Transition from IPv4 to IPv6

Computer Network Technologies and Services

Copyright Notice

The road to IPv6

IPv4 to IPv6 transition

- Ideally:
  - Incremental
  - Seamless
  - Smooth

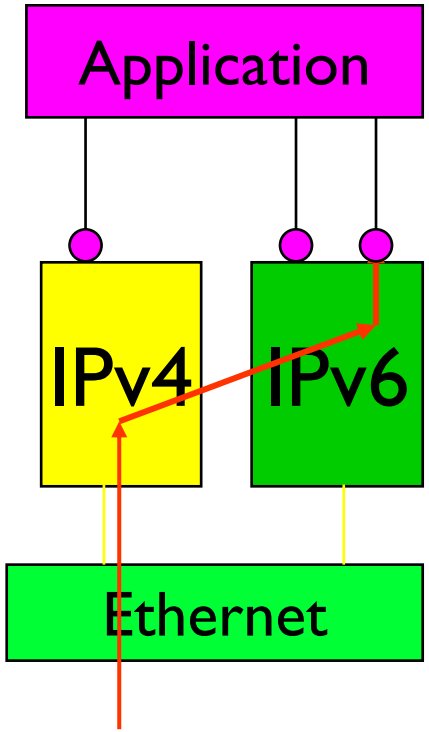
Ipv6 - © see page 2

How can it be achieved?

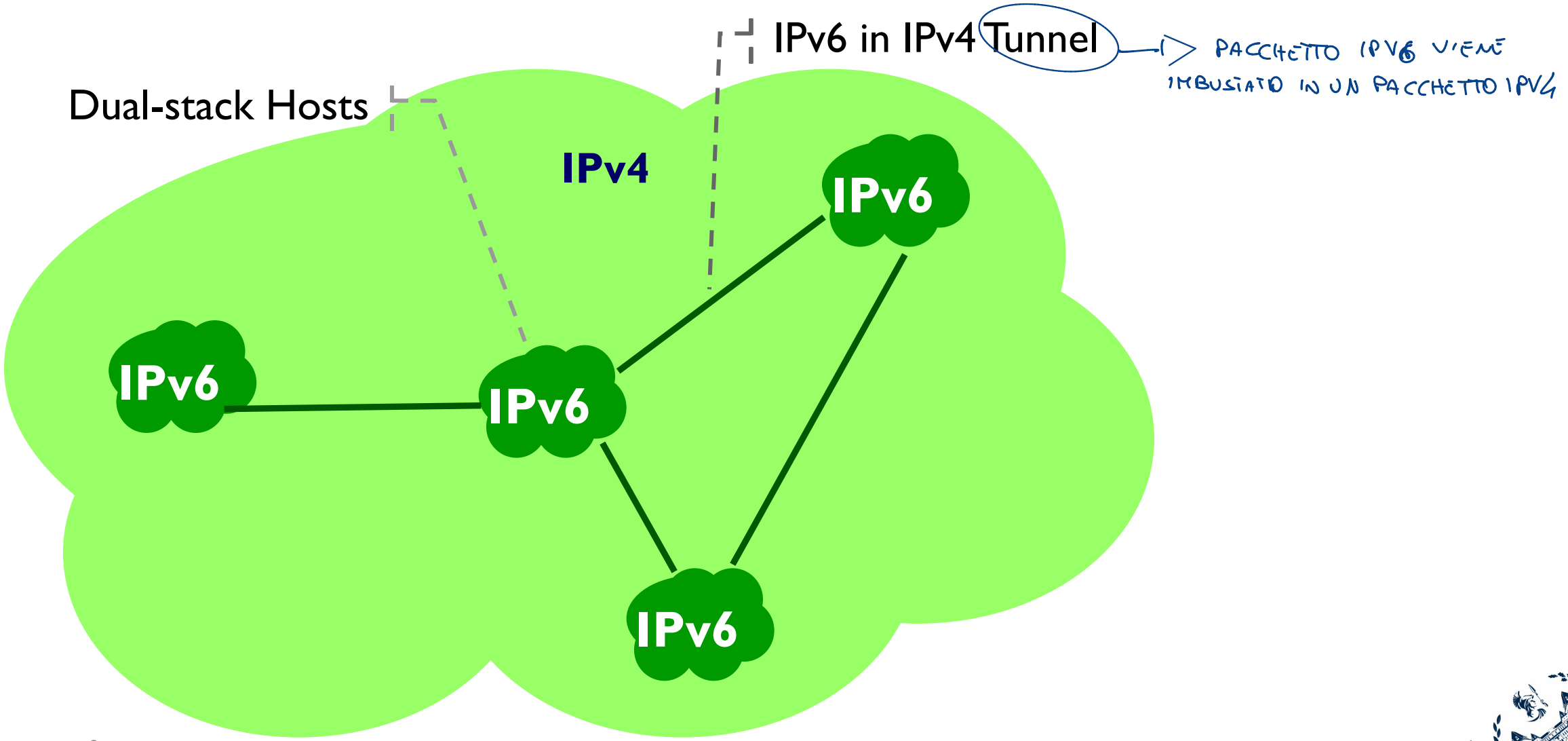
Come gestire macchine dual stack in uno scenario dove devono convivere IPV4 e IPV6

- Dual-stack approach
  - IPv6 as a new layer-3 protocol
  - Generate/receive v6 or v4 packets as needed
- Address mapping
- Tunneling
- Translation mechanisms

Come metto in comunicazione le reti?

