IPv6-ONLY NETWORK A REAL CASE SCENARIO

timenet
connessi sicuri soddisfatti

Elia Aielli

ITNOG8 - Bologna - 7 Maggio 2024

Introduzione

Elia Aielli

Ingegnere delle Telecomunicazioni - Sicurezza nelle reti - Unipi
NOC Support Engineer
Network Engineer presso Timenet SpA

Motivazioni

Divulgazione IPv6
Sperimentazione con OpenWRT
Preparazione per il futuro
Divertimento a casa

Che cos’è OpenWRT?

OpenWrt®
WIRELESS FREEDOM

www.openwrt.org

Il progetto

- Linux OS per dispositivi embedded
- Open Source
- Performance e stabilità
- Sicurezza
- Community
- Licenza GPL, costo 0

Cambio firmware

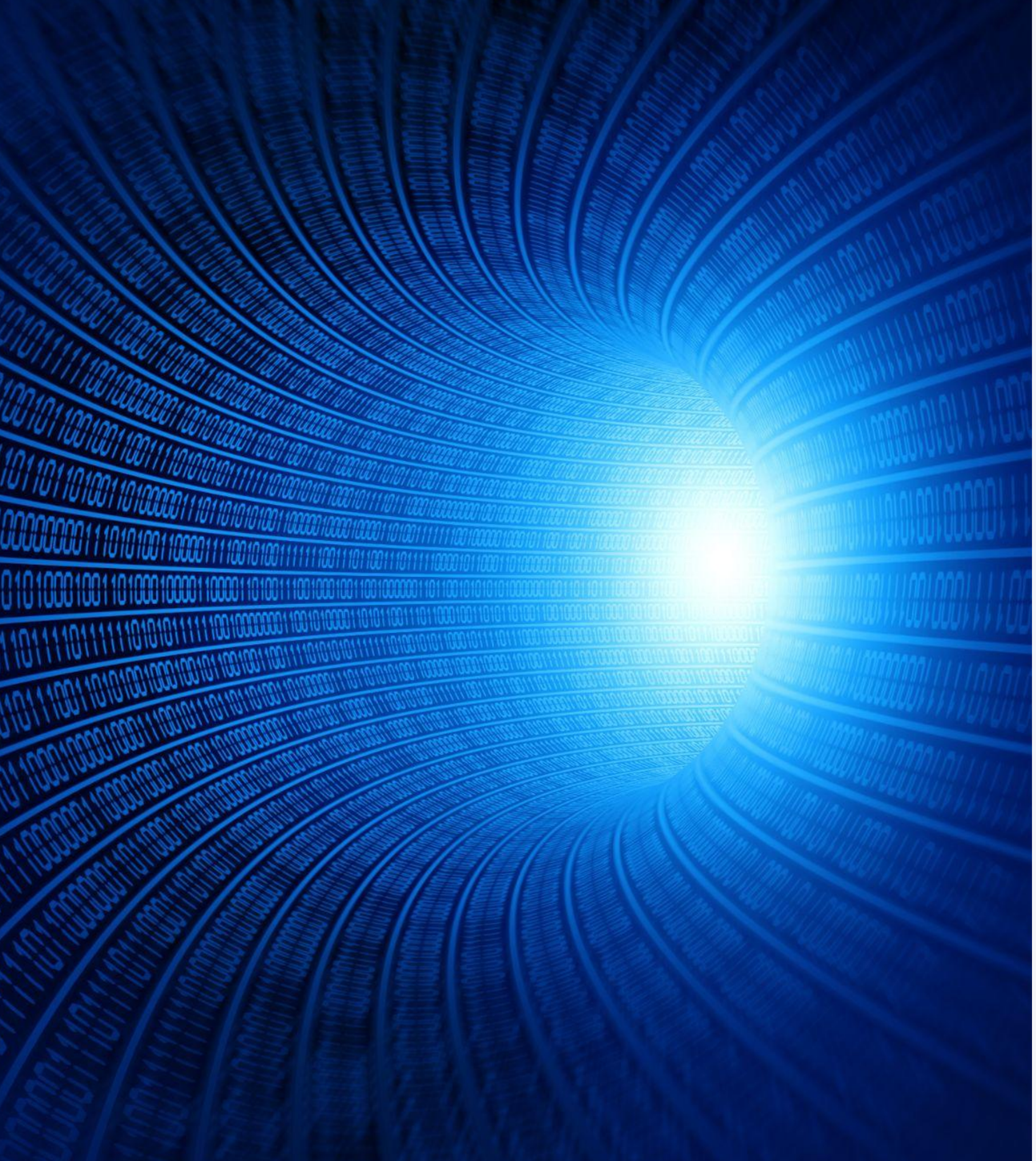
- Download firmware dal sito
- Web GUI OEM firmware
- Bootloader e porta Ethernet
- Bootloader e porta Seriale
- Via JTAG
- Procedure di recovery

