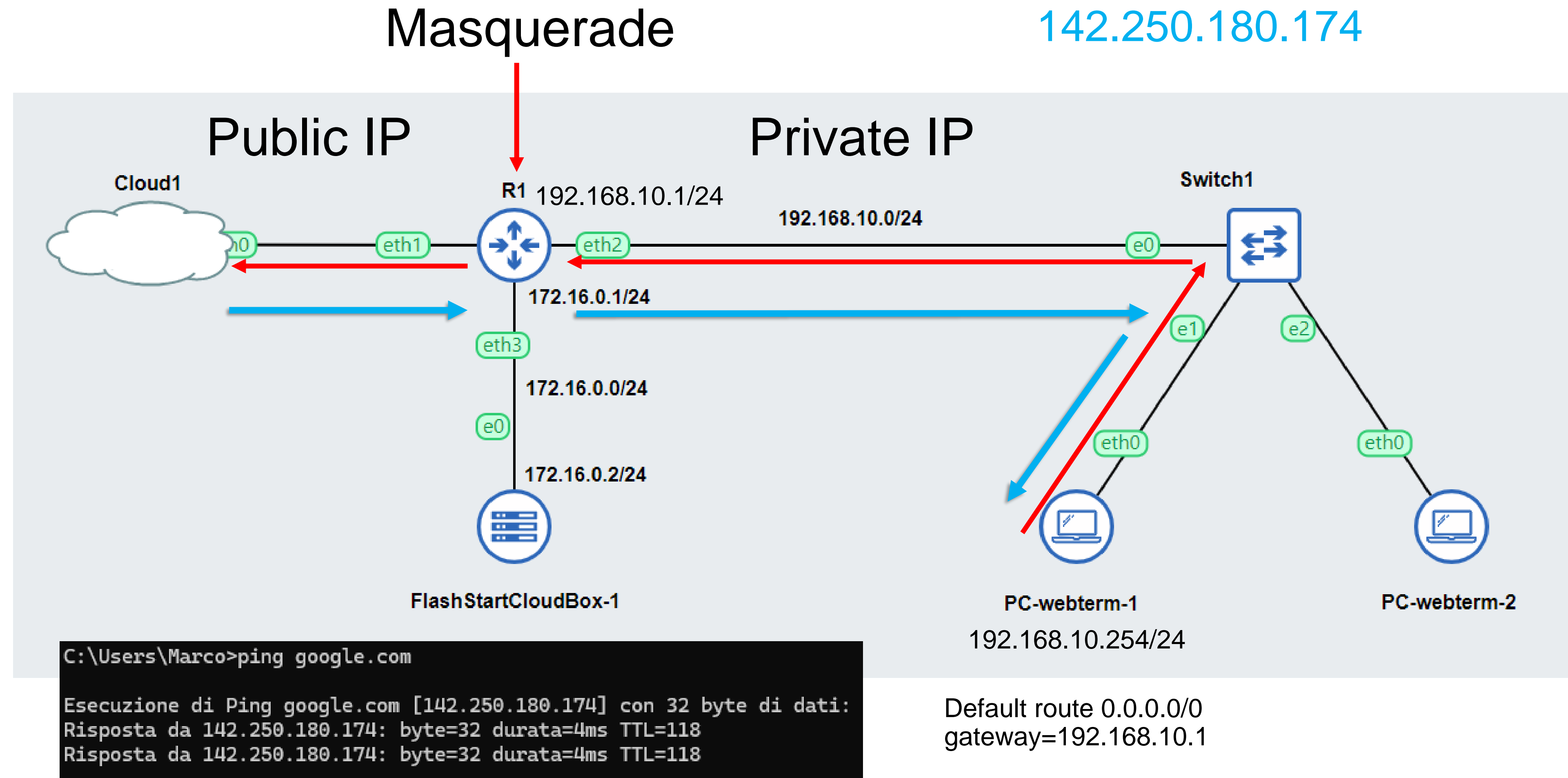
Routing



DNS

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

DNS: L'indirizzo IP è
142.250.180.174



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

The screenshot displays the Mikrotik WinBox DHCP configuration interface. At the top, a table lists the configured DHCP networks. Below this, two configuration windows are open. The 'DHCP Server <dhcp1>' window shows general settings such as Name (dhcp1), Interface (ether2-LAN), Lease Time (00:30:00), and Address Pool (dhcp_pool0). The 'DHCP Network <192.168.10.0/24>' window shows network-specific settings, including Address (192.168.10.0/24), Gateway (192.168.10.1), and DNS Servers (8.8.8.8). A red arrow points from the text on the right to the DNS Servers field in the network configuration window.