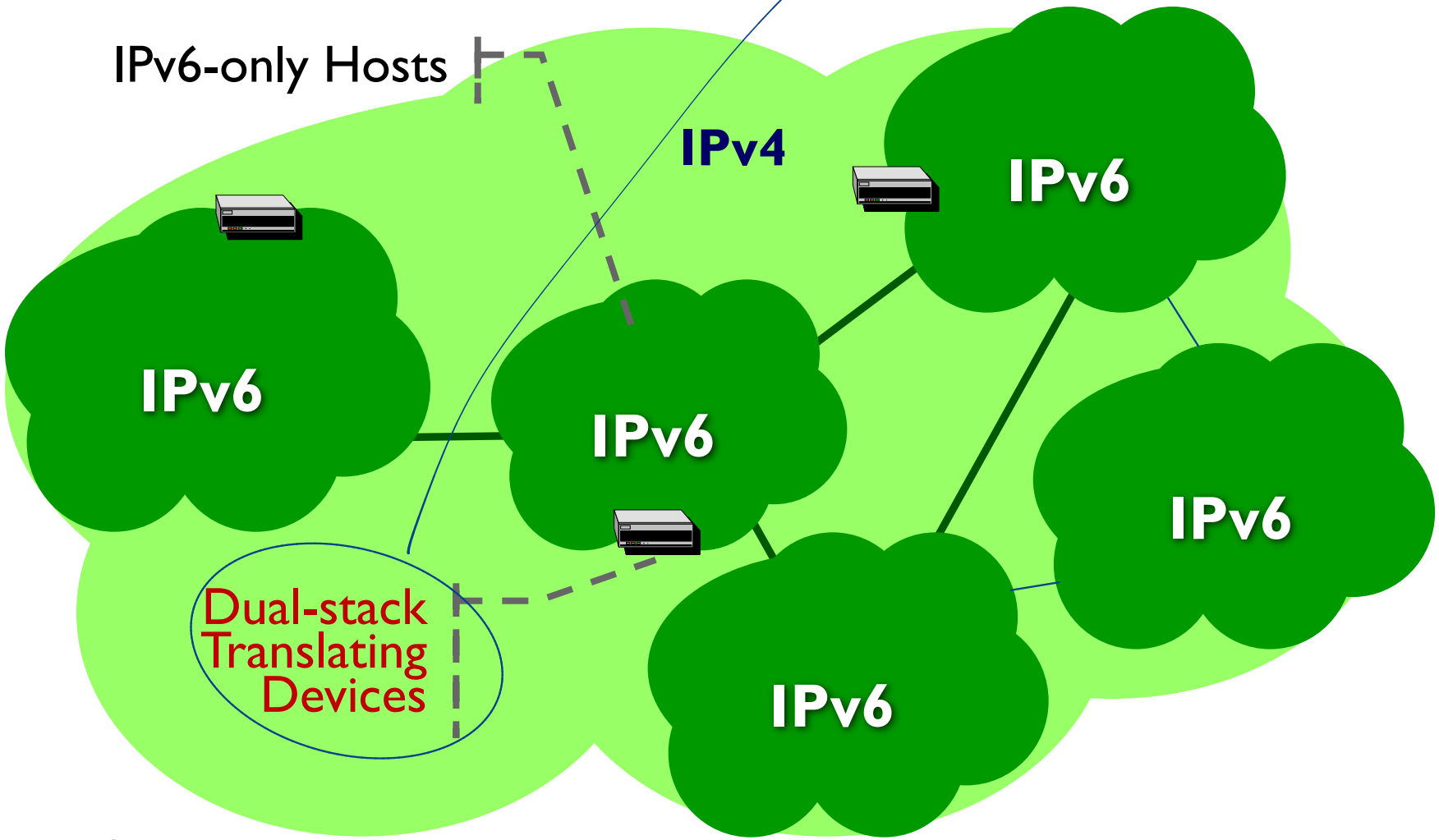


Step 1: isolated IPv6 networks

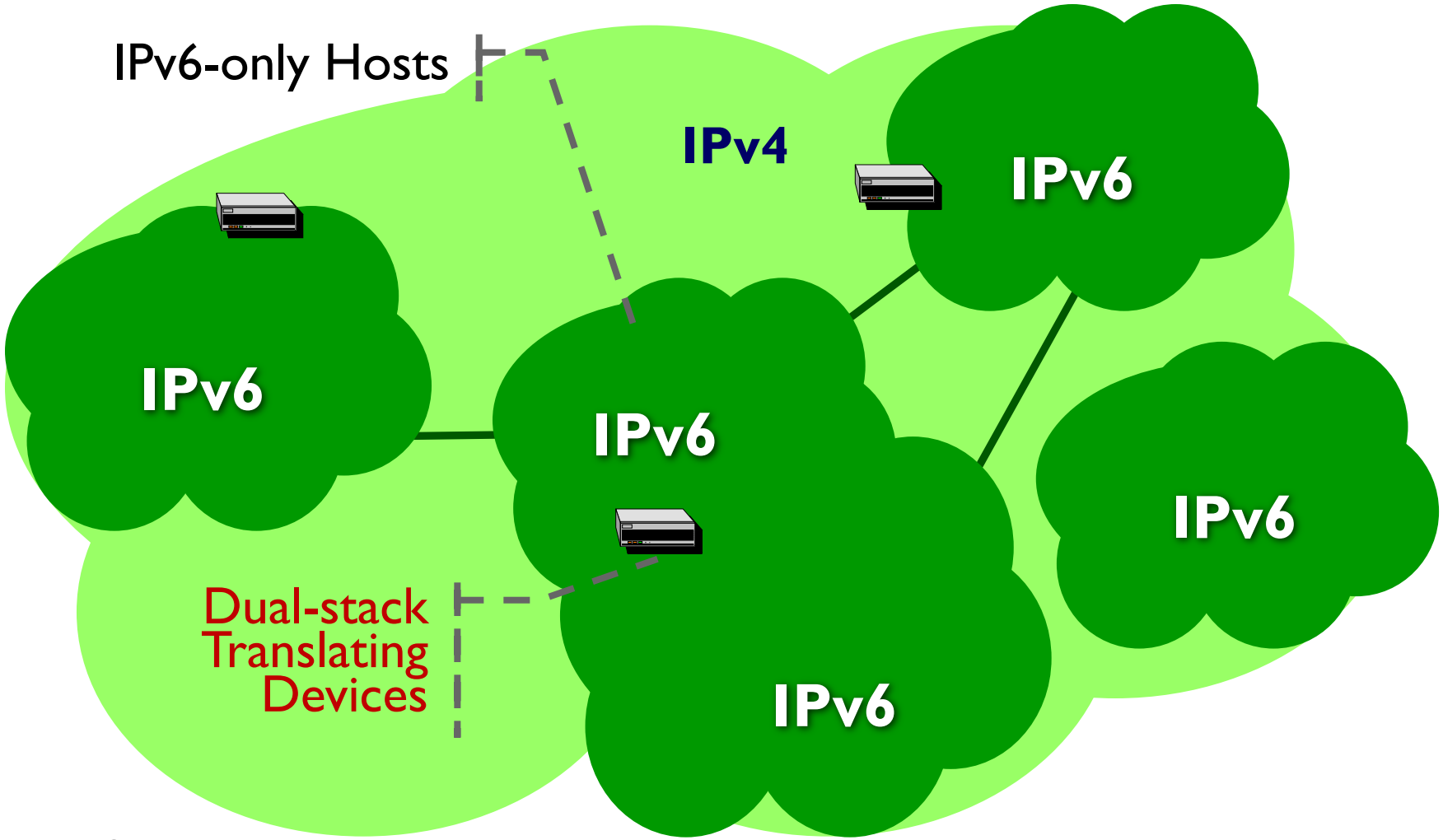


Step 2: IPv6 islands grow

TRADUCONO IL PACCHETTO IPV6 IN UN PACCHETTO IPV4

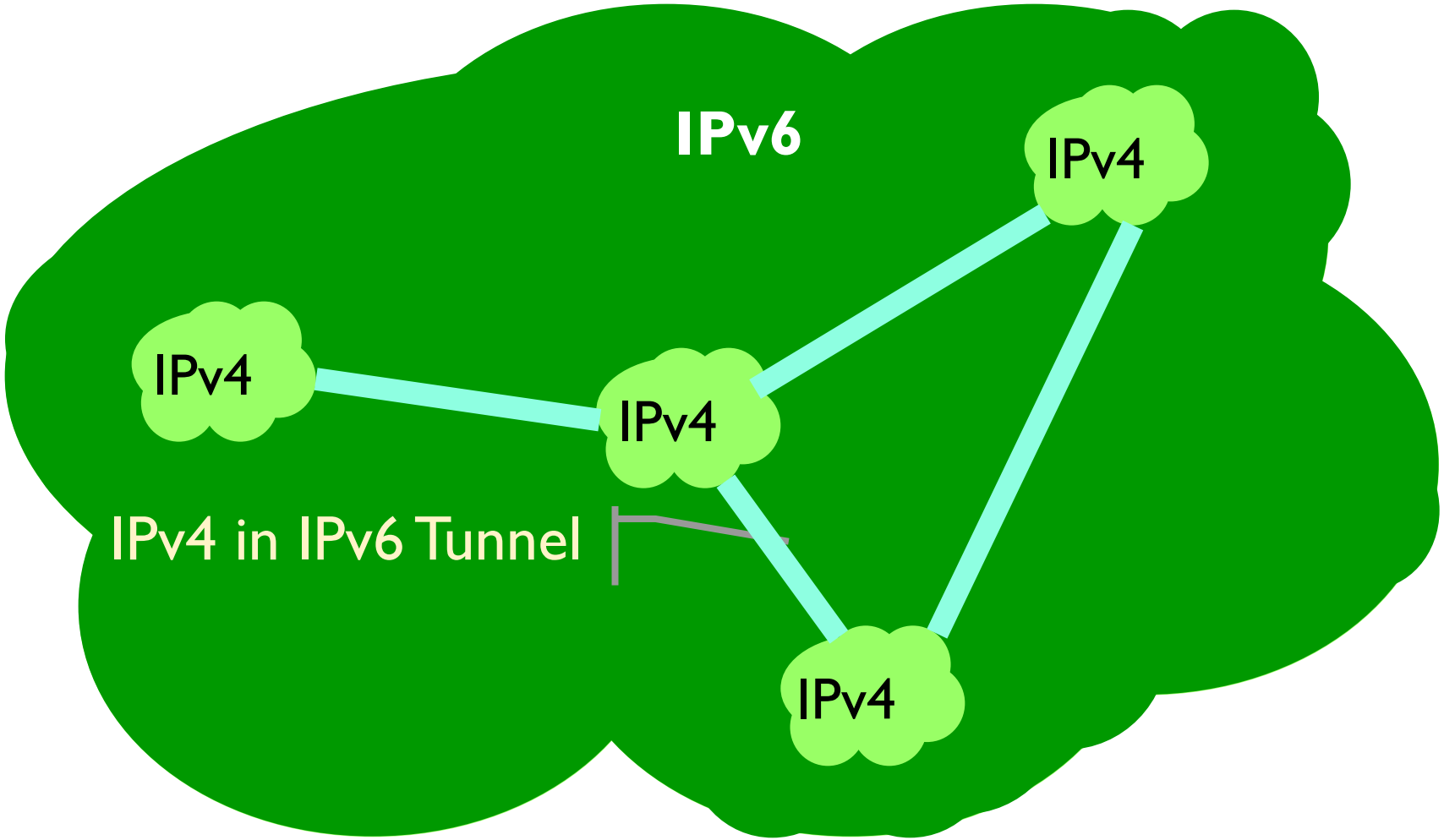


Step 3: Native IPv6 connectivity



Step 4: IPv6 takes over

(ARRIVEREMO A DAVERE TANTE RETI IPV6 e MENO IPV4 QUINDI LA SITUAZIONE SI RIBALTERÀ e DOVREMO USARE IL TUNNEL PER IMBUSTIARE IPV4 IN IPV6)