Dispositivi compatibili

- https://openwrt.org/toh/start
- Asus, Netgear, Ubiquiti, etc
- x86 hardware PC / VM / server

Funzionalità

- Firewall
- VPN
- PBX (sip)
- AP
- Switch
- e molto altro



IPv6, come procurarmelo?

Tunnelbroker

Hurricane Electric fornisce un servizio di tunnel v6-in-v4 gratuito
E’ sufficiente registrarsi su https://tunnelbroker.net/
39 locations dove terminare il tunnel

Tunnel v6-in-v4

Tunnel stabilito tra due endpoint che comunicano solo in IPv4
All’interno passerà traffico IPv6
CPE riceve in DHCPv6-PD una /48 IPv6

Prefix Delegation

Via DHCPv6 i BNG di HE forniscono un prefix fino a /48 alla CPE
La CPE assegna gli IPv6 delegati ai dispositivi in LAN
A sua volta la CPE può delegare in downstream prefix variabili
Possibile segmentare in più /64 la propria rete
Raccomandazione RIPE per Aziende: /48, Privati /56

Update dinamico endpoint

Dyn-compliant endpoint updates
Tramite username, password e tunnel ID aggiornamento automatico dell’ip pubblico della CPE, lato HE

IPv6, come implementarlo

Dual Stack

- Presenza di doppio IP, v4 e v6 sulle NIC
- Happy Eyeballs, algoritmo IETF per minimizzare i tempi di connessione dual stack
- Check contemporaneo della raggiungibilità v4 e v6 (preferenziale)
- Nasconde problemi ipv6 all'end user
- App dependant (es. chrome, opera, OS X, FreeBDS, etc)
- Non riduce utilizzo IPv4
- 2 protocolli, scenari non prevedibili, tshoot difficile

IPv6-Mostly

- Client indicano la capacità di utilizzare IPv6-only (DHCP opt 108)
- Server check se la rete supporta IPv6-only
- Se entrambe le condizioni sono realizzate, assegna al client un IPv6 e basta e stoppa il DHCPv4 per X min
- Se una delle due fallisce, viene associato solo un IPv4

IPv6-Only

- Studio della situazione meno elastica
- Cosa si rompe?
- Nuova VLAN con SSID dedicato
- Necessita di altre componenti per raggiungere internet v4-Only