Address	Gateway	DNS Servers	Domain	WINS Servers	Next Server
192.168.10.0/24	192.168.10.1	8.8.8.8			

DHCP Server <dhcp1>

General

Name: dhcp1

Interface: ether2-LAN

Relay:

Lease Time: 00:30:00

Bootp Lease Time: forever

Address Pool: dhcp_pool0

DHCP Option Set:

Server Address:

Delay Threshold:

Authoritative: yes

Bootp Support: static

DHCP Network <192.168.10.0/24>

Address: 192.168.10.0/24

Gateway: 192.168.10.1

Netmask:

☐ No DNS

DNS Servers: 8.8.8.8

Domain:

WINS Servers:

NTP Servers:

CAPS Managers:

Next Server:

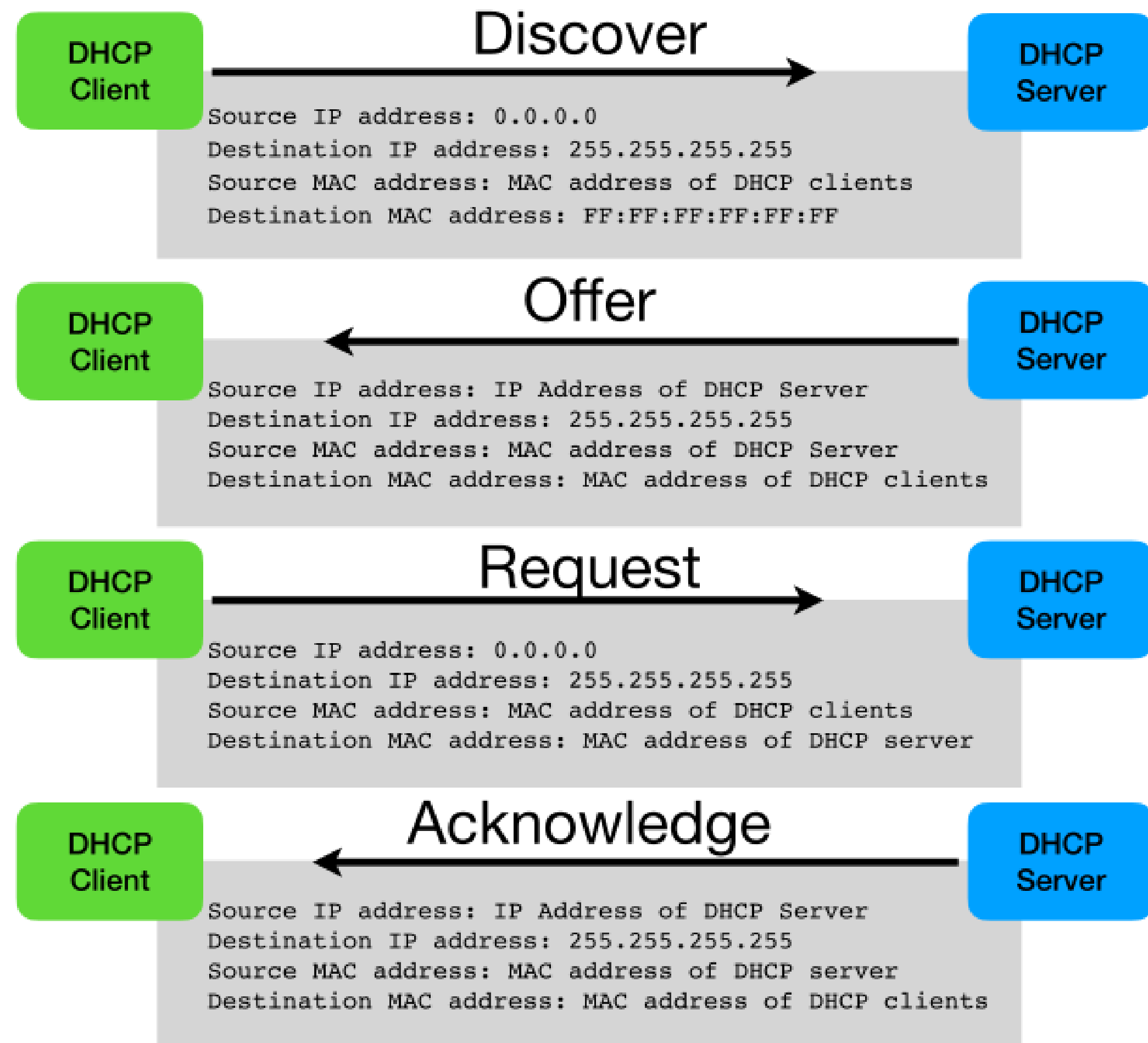
Boot File Name:

DHCP Options:

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

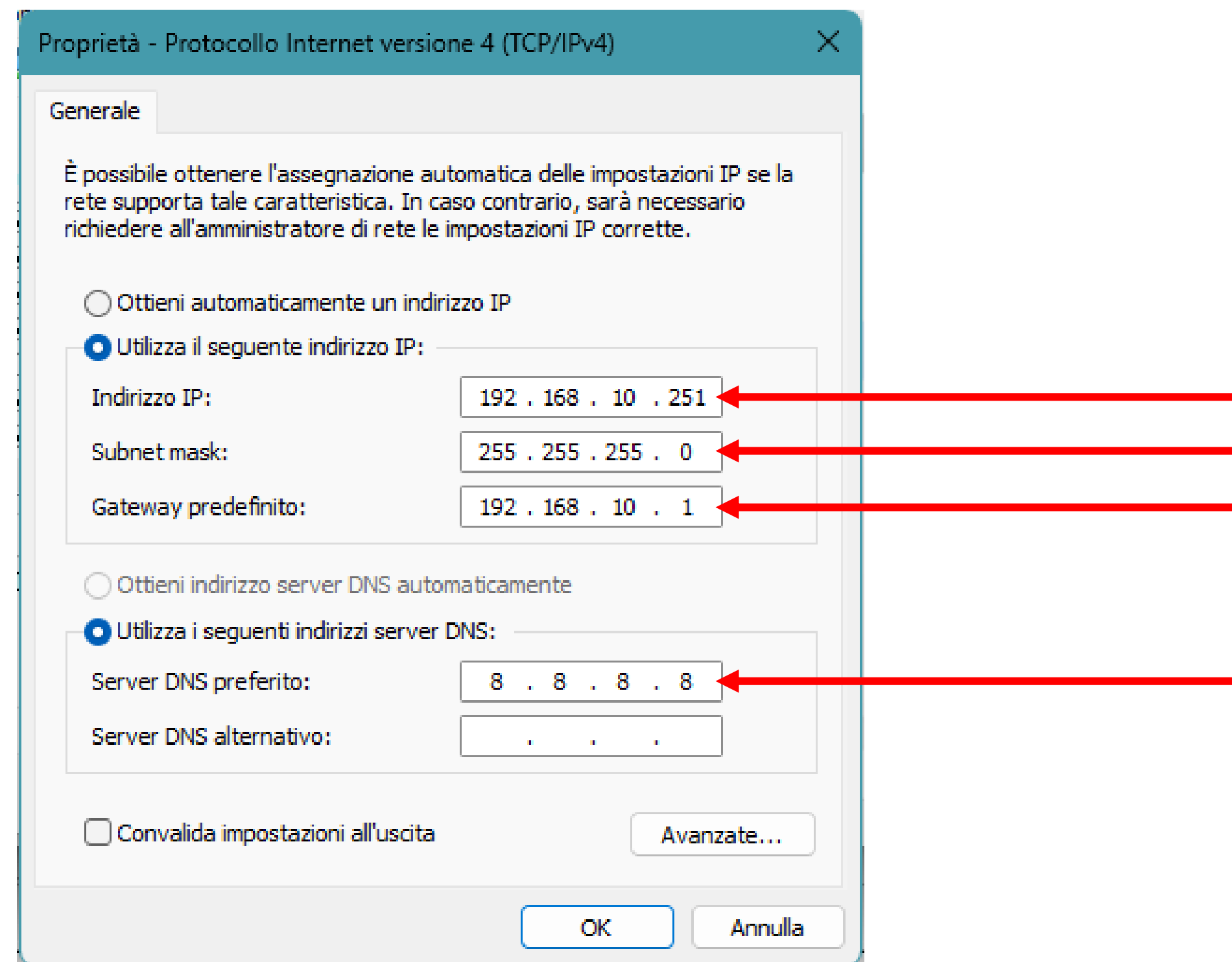
Come funziona il DHCP Server

- DORA Process
- Discover
- Offer
- Request
- Acknowledge



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 destinata ad un sito proibito o malevolo (non considerate sicuro o bloccato)