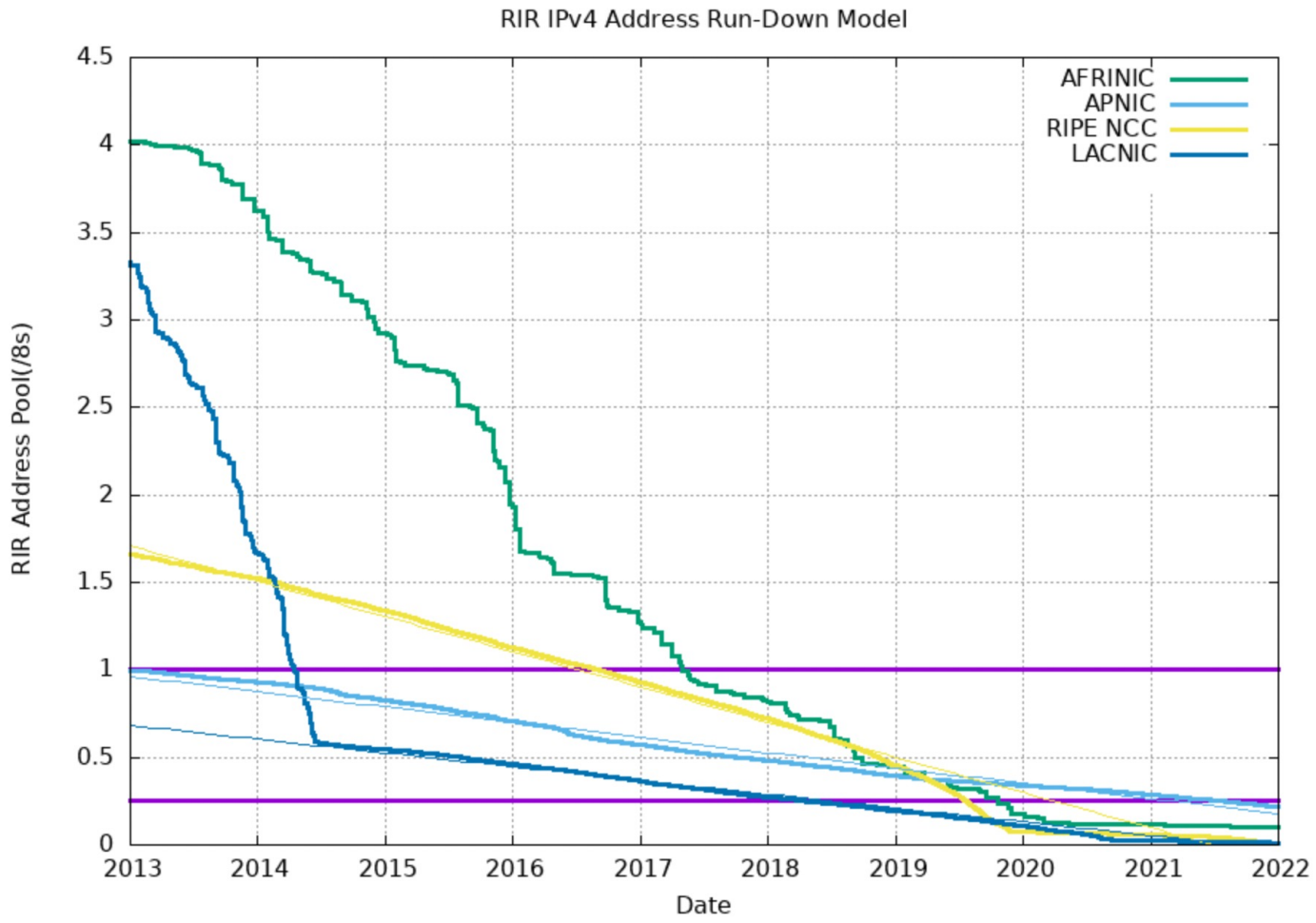


Are we ready?

- Quite so!
  - All protocols specified since 1996
- IPv6 implemented on **routers**
  - Even if less stable than IPv4
  - Possibly missing some functionalities
  - Also hardware implementations (Layer-3 switches)
- IPv6 implemented in **end systems**
  - Windows (since 2000 version)
  - Unix: Ubuntu, Debian, FreeBSD…
  - MAC (since MAC OS X)

When will it happen?

- Large IPv4 install base
- As of March 2022, according to Google, the IPv6 adoption rate globally is around 34%, (46% in the U.S. alone!)
- Only one true motivation: <u>Address space depletion</u>
- no official switch-off date
  - Will happen gradually



Transition from IPv4 to IPv6

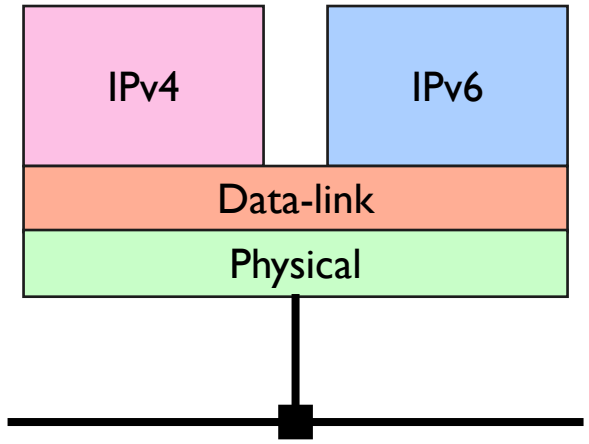
Assumption
(and problem to solve)

IPv4 and IPv6 will coexist

(at least for a while)

Dual Stack Approach

- Both IPv4 and IPv6 capabilities
  - In all hosts and routers supporting IPv6
  - IPv4 support can be (gradually) removed (and included in new hosts) once all hosts have IPv6
- Hosts communicate natively with both
- Complete duplication of all protocol stack components
  - Routing protocols
  - Routing table
  - Access lists



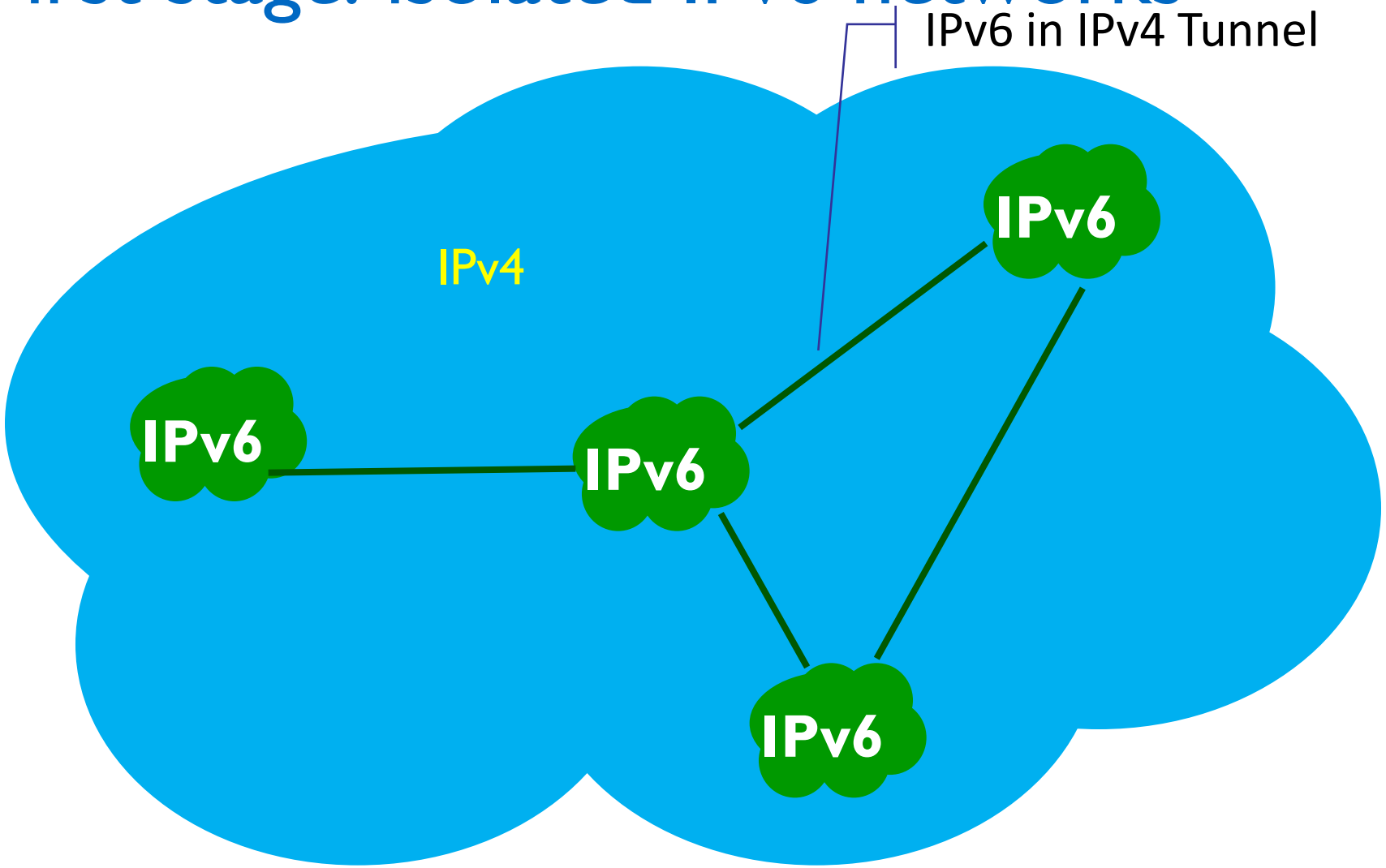
Dual Stack Limitations

- It does not reduce the need for IPv4 addresses
  - Each host still needs an IPv4 address to use IPv4
- Applications have the responsibility whether to use IPv4 or IPv6