Scenario

IPv6-only

Con questa configurazione la LAN6 è IPv6-only

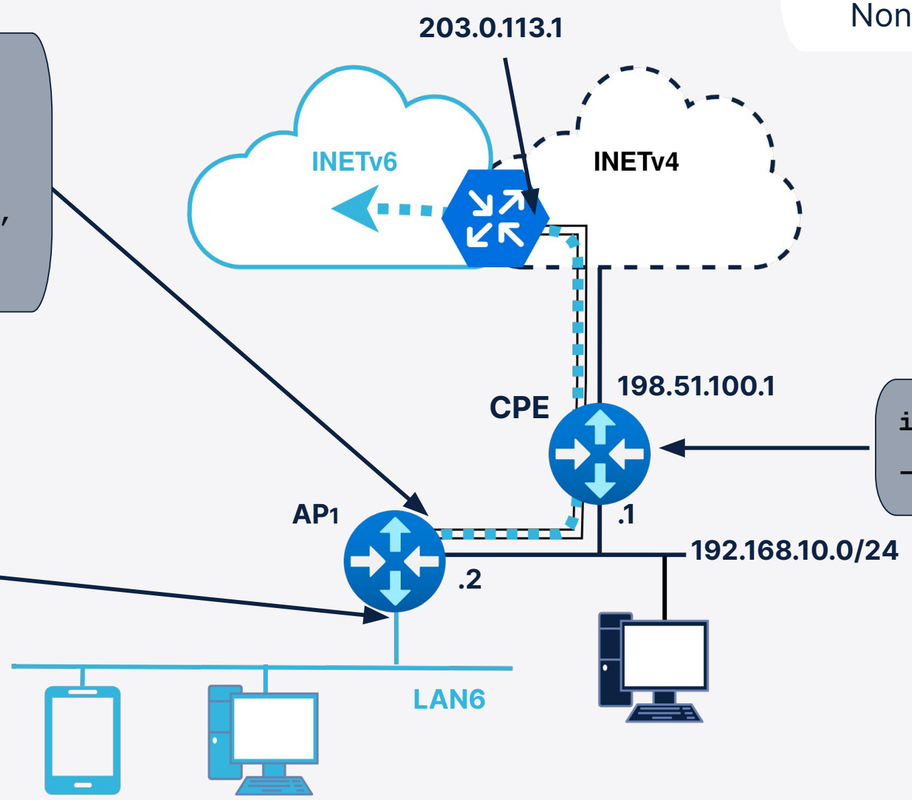
Non ho la possibilità di raggiungere le risorse IPv4-only

DHCPv6

```
interface 'henet'
    option proto '6in4'
    option peeraddr '203.0.113.1'
    option ip6add '2001:db8:0:f00::2/64'
    [...]
```

SLAAC

```
interface 'lan6'
    option proto 'static'
    option ip6assign '60'
    option ip6hint '60'
    [...]
```




```
iptables -t nat -A PREROUTING -p 41
-d 198.51.100.1 -j DNAT --to 192.168.10.2
```

v4-only

v6-only

6-in-4 tunnel

WAN Sfrutto DHCPv6 per la Prefix Delegation

LAN6 Utilizzo SLAAC per assegnare gli IPv6 agli host. Dinamico, leggero e supportato da tutti gli OS (Android non supporta DHCPv6)

DNS, cosa utilizziamo?

DHCPv6

-Il router AP1 utilizzerà come DNS quelli forniti via DHCPv6 dal Tunnel Broker
-I dispositivi in LAN invece faranno appoggio su AP1

Risoluzione DNS

-I DNS forniti dal Tunnel Broker saranno IPv6
-Risponderanno sia con record IPv4 che con record IPv6

dig www.facebook.com
star-mini.c10r.facebook.com.
AAAA 2a03:2880:f150:82:face:b00c:0:25de
A 157.240.210.35

-Compliant con Happy Eyeballs

IPv6 Checklist

IP Assegnato

```
IPv6 - 2001:db8:0:f00:a21c:c4ff:fecf:4ed0/64
IPv6 privacy extension - 2001:db8:0:f00:f164:c653:38a6:4764/64
IPv6 link local - fe80::a21c:c4ff:fecf:4ed0/64
```

Query DNS

```
root@AP1:~# dig AAAA ipv6.google.com +short
ipv6.l.google.com.
2a00:1450:4002:416::200e
```

Ping

```
root@AP1:~# ping 2a00:1450:4002:416::200e
64 bytes from 2a00:1450:4002:416::200e: seq=0 ttl=119 time=106 ms
```

Traceroute

```
root@AP1:~# traceroute 2a00:1450:4002:416::200e
1  tunnel234567.tunnel.tservxx.zrh1.ipv6.he.net (2001:db8:0:f00::1)
2  fqdn.corex.zrh3.he.net (2001:db8:0:f01::1)
[...]
9  mil07s19-in-x0e.1e100.net (2a00:1450:4002:416::200e)
```

Come raggiungo le risorse v4 only?

