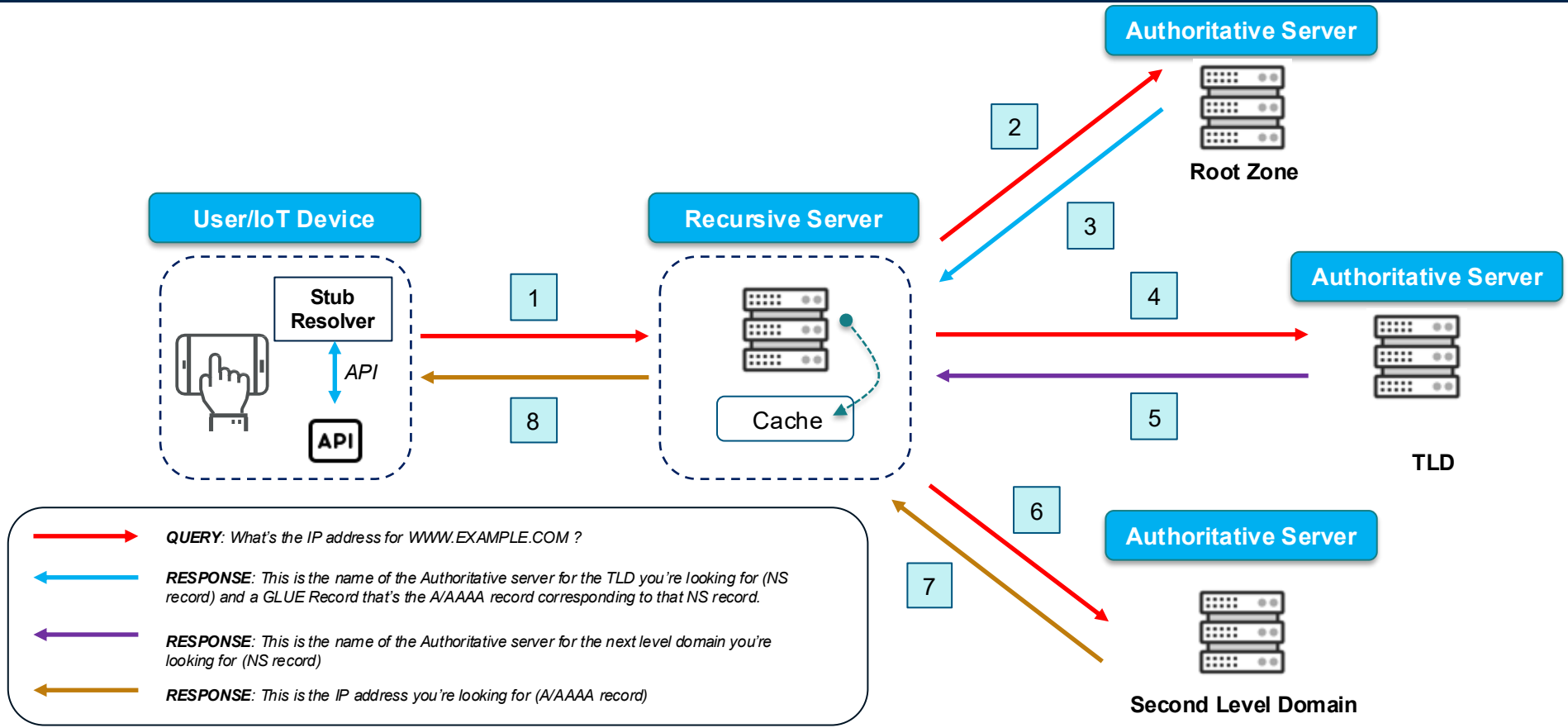
DNS for IPv6 Only Networks

Champika Wijayatunga, Technical Engagement Director - APAC

Vietnam Internet Conference 2026

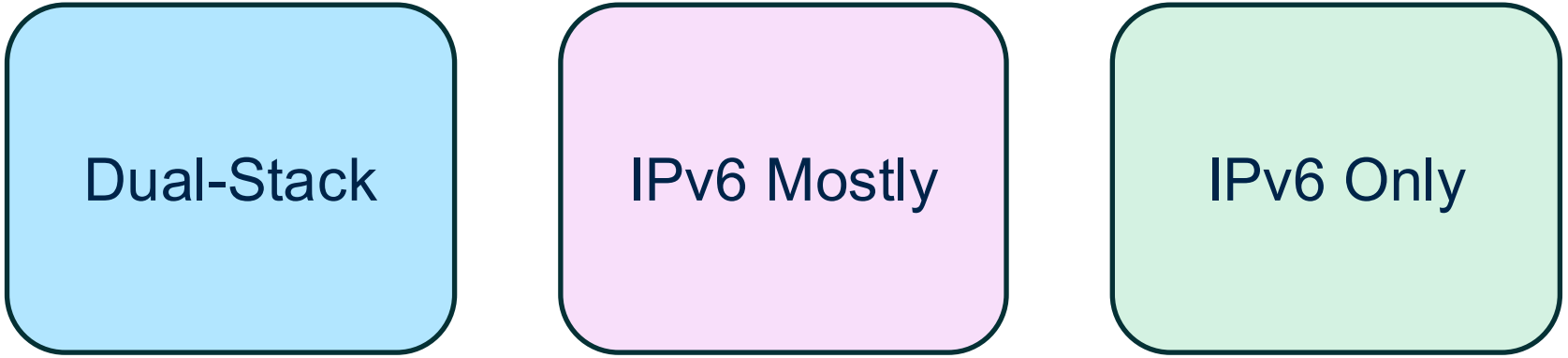
DNS Components

DNS Query Resolution



Deployment of IPv6

IPv6 Deployment Stages



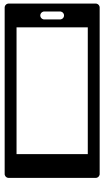
IPv6 Deployment Stages

- Dual-Stack
  - Both protocols are treated equally
- IPv6 Mostly
  - Most traffic is IPv6, but IPv4 support still exists for exceptions
- IPv6 Only
  - IPv4 is no longer present on hosts