Not all hosts will be dual stack

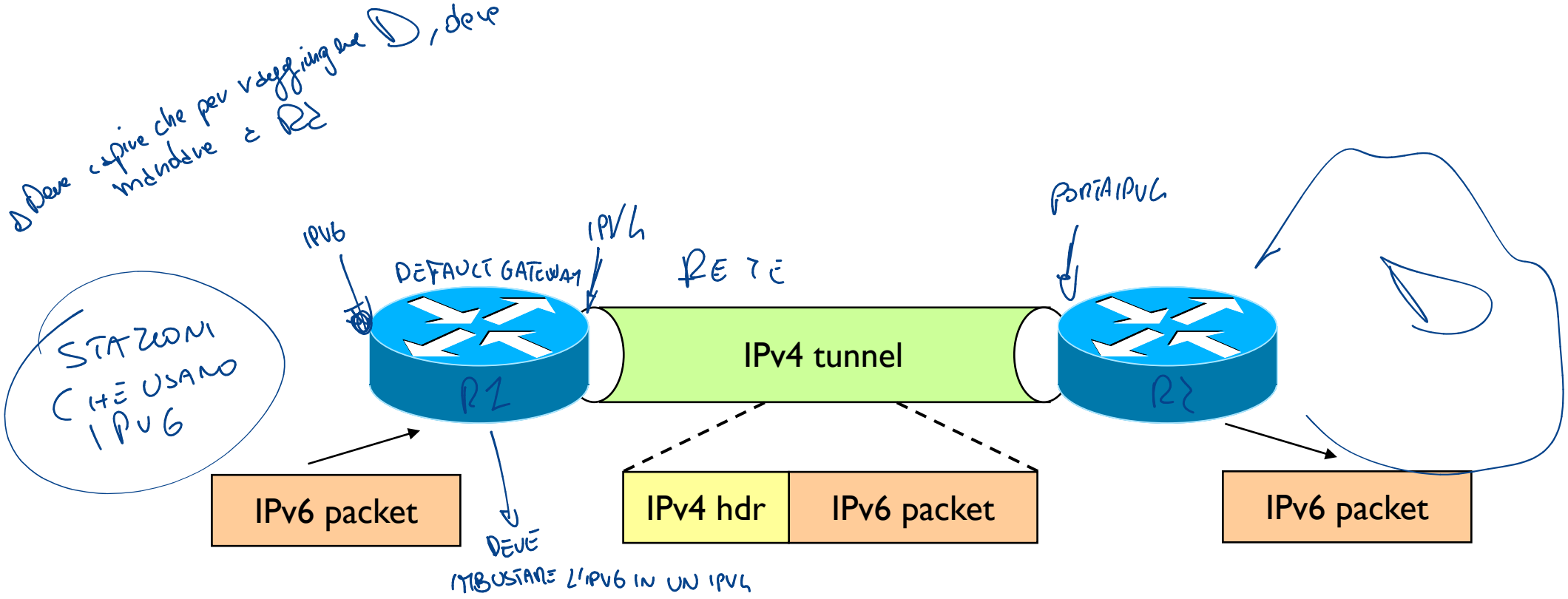
- IPv6 hosts shall communicate with IPv6 hosts through an IPv4 network
  - Same for IPv4 hosts through an IPv6 network
- IPv6 hosts shall communicate with IPv4 hosts
  - Translation mechanisms must be used
  - Not targeting IPv4 hosts contacting IPv6 ones
    - Difficult to map the large IPv6 address space on smaller IPv4 address space

First stage: isolated IPv6 networks



Traversing a IPv4-only Network

- Tunnelling
  - Encapsulation of IP (v6) packets into IP (v4) packets
- Emulates a "direct" link among IPv6 devices



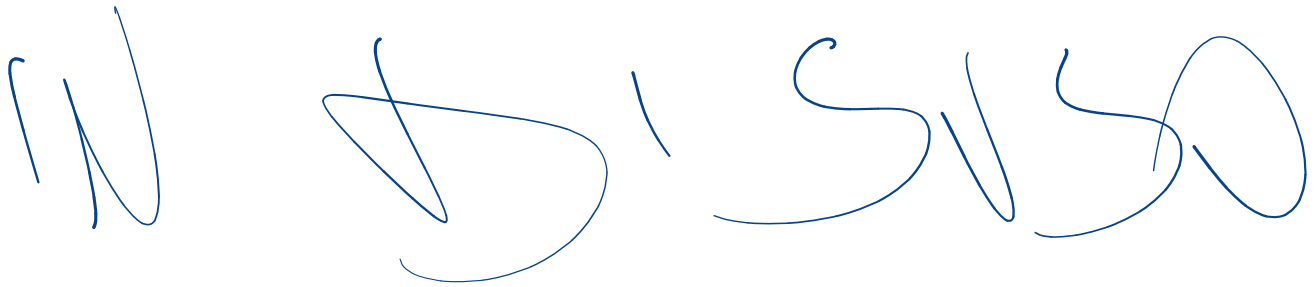
Tunnelling : x far passare del traffico su una rete che non è in grado di capire quel traffico o che non voglio lo capisca

- End points: hosts and routers
- Protocols
  - GRE (Generic Routing Encapsulation) → PROTOCOLLO PENSATO X IL TUNNELLING
  - IPv6 in IPv4
    - Protocol type = 41
- Set up: manual and automatic → presumendo ad R1 di capire in maniera automatica che per raggiungere D (IPv6) deve andare da R2
  - IPv4-compatible addresses, 6over4 (RFC 2529), 6to4, Tunnel Broker (RFC 3053), ISATAP, Teredo