64:ff9b::/96 il prefisso chiave

-Mappa tra il mondo IPv4 ed il mondo IPv6
-Prefix (96bit) + IPv4 (32bit) = IPv6 (128bit)

NAT64

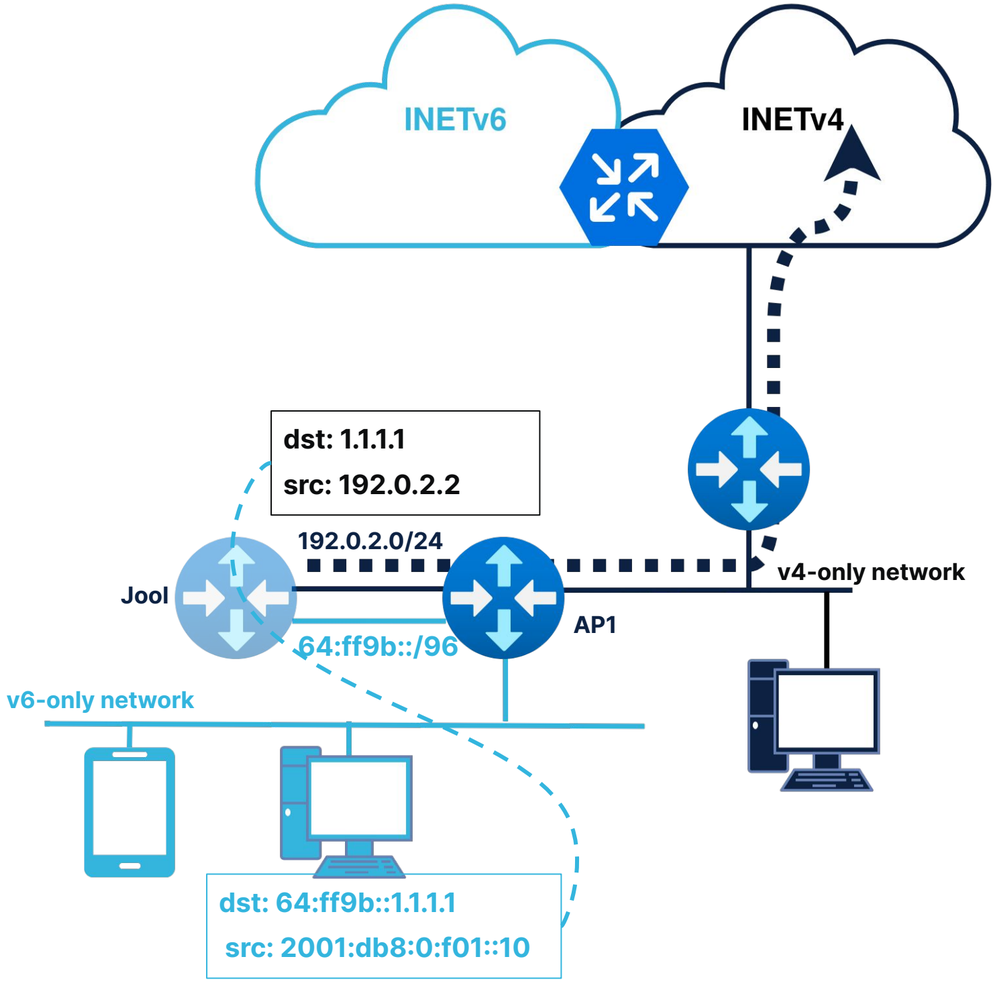
-Il prefisso 64:ff9b::/96 serve per assegnare una corrispondenza 1:1 - IPv6:IPv4
-Quando al gateway arriva un pacchetto con destinazione 64:ff9b::/96 viene ruotato verso il translator