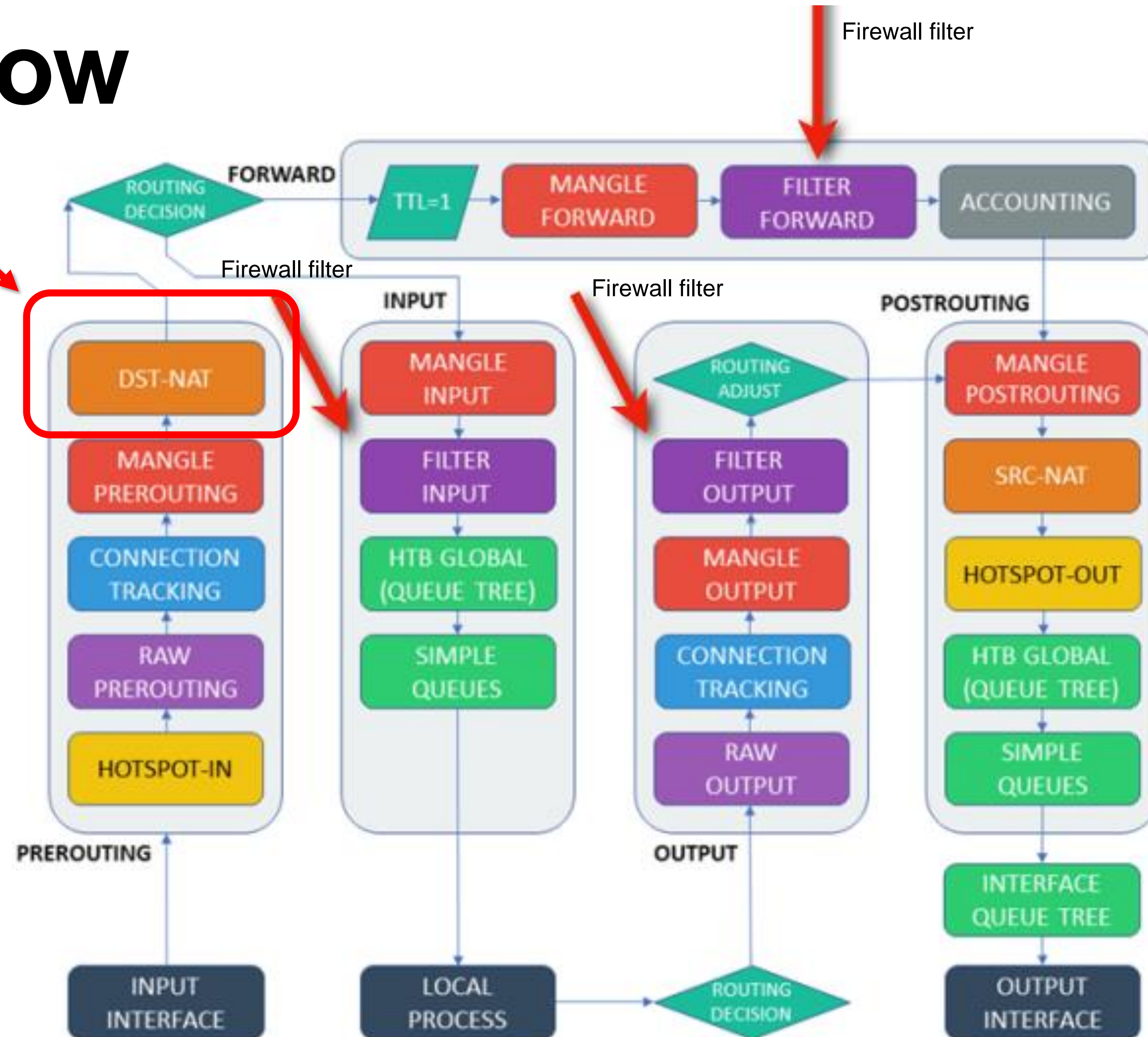
Packet Flow

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

The screenshot shows the 'NAT Rule <53>' window with the 'General' tab selected. Red arrows point to the following fields:

- Chain: dstnat
- Protocol: 17 (udp)
- Dst. Port: 53
- In. Interface: ether2-LAN

Other visible fields include Src. Address, Dst. Address, Src. Address List, Dst. Address List, Src. Port, Any. Port, Out. Interface, In. Interface List, Out. Interface List, Packet Mark, and Connection Mark. The status at the bottom is 'enabled'.

IP > Firewall > NAT > Add (+)

The screenshot shows the 'NAT Rule <53>' window with the 'Action' tab selected. Red arrows point to the following fields:

- Action: dst-nat
- To Addresses: 185.236.104.104
- To Ports: 53

Other visible fields include Log, Log Prefix, and buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. The status at the bottom is 'enabled'.

Come cambiare l'IP di destinazione di una richiesta DNS

The screenshot shows the 'NAT Rule <53>' configuration window with the 'General' tab selected. Red arrows point to the following fields:

- Chain: dstnat
- Protocol: 6 (tcp)
- Dst. Port: 53
- In. Interface: ether2-LAN

Other visible fields include Src. Address, Dst. Address, Src. Address List, Dst. Address List, Src. Port, Any. Port, Out. Interface, In. Interface List, Out. Interface List, Packet Mark, and Connection Mark. The status at the bottom is 'enabled'.