CREANDO TUNNEL DA INDIRIZZO DUAL-STACK A INDIRIZZO DUAL-STACK

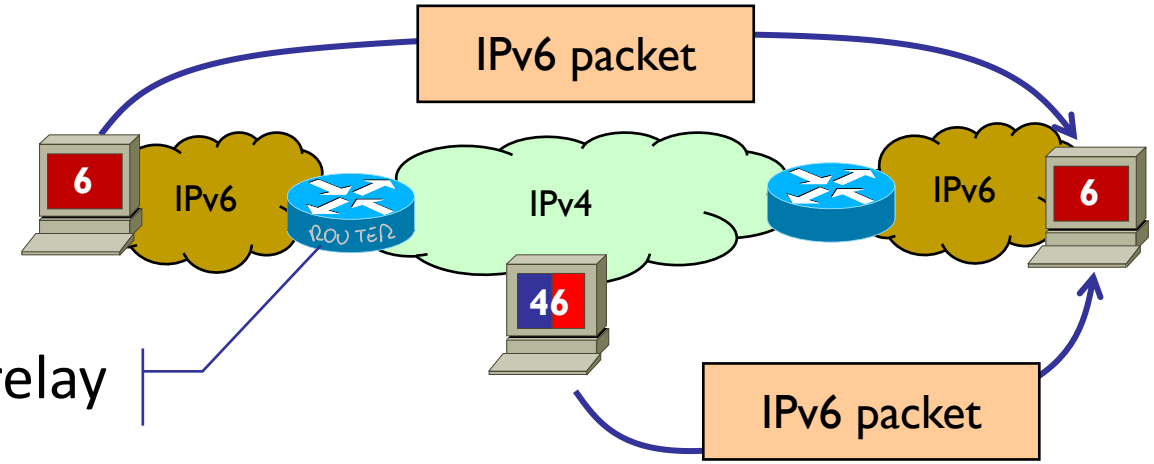
DEFINIRE SOLUZIONI PER IL TUNNEL AUTOMATICO

Host-centered solutions — *Network-centered solutions*



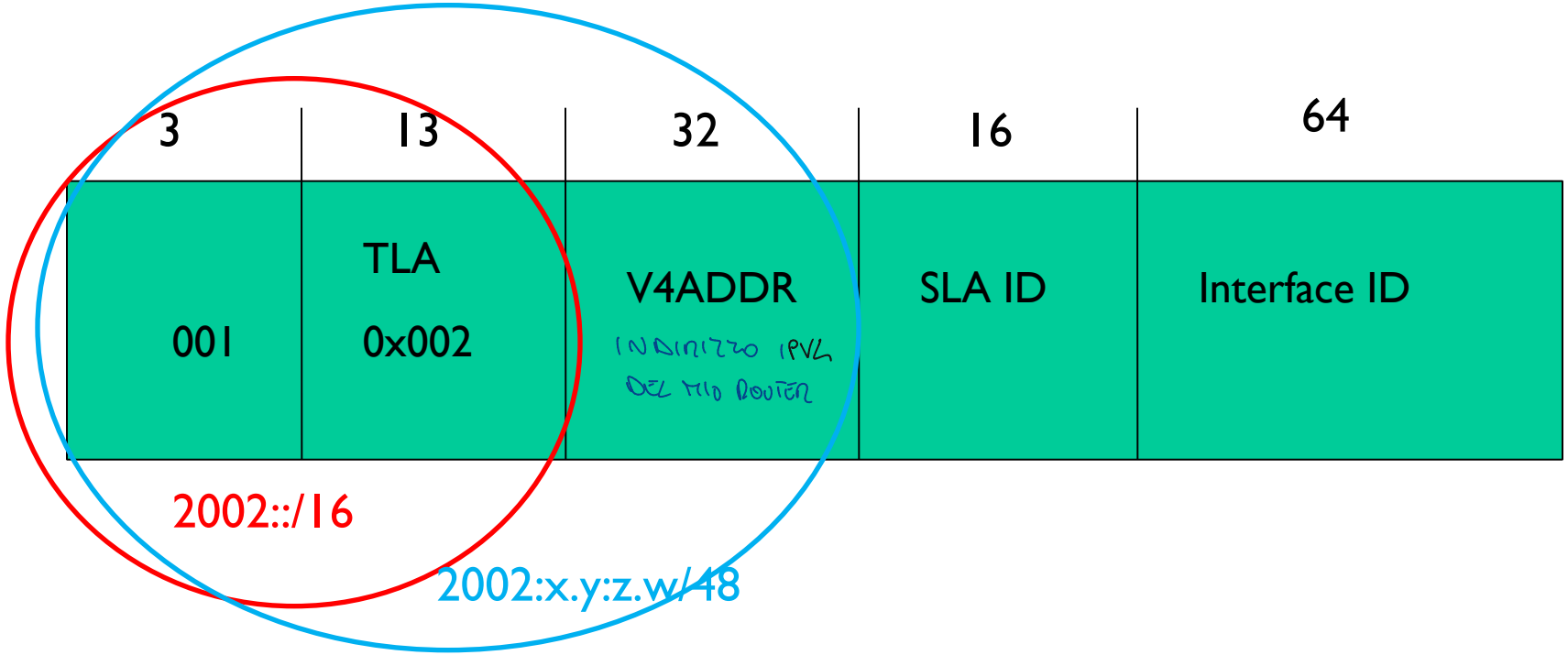
6to4

HOST IPV6 CON INDIRIZZO GLOBAL UNICAST 2002::/16



6to4 router or relay

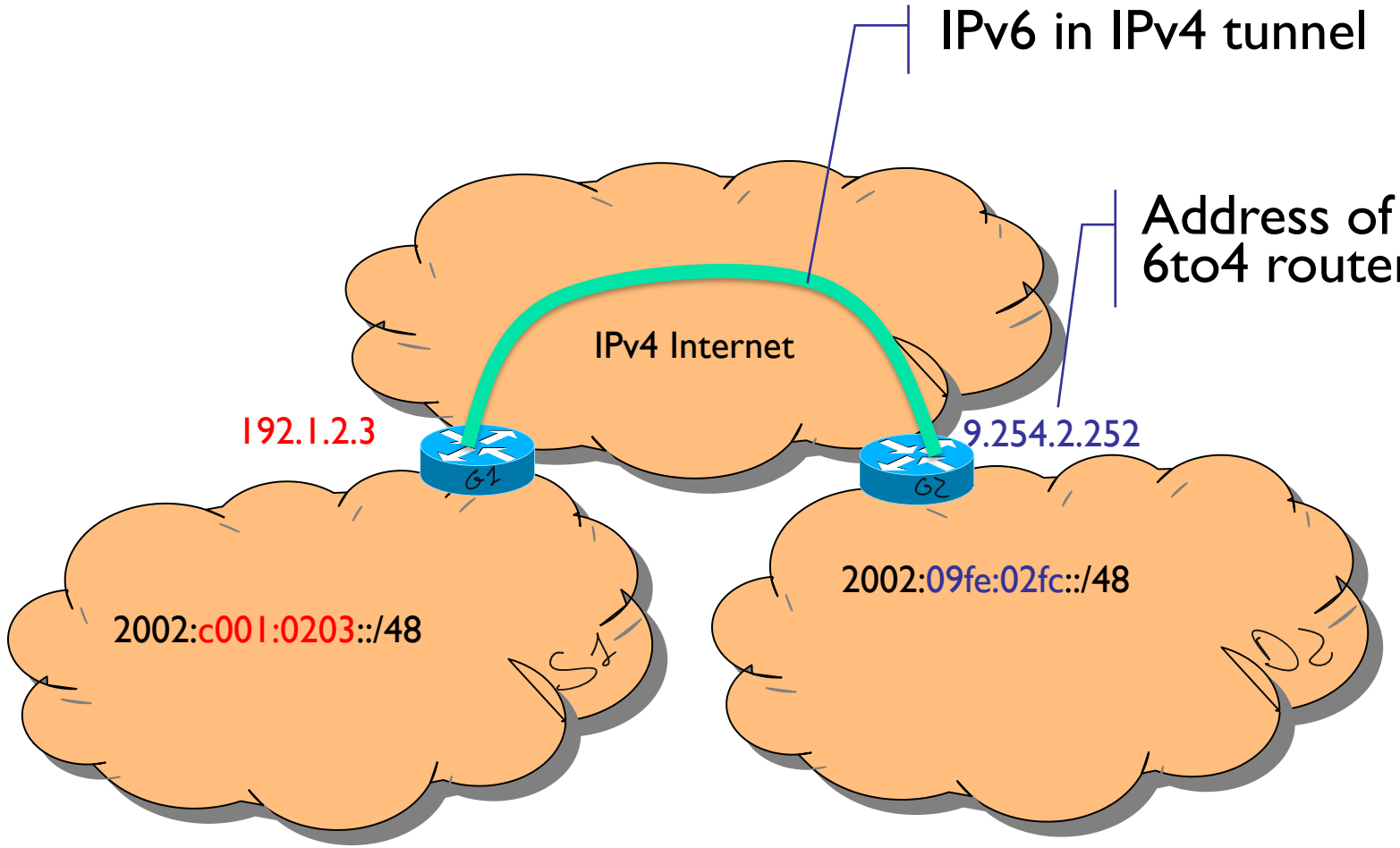
- Relay address embedded in IPv6 prefix



Basic 6to4 Scenario

S1 CONTATTA G1 → CAPISCE DAI PRIMI BIT (2002:) CHE BISOGNA USARE IL 6to4
G1 CONTATTA G2
G2 MANDA A D2

Not meant for IPv4 host to IPv6 host communication



NOTA
192.1.2.3 = c001:0203

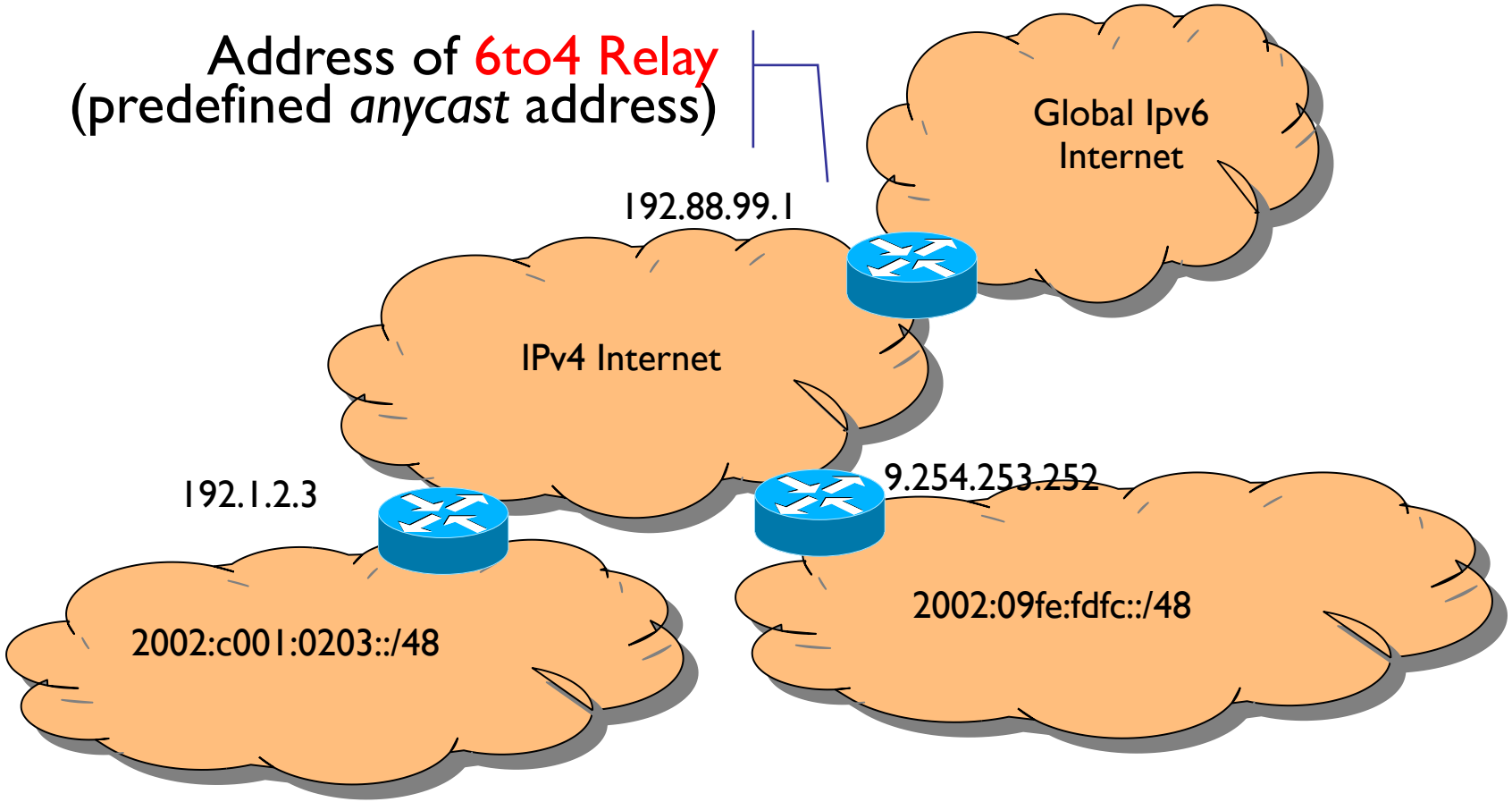
NOTA
9.252.2.252 = 09fe:02fc

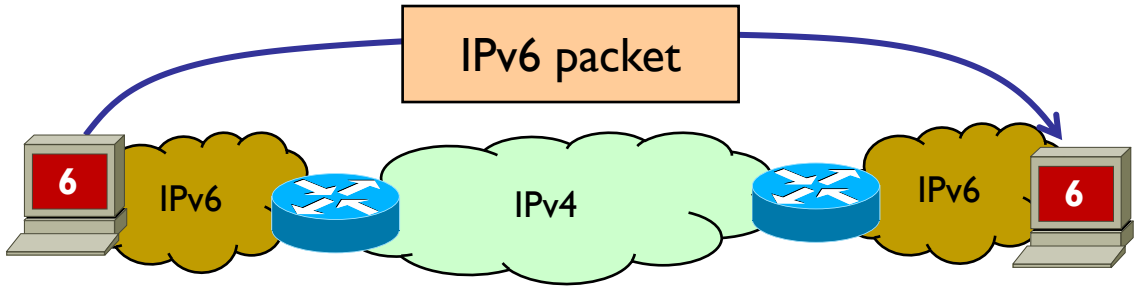
PROBLEMA:
SONO COSTRETTO AD USARE 2002

Mixed 6to4 Scenario