La mia applicazione

-Utilizzo il demone Linux Jool per fare NAT64 su AP1
-Package aggiuntivo pronto per OpenWRT
-Pacchetti presi in PREROUTING e passati in POSTROUTING
-Bypass completo della catena FILTER

Network Namespace

-Idea di Ondřej Caletka
-Confino il demone Jool all'interno di un network namespace a sè
-Instrado il traffico destinato al prefisso 64:ff9b::/96, tramite una rotta statica, al namespace Jool
-Jool traduce da v6 a v4 e rimanda il pacchetto al default ns, correttamente filtrabile dal nostro firewall



Come utilizzare il prefisso 64:ff9b?

Soluzione 1: DNS64

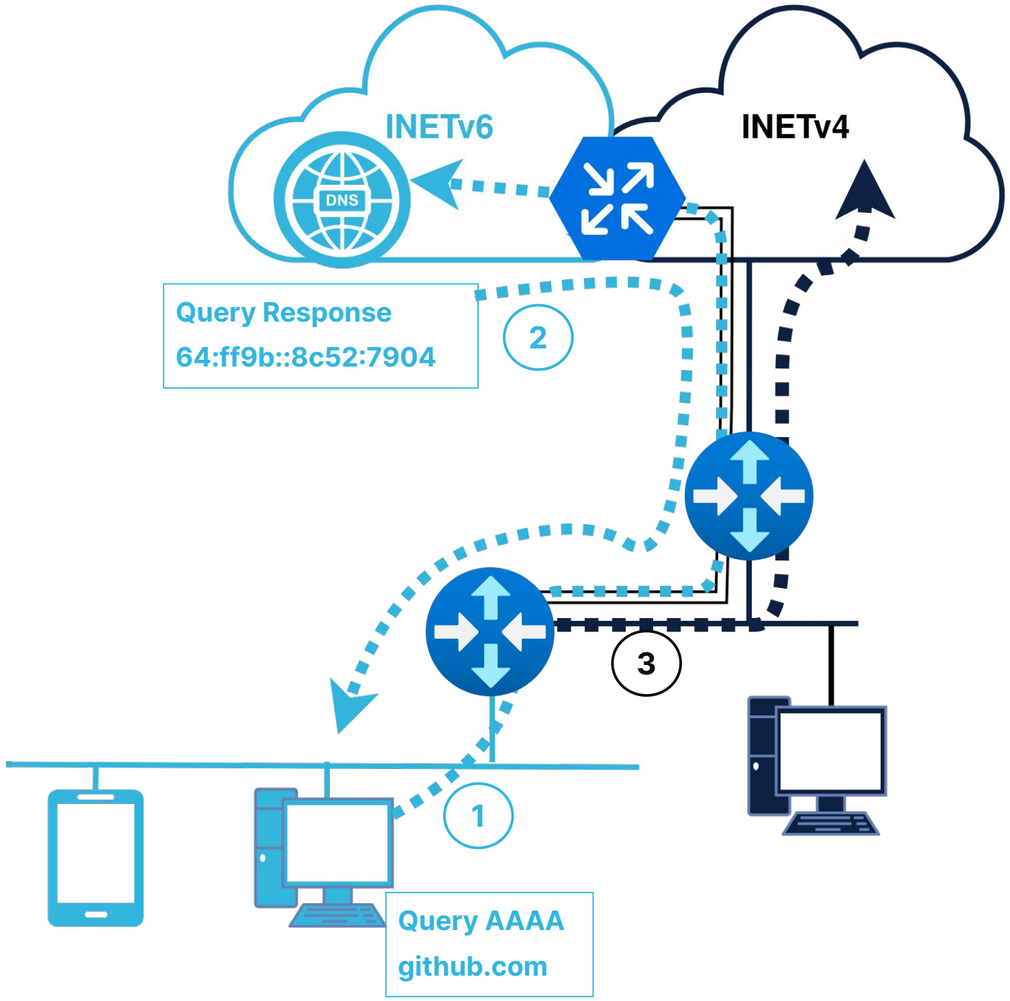
-Alcuni resolver pubblici rispondono in autonomia con il prefisso 64:ff9b::/96 come risposta alle query di tipo AAAA per fqdn v4-only
-Cloudflare e google sono i due maggiori esempi