IP > Firewall > NAT > Add (+)

The screenshot shows the 'NAT Rule <53>' configuration window with the 'Action' tab selected. Red arrows point to the following fields:

- Action: dst-nat
- To Addresses: 185.236.104.104
- To Ports: 53

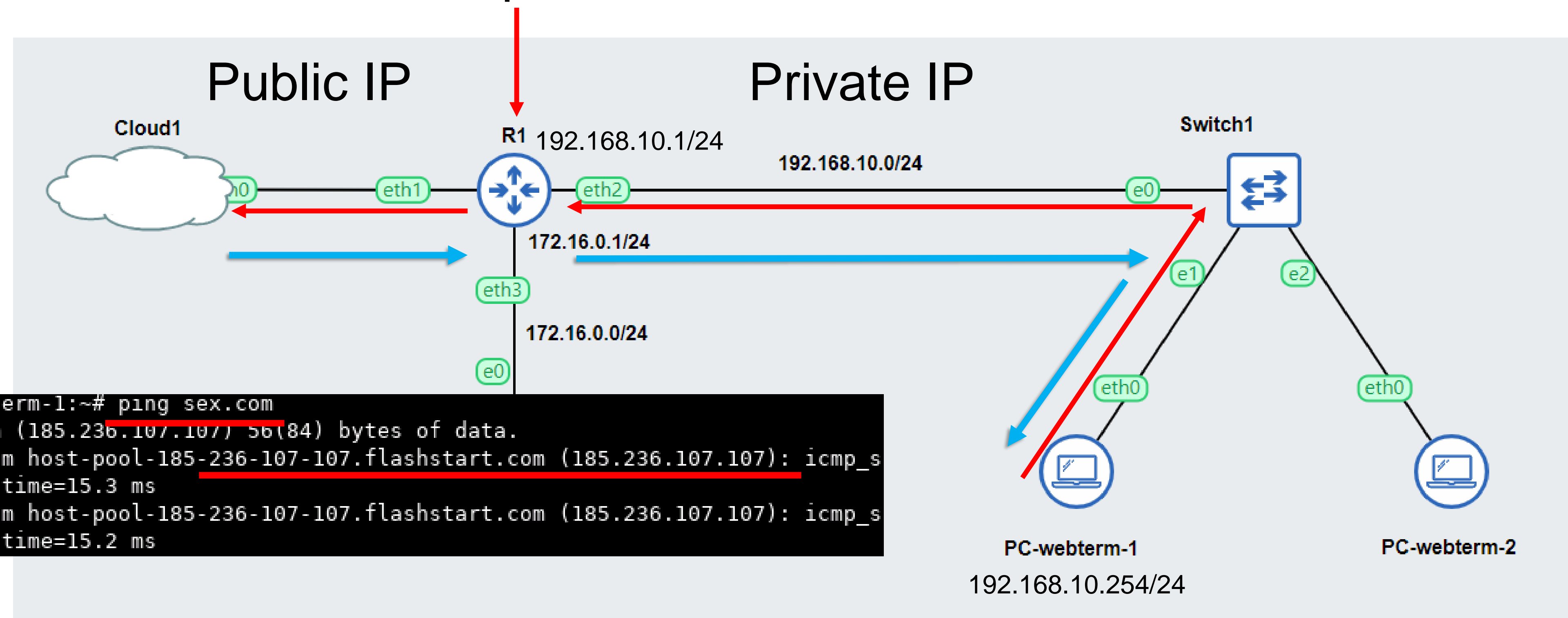
Other visible fields include Log, Log Prefix, and the status at the bottom is 'enabled'.

FlashStart

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

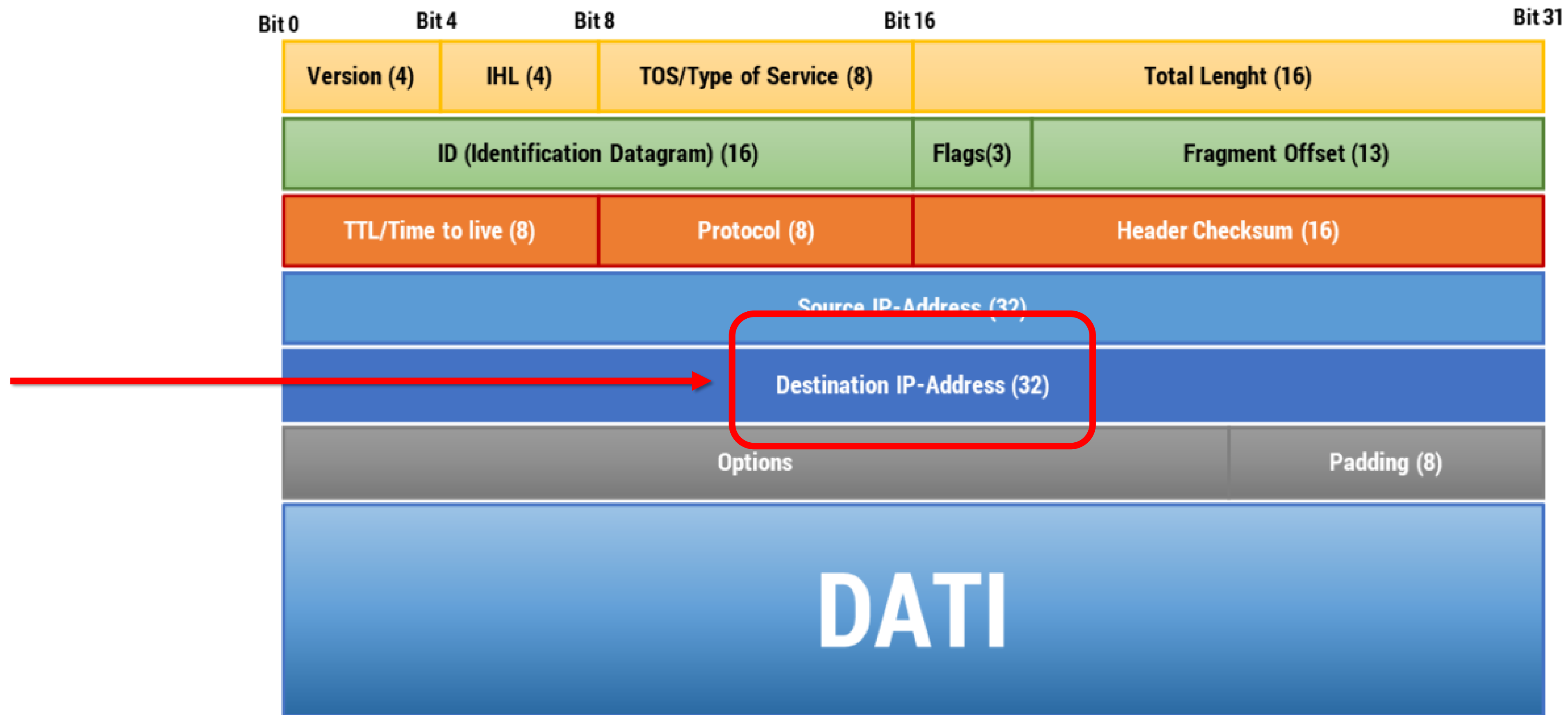
FlashStart: l'indirizzo IP è
185.236.107.107 (FlashStart)