6to4 Relay must be default gateway of 6to4 routers

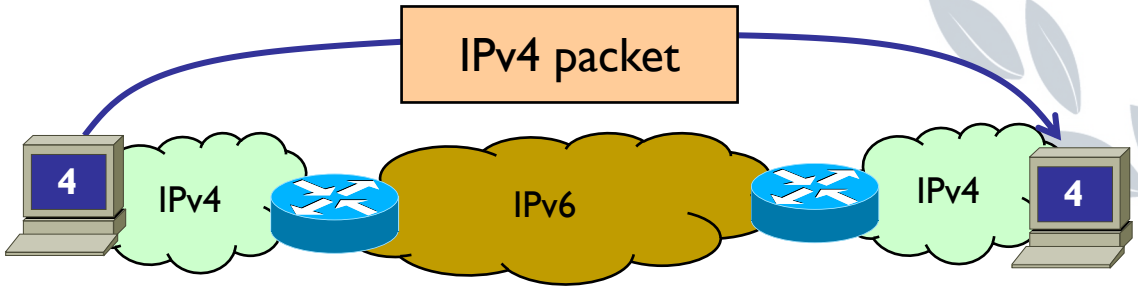
ALTRO
QUANDO CREAVI IPV6
DOVEVI COMUNICARE
DA QUALE ROUTER
ERI RAGGIUNGIBILE





Scalable, Carrier-grade Solutions

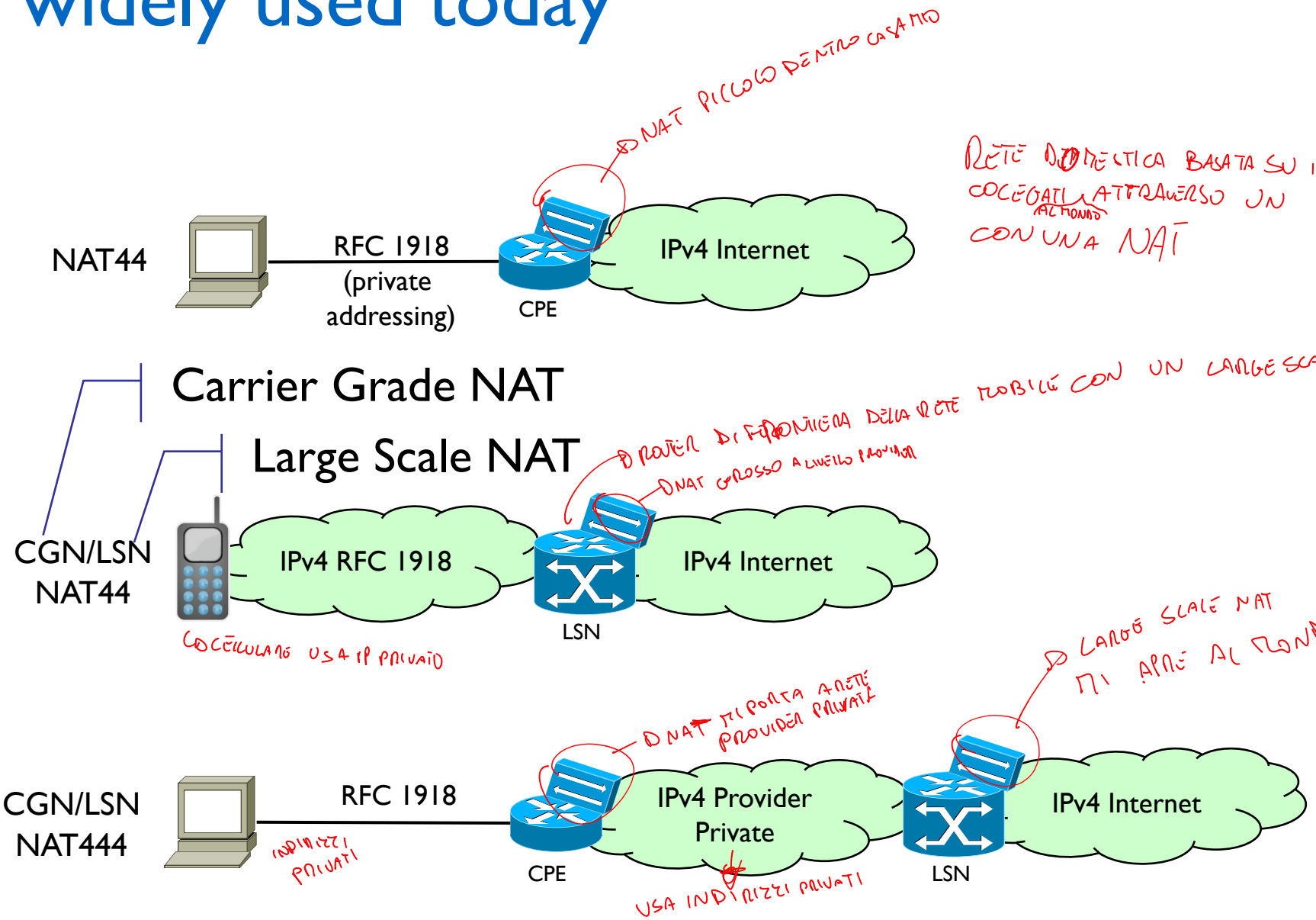
Native IPv6 (IPv4) hosts exchange IPv6 (IPv4) packets through an IPv4 (IPv6) network



Goals

- Still need to support
  - IPv4 servers possibly communicating with IPv6 hosts
  - IPv4 clients
- Several Options
  - DS-Lite
  - A+P (DS-Lite evolution)
  - NAT64
  - *MAP-T and MAP-E*
  - *6PE (MPLS-based)*

NAT is widely used today



COSA SI FA PRE-IPV6

How do we like NAT?

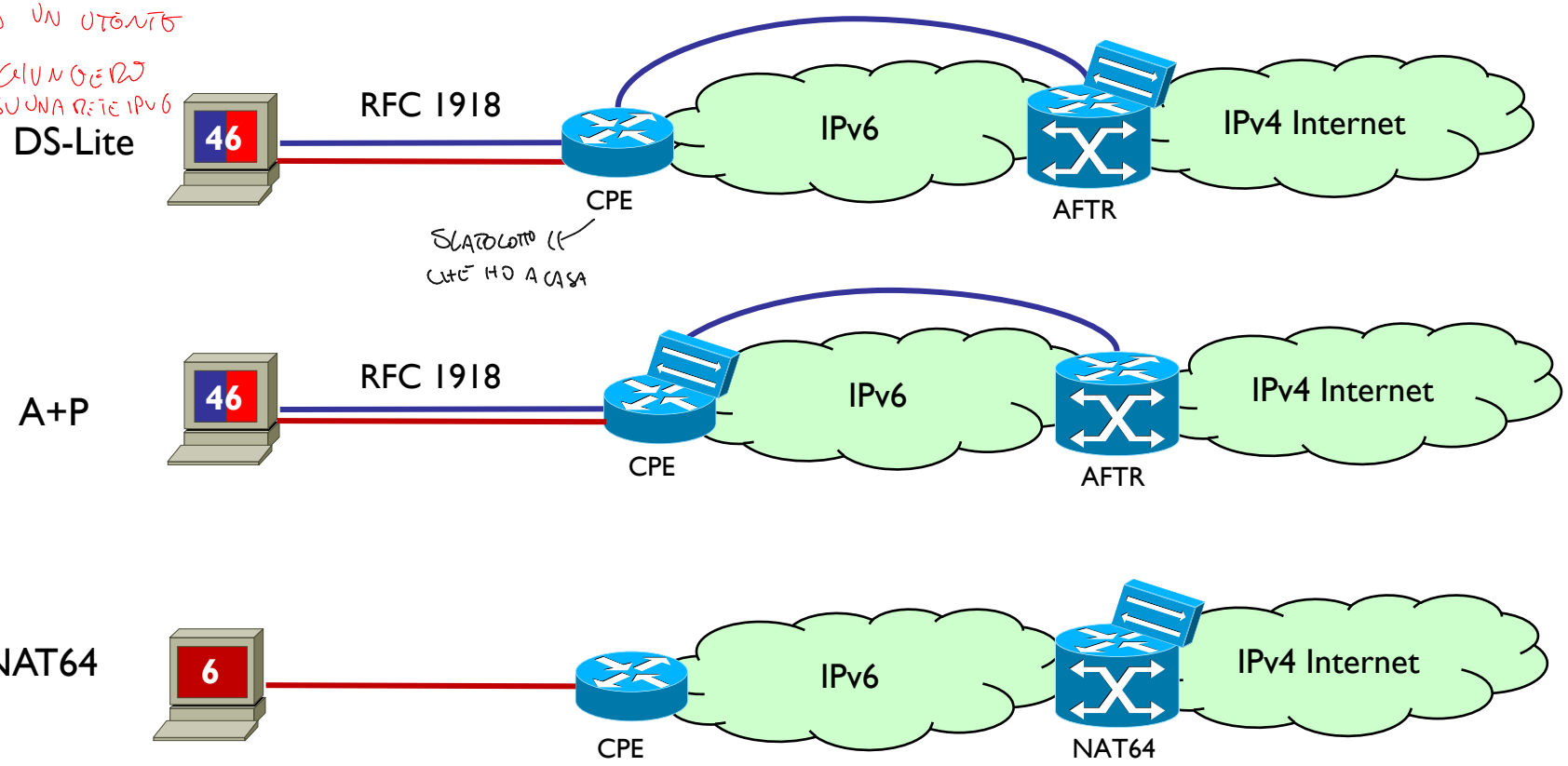
- Problematic with inbound sessions
  - E.g., servers
  - NAT + STUN/TURN may be ok for peer-to-peer sessions
- Bottleneck and single point of failure