Upstream DNS

-Oltre ai DNS64 pubblici segnalati, potete utilizzare anche altre opzioni
-OpenWRT stesso per avere anche entry statiche
-Pi-Hole per blocco ADV, con upstream i DNS64 di Google o CF da soli
-DNS Proxy per traduzione automatica degli IP delle maggiori CDN con IPv6 GUA, evitando NAT64. es. https://gitlab.com/miyurusankalpa/IPv6-dns-server

Limitazioni

-IPv4 literals
-DNSSEC
-Legacy ipv4 API



HEX 8C52:7904 = DEC 140.82.121.4

Come utilizzare il prefisso 64:ff9b?

Soluzione 2: 464xLAT

-Transition mechanism per IPv6
-Traduce da v4 a v6 quindi di nuovo a v4
-Composto dalla parte CLAT e dall'opzione PREF64

CLAT

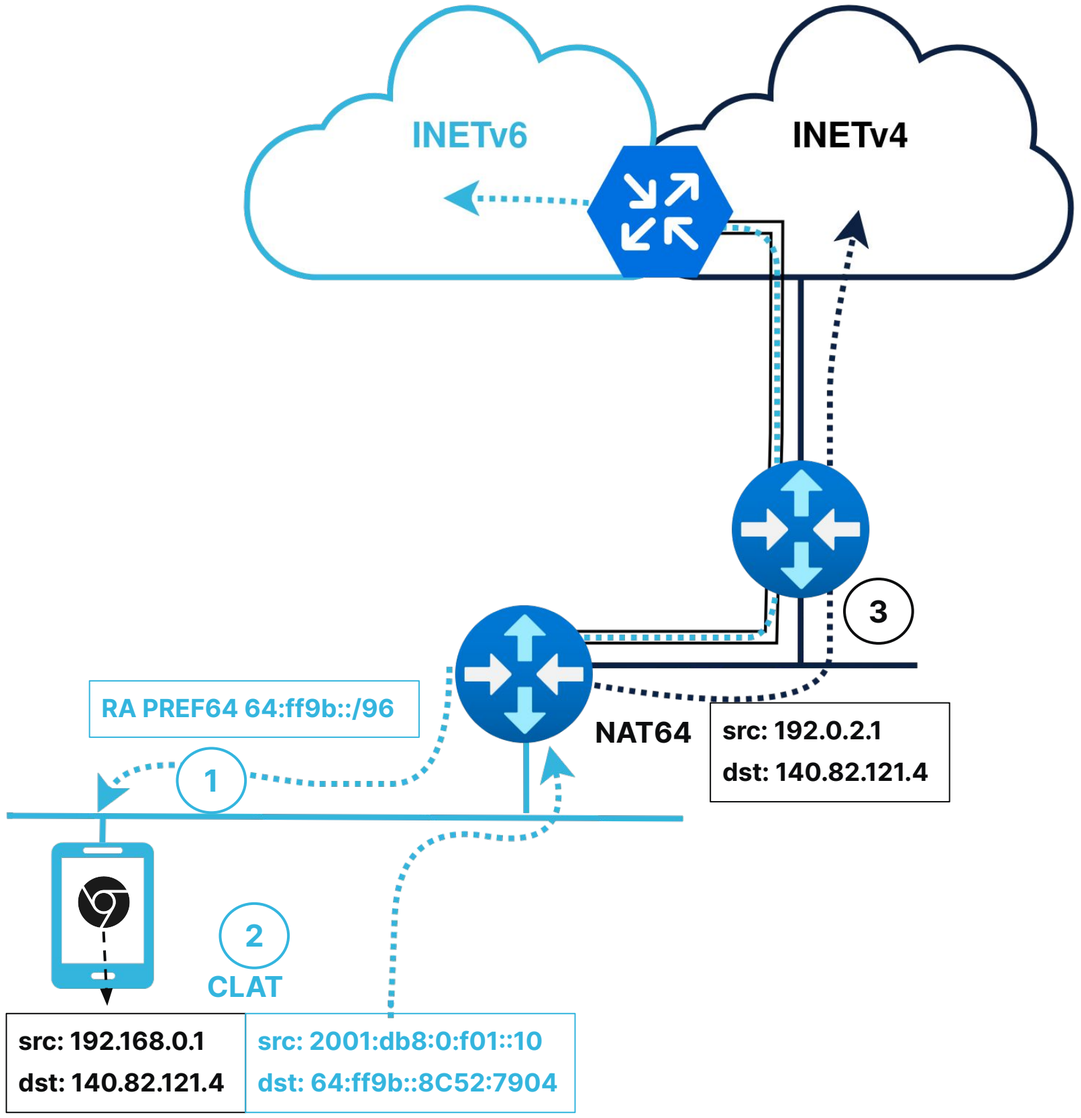
-Demone di traduzione **sul dispositivo** che fornisce IPv4 e default route alle applicazioni che non funzionano altrimenti
-Quindi lo traduce in autonomia nell'IPv6 presente sulla NIC