Masquerade



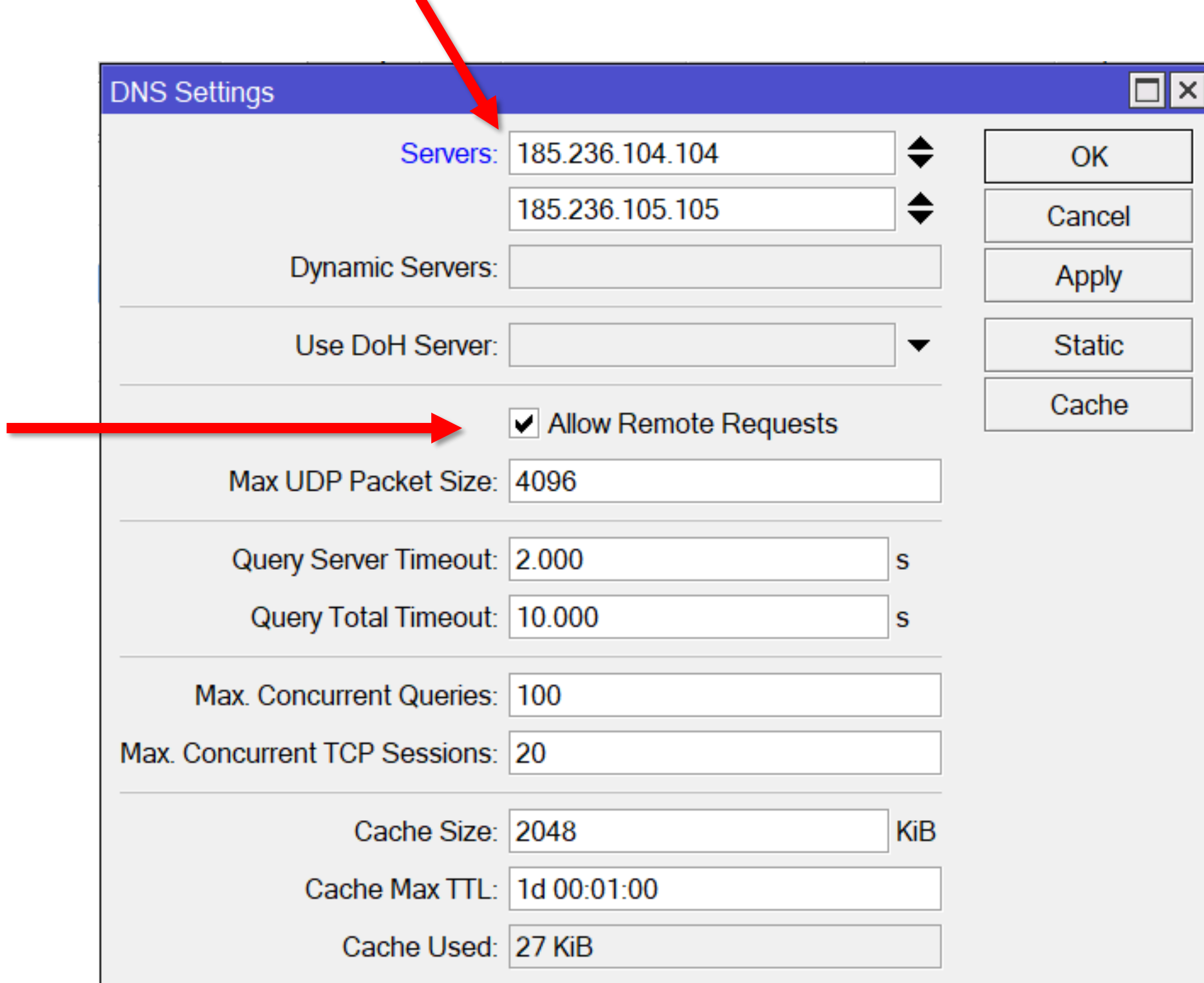
Default route 0.0.0.0/0
gateway=192.168.10.1