Nevertheless

- Several (independent) cascaded instances of NAT are now very common
  - Starting from virtual machines
- Difficult to do without due to scarce addresses

Same Architecture with IPv6

DEVO PE ROUTARE A UN UTENTE PRIVATO IPV4 DI RAGGIUNGERE I SERVIZI IPV4 PASSANDO SU UNA RETE IPV6



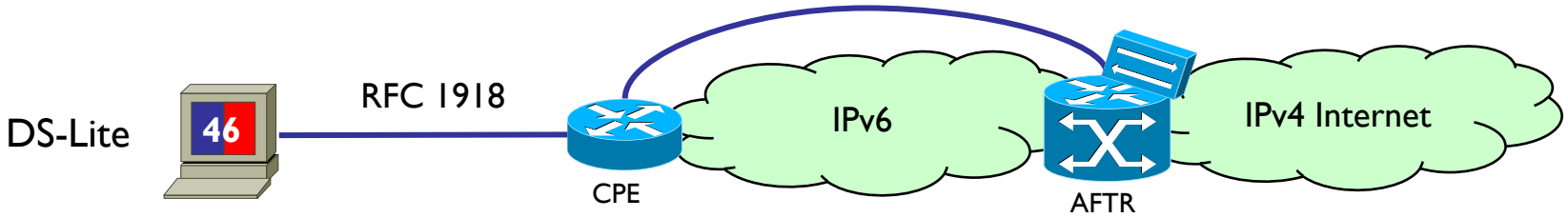
CPE: Customer Premises Equipment
AFTR: Address Family Transition Router

Note where the NAT function is located!

AFTR: Address Family Transition Router

RETE IN COMUNICAZIONE PROVIDER IPV6 CON ROTTE INTERNET IPV4

- Allows IPv4 host to communicate with IPv4 hosts over an IPv6 carrier infrastructure
  - Residential host and current providers
- Features an IPv6 tunnel concentrator and possibly a large-scale NAT
- In use in DS-Lite and A+P

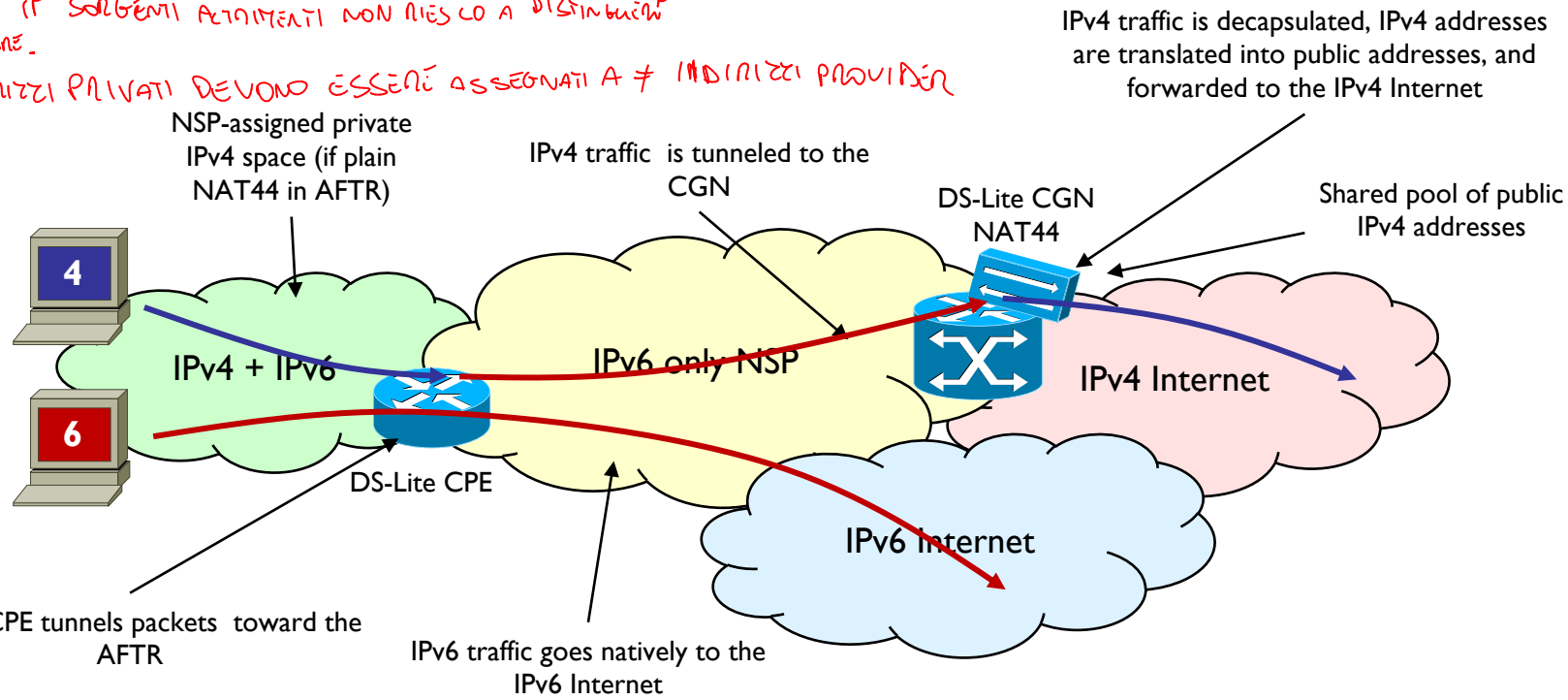


DS-Lite (Dual-Stack Lite)

- Dual-stack at the edge
- IPv6-only Service Provider backbone

- ARRIVA PACCHETTO IPV4 SUL CPE PRIVATO
- CPE CREE TUNNEL VERSO AFTR
- TRAMITE AFTR RAGGIUNGO IL CGNAT (un luogo scala 24)
- ATTRAVERSO QUESTO NAT, IL PACCHETTO PUÒ VIAGGIARE SU INTERNET

NOTA:
NON POSSO AVERE STESSI IP SORGENTI ALTRIMENTI NON RIESCO A DISTINGUERE A CHI DEVO RECAPITARE.
→ TUTTI GLI INDIRIZZI PRIVATI DEVONO ESSERE ASSEGNATI A # INDIRIZZI PROVIDER



SOLUZIONE: ALLA NAT AGGIUNGO INDIRIZZI IPV6 DEL CPE

Properties

- Reduces requirement for IPv4 addresses compared to dual-stack approach
  - Dual-stack requires public IPv4 address per host
- Extended NAT enables customer assigned (i.e., overlapping) addressing
  - IPv6 address of CPE in NAT table

Limitations

- NAT is not under control of customer
  - Same problem as with CGN
- Problematic with servers
  - Static mapping and port forwarding cannot be configured

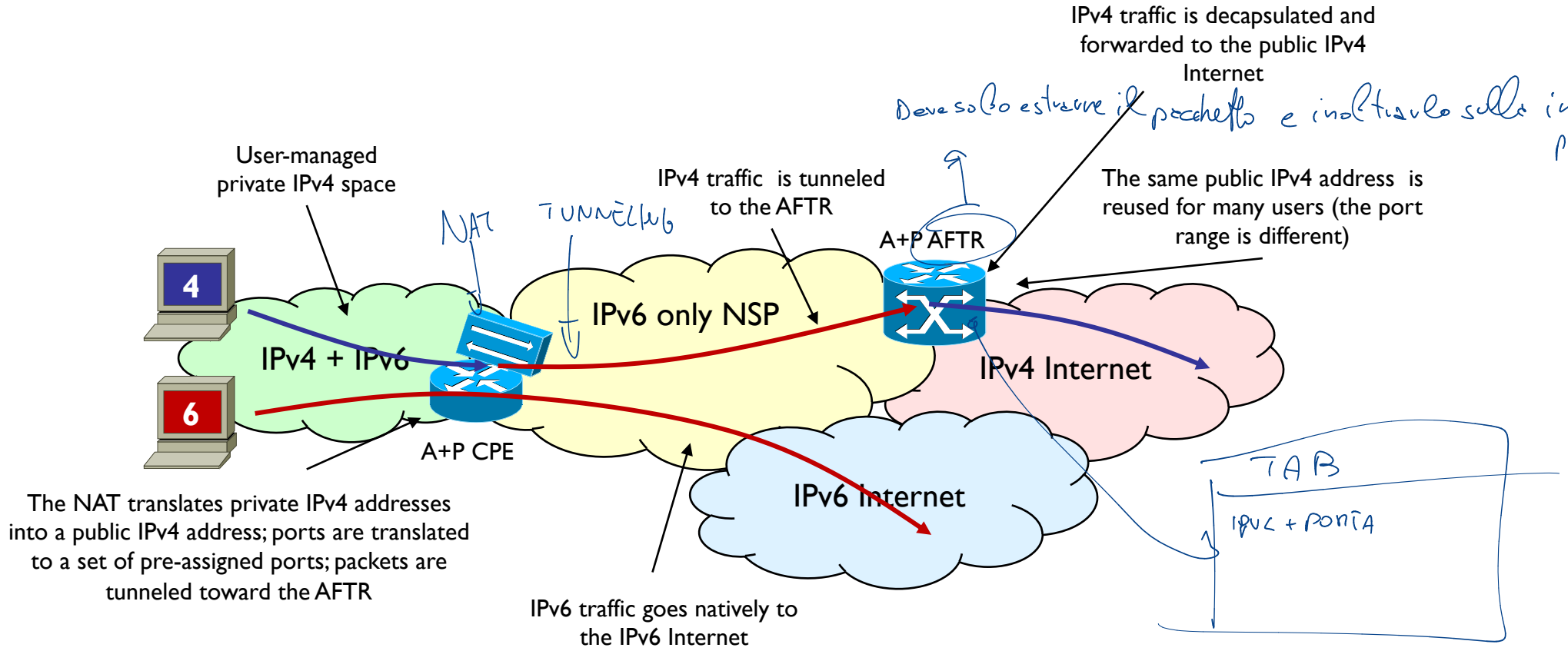
BASATA SULLO SPOSTAMENTO DEL NAT SULLA CPE - OGNI UTENTE HA IL CONTROLLO SUL SUO NAT

A+P (Address plus Port)

OGNI CPE HA UN PROPRIO IPV6 MA UN IPV4 IN COMUNE CON PIÙ CPE.