Dual-Stack

Dual-Stack

- The traditional approach.
- Maximum compatibility

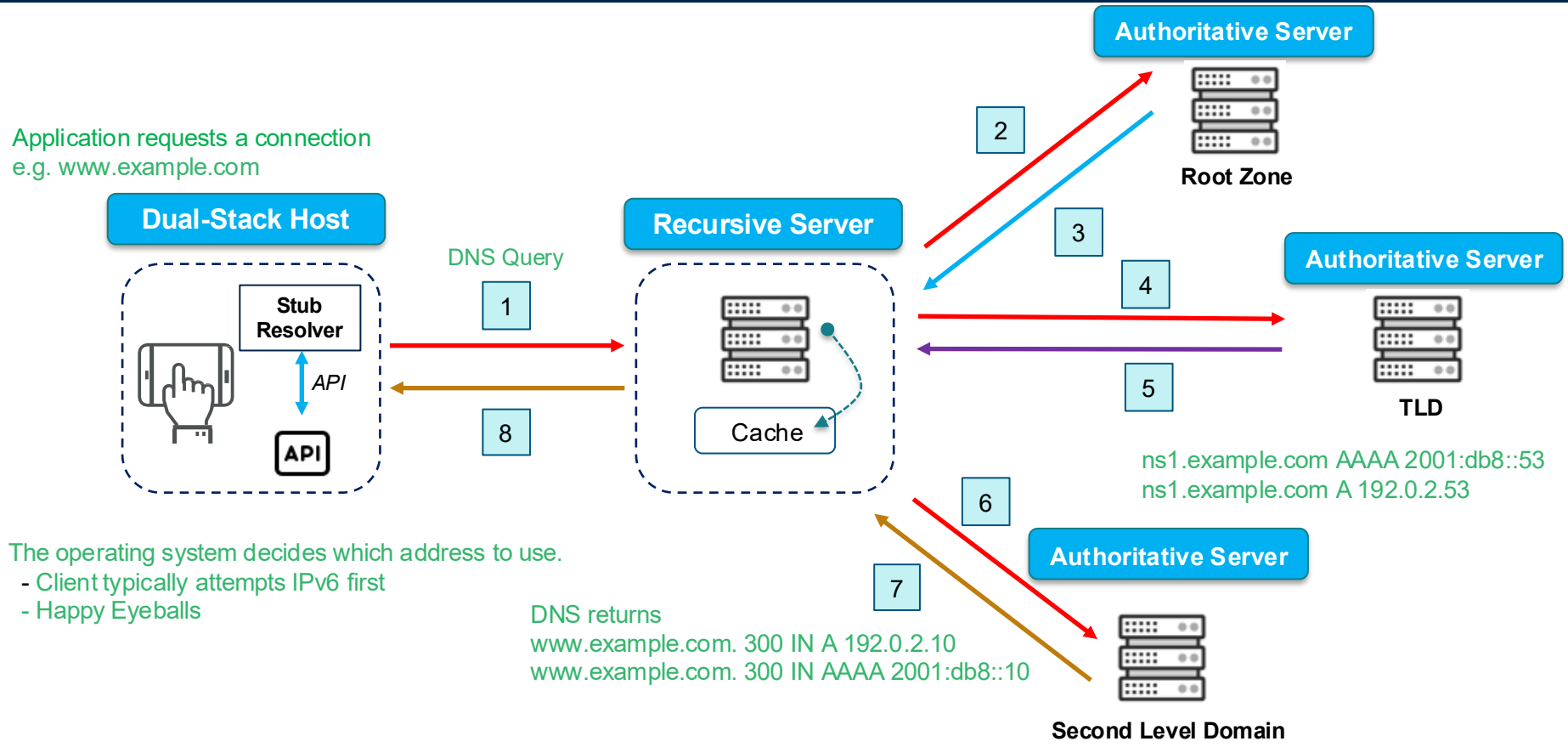


- DNS returns,

```
www.example.com.  IN A      192.0.2.10
www.example.com.  IN AAAA   2001:db8::10
```

- The client chooses IPv6 if available and falls back to IPv4.
- Challenges
  - Requires managing both protocols
  - Higher operational complexity