IP Packet



MikroTik DNS Relay

- Puoi usare un router MikroTik come DNS Relay
- RouterOS richiede al server DNS la 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)



DNS Settings

Servers: 185.236.104.104
185.236.105.105

Dynamic Servers:

Use DoH Server:

☒ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 1d 00:01:00

Cache Used: 27 KiB

OK
Cancel
Apply
Static
Cache

IP > DNS

Redirect

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

Redirect

NAT Rule <53>

General Advanced Extra Action Statistics

Chain: **dstnat**

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol: ☐ 17 (udp)

Src. Port:

Dst. Port: ☐ 53

Any. Port:

In. Interface: ☐ ether2-LAN

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

IP > Firewall > NAT > Add (+)

NAT Rule <53>

General Advanced Extra Action Statistics

Action: **redirect**

☐ Log

Log Prefix:

To Ports:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

Redirect

NAT Rule <53>

General Advanced Extra Action Statistics

Chain: **dstnat**

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 53

Any. Port:

In. Interface: ☐ ether2-LAN

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

IP > Firewall > NAT > Add (+)

NAT Rule <53>

General Advanced Extra Action Statistics

Action: **redirect**

☐ Log

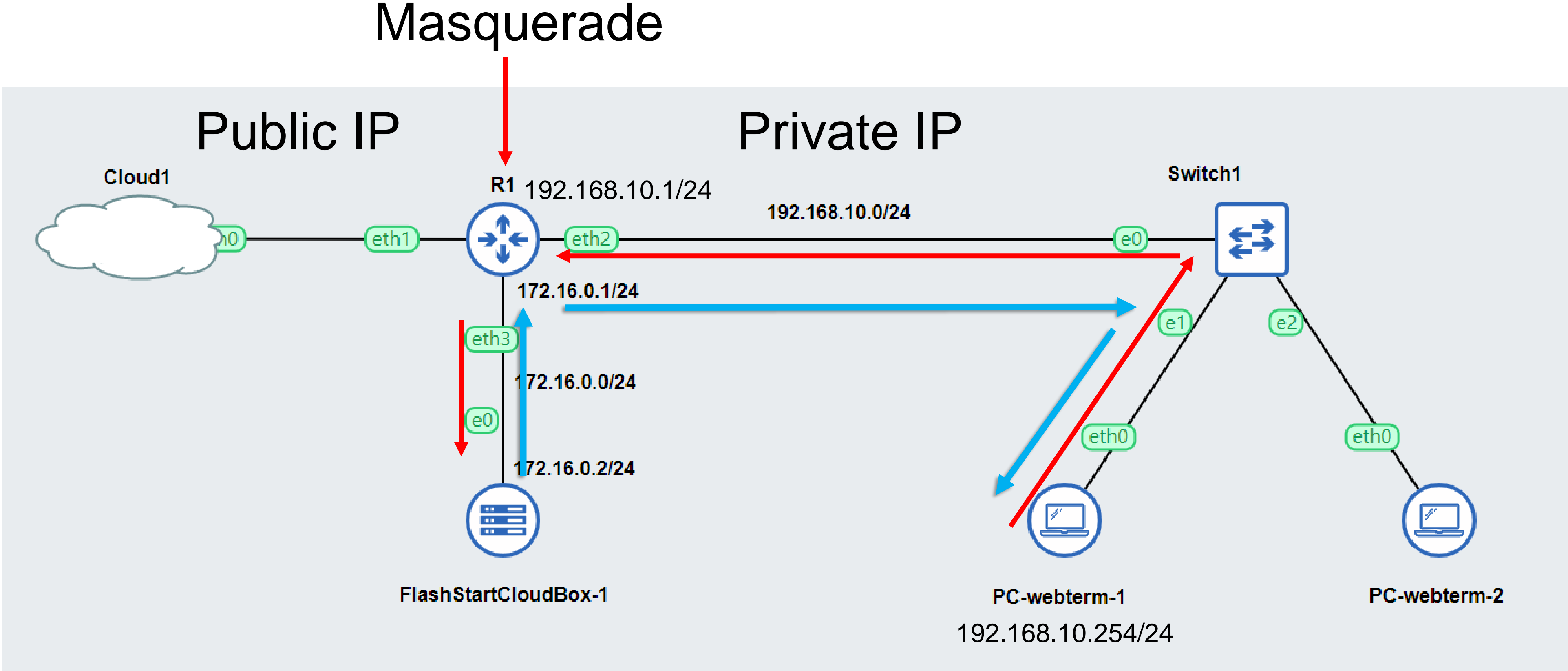
Log Prefix:

To Ports:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

CloudBOX



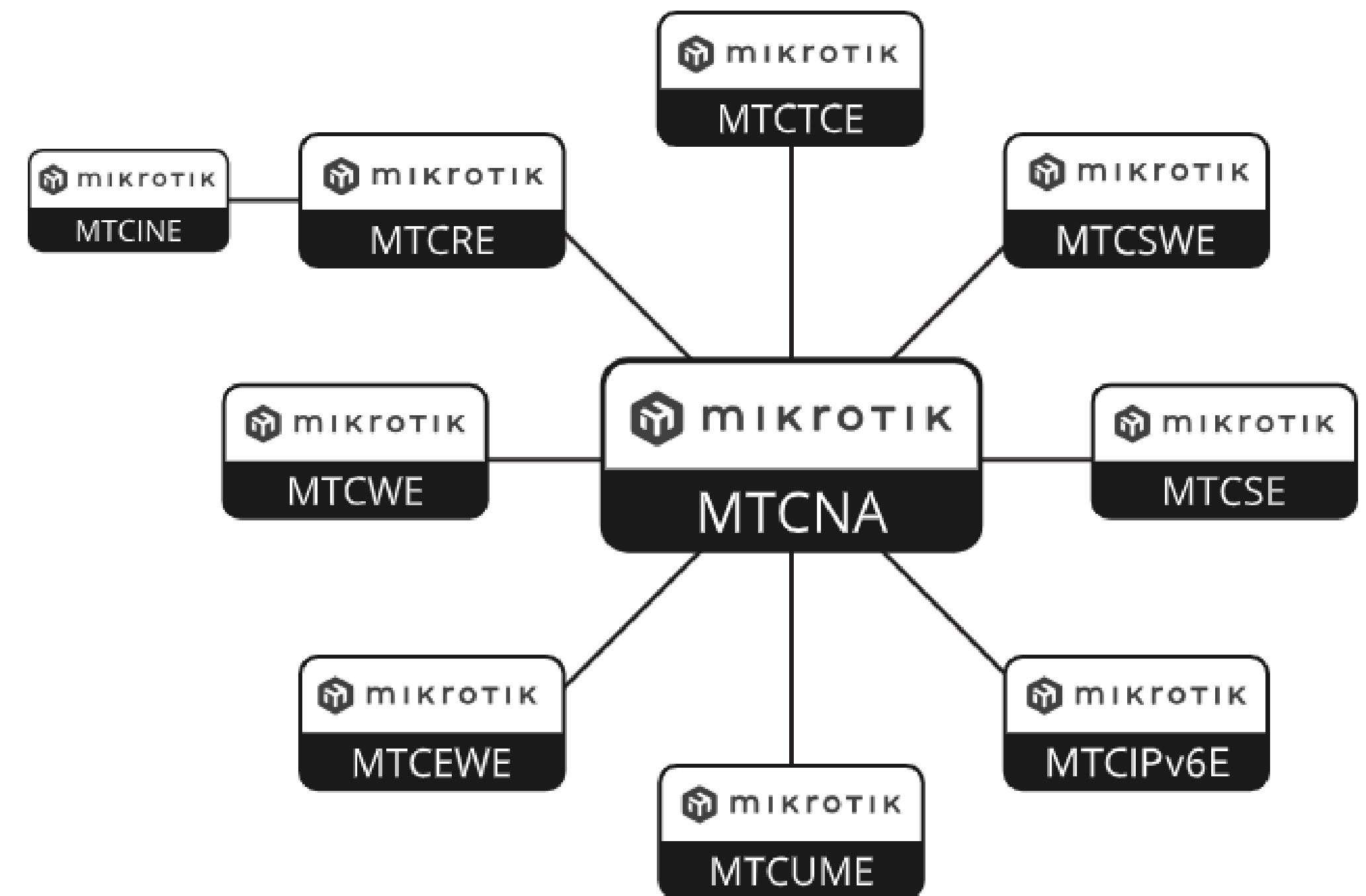
CloudBOX

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

MikroTik Training



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



Q&A?

- Sito Web corsimikrotik.it
- YouTube <https://youtube.com/corsimikrotik>
- [Canale telegram https://t.me/corsimikrotik](https://t.me/corsimikrotik)