QUANDO IL TRAFFICO TORNA INDIETRO LA AFTR NON SA A CHI MANDARE XKÉ HANNO STESSI IPV4 → DEVO USARE LE PORTE.

- NAT is under control of customer
- Ranges of TCP/UDP ports are assigned to each customer
  - Only ports used by NAT on outside



Features

- No problem with overlapping private address spaces at customers'
- Ports can be assigned automatically to CPE using the Port Control Protocol (PCP)
  - CPE can negotiate more ports any time
- AFTR is just a IPv4-in-IPv6 (proto-41) tunnel terminator
  - NAT44 is no longer needed in the AFTR

NAT64 + DNS64: Principles

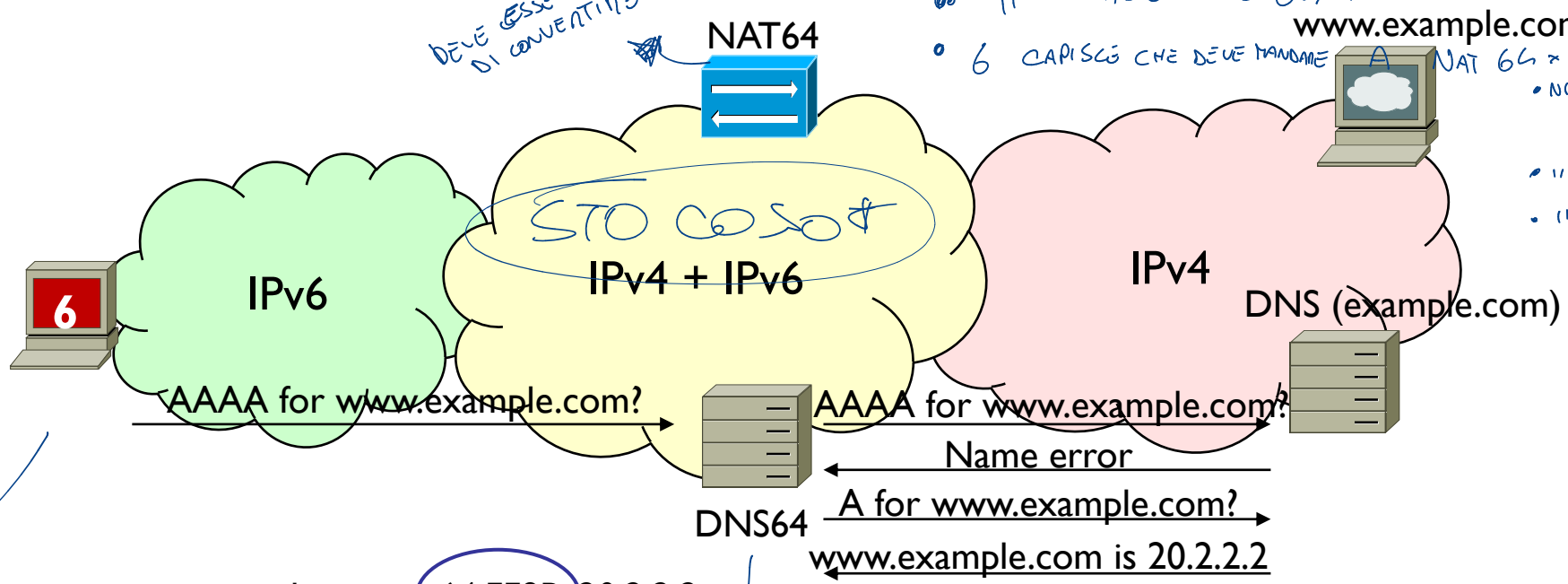
- An IPv6 prefix is dedicated to mapped IPv4 addresses
  - Either well-known or network-specific
  - RFC 6052
- DNS64 maps A records into AAAA using NAT64 prefix, then serves A and AAAA records to the client
- NAT64 router advertises NAT64 prefix into IPv6 network to attract traffic toward IPv4 hosts

HOST IPV6 CHE VUOLE PARLARE CON CLIENT IPV4

DNS64: Name Resolution

- 6 CONTATTA LOCAL DN SERVER (DNS 64) CON UNA QUERY AAAA
- DNS64 INOLTRA LA QUERY AAAA AL SERVER
- DNS64 RICEVE MESSAGGIO DI ERRORE
- " CAPISCE E PROVA A CHIEDERLO CON QUERY DI TIPO A
- " RICEVE IP_{v4} DEL SITO
- " AGGIUNGE 64:FF9B:: E MANDA AD HOST IPV6
- 6 CAPISCE CHE DEVE MANDARE A NAT 64 x COMUNICARE CON WWW.example
  - NAT 64 GRAZIE AL PREFISSO CAPISCE
  - " TOGLIE PREFISSO IPV6
  - " METTE L' IPV4

DEVE ESSERE INGRADO DI CONVERTIRE IN IPV4



COSA CONTATTA DNS 64?

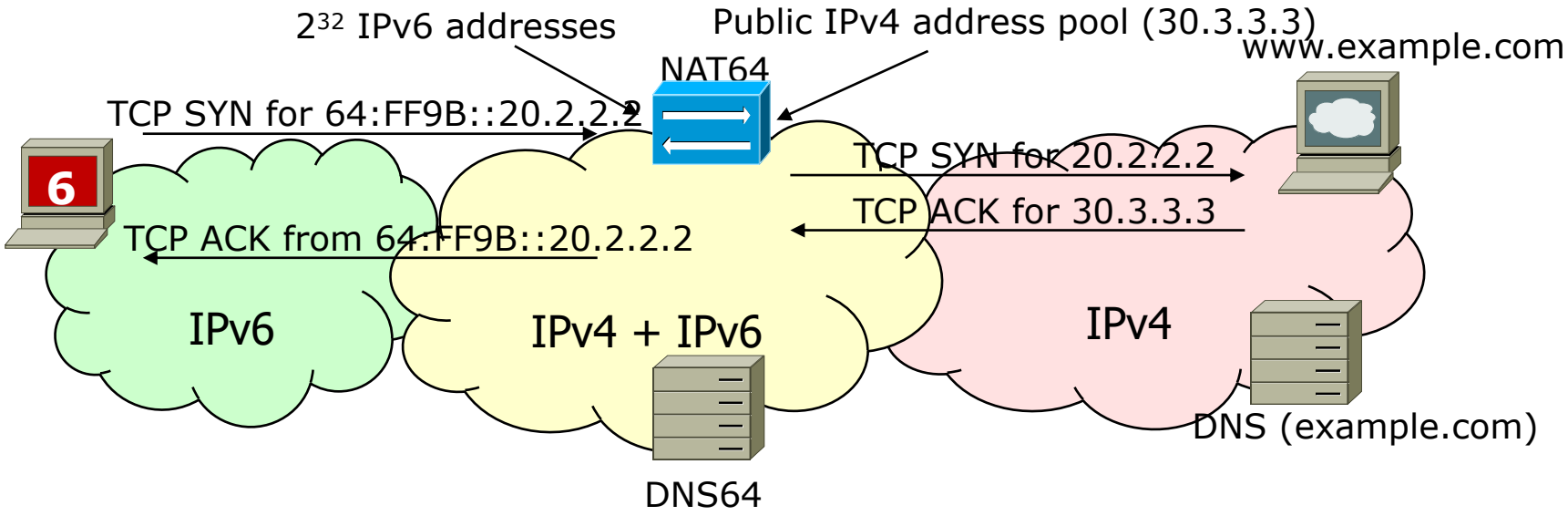
NAT64 MANDA DEGLI AVVISI DICENDO CHE LA RETE 64:FF9B:: QUALCOSA È RAGGIUNGIBILE TRAMITE LUI

DEVE essere in grado di parlare con HOST IPV6 e RETE IPV4

Well-known or deployment specific prefix (configured on DNS64 and possibly NAT64)

NAT64: Packet Forwarding

- NAT64 (outbound)
  - Translates IPv6 address and packet into IPv4
  - Picks a free IPv4 address/port from its pool
  - Builds NAT session entry



NAT64 + DNS64 Limitations

- Only when the DNS is involved
  - I.e., hostnames are used
  - E.g., it does not work in case the user directly specifies an IPv4 address
    - E.g., `ping 1.2.3.4`
- No DNSSEC
  - In DNSSEC authoritative DNS signs record
  - But DNS64 modifies records