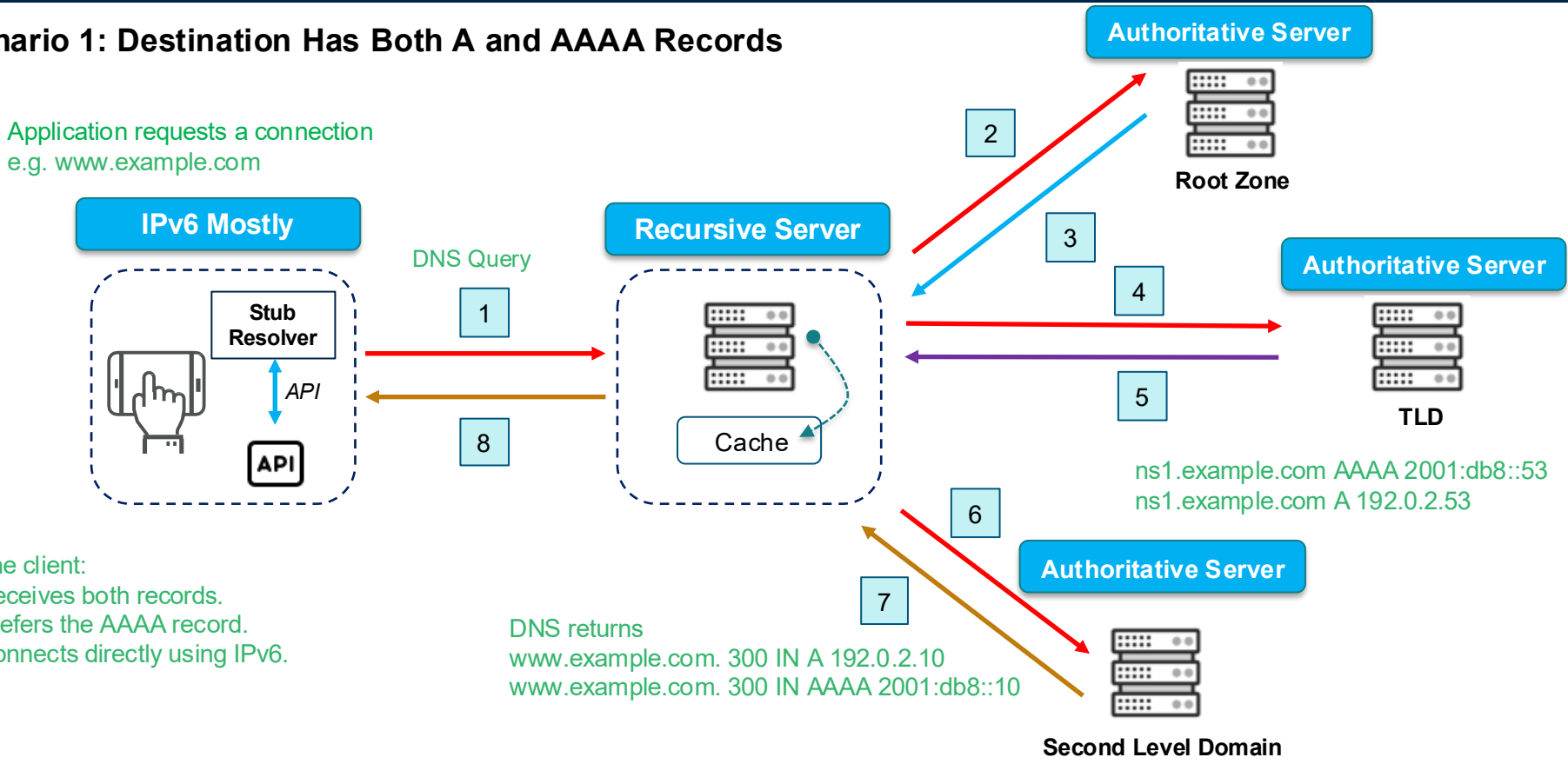
DNS Query Resolution – Dual-Stack



IPv6 Mostly

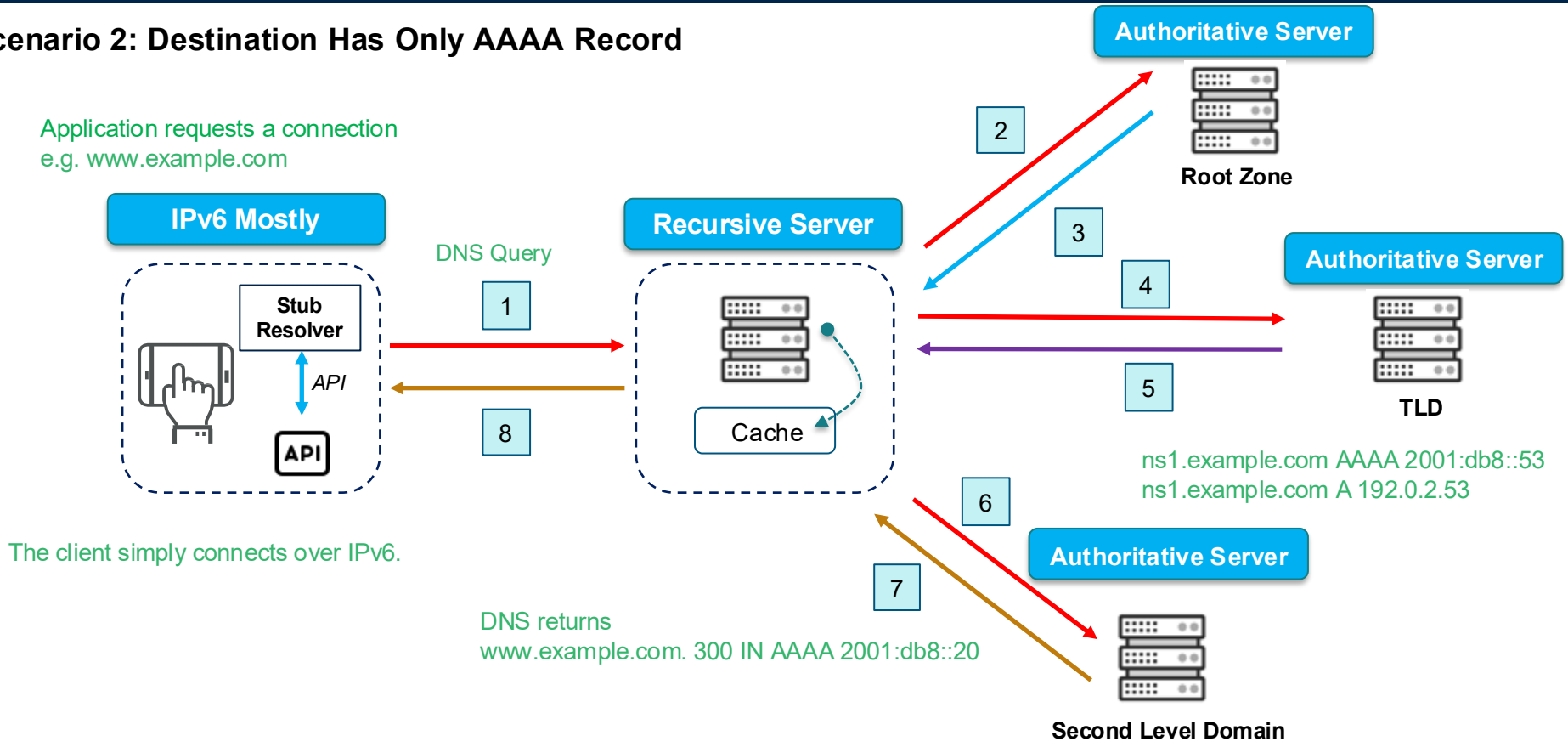