PREF64

-Tramite RA viene comunicato alla LAN il prefisso di NAT64 configurato
-Nel nostro caso è il prefix standard 64:ff9b::/96
-Presente dalla versione 23.05 del firmware OpenWRT
-Integrato nella WebGUI

Funzionamento

-I demone di CLAT forma i pacchetti destinati a reti v4 only, con il prefix ricevuto via PREF64
-Non necessita di DNS64
-Non ha le limitazioni elencate in DNS64
-Implementazione dipende dal Sistema Operativo



IPv6 State of art

	DHCPv6	SLAAC	DHCP108	PREF64	CLAT	DNS64
Windows	✓	✓	✗	✗	✗	✓
macOS	✓	✓	13+	13+	13+	✓
Ubuntu	✓	✓	systemd-networkd v 255	✗	✗	✓
iOS	✓	✓	15+	15+	15+	✓
Android	✗	✓	11+	11+	11+	✓

Considerazioni finali

IPv6-only funziona meglio del previsto

-Anche Win11 senza 464xLAT non da pressoché nessun problema
  Solo il download di alcune app/giochi ha ipv4 literals
-Sui cellulari non ci si rende conto della differenza
-Una rete IPv6-mostly è tranquillamente applicabile nella realtà

C’è fermento su IPv6!

-Windows ha dichiarato a Marzo di cominciare a lavorare su 464xLAT
-Linux ha messo il focus su 464xLAT da poco (dhcp option 108)

IoT ancora acerbo

-Far funzionare i device IoT in IPv6 è stata la cosa più complicata
-Alla fine si è reso necessario il dual stack
-Test effettuati con 4 vendor diversi, stesso risultato

Thank You!

Link Utili

OpenWRT project: www.openwrt.org
Table of hardware: https://openwrt.org/toh/start
Tunnel Broker: https://tunnelbroker.net/
Jool project: https://nicmx.github.io/Jool
IPv6 test: http://test-ipv6.com
IPv6 sinners: http://whynoipv6.com
DNS Proxy: https://gitlab.com/miyurusankalpa/IPv6-dns-server

Contatti

elia.aielli@timenet.it

Domande?