DNS Query Resolution – IPv6 Mostly

Scenario 1: Destination Has Both A and AAAA Records



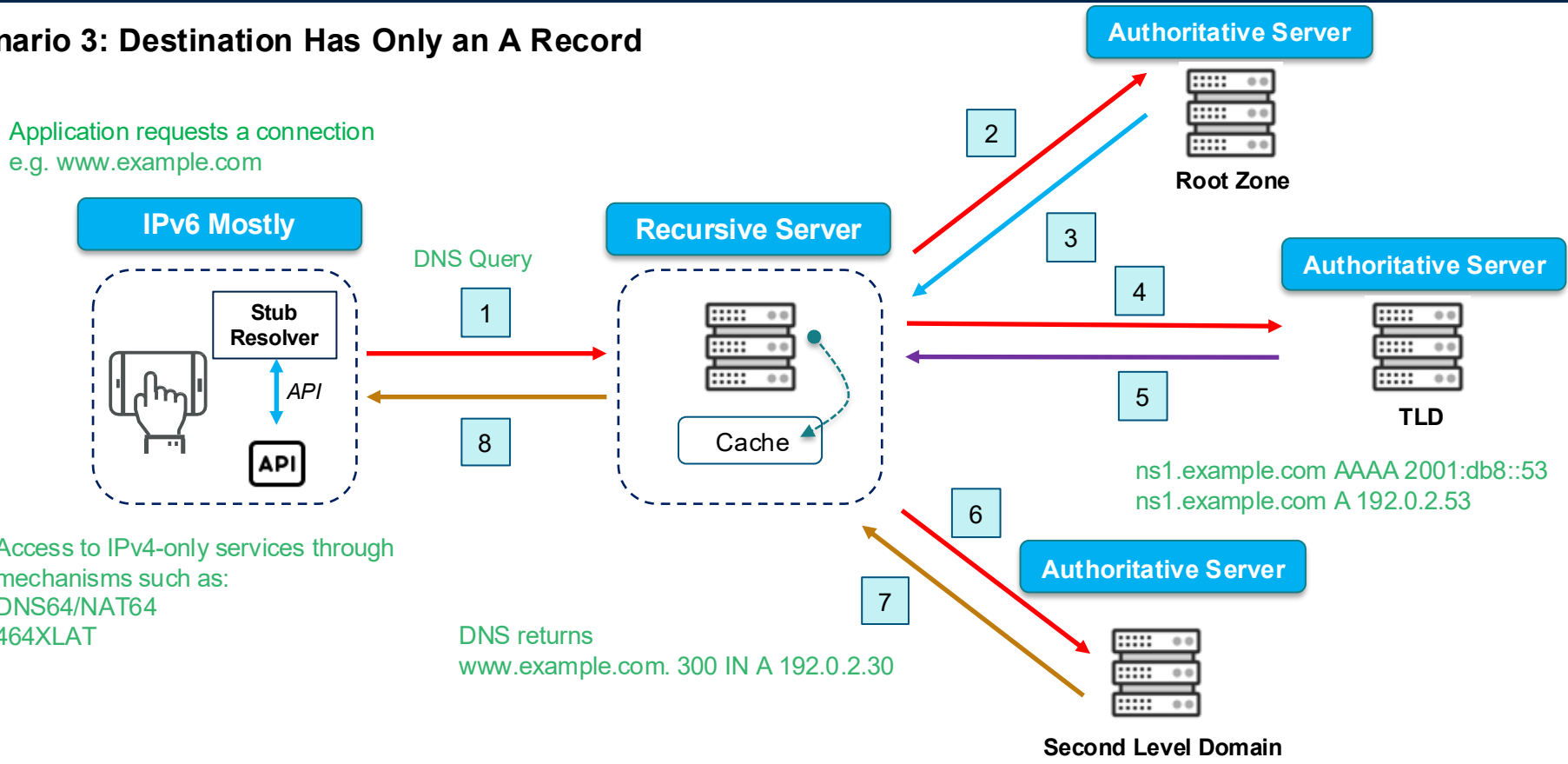
DNS Query Resolution – IPv6 Mostly

Scenario 2: Destination Has Only AAAA Record



DNS Query Resolution – IPv6 Mostly

Scenario 3: Destination Has Only an A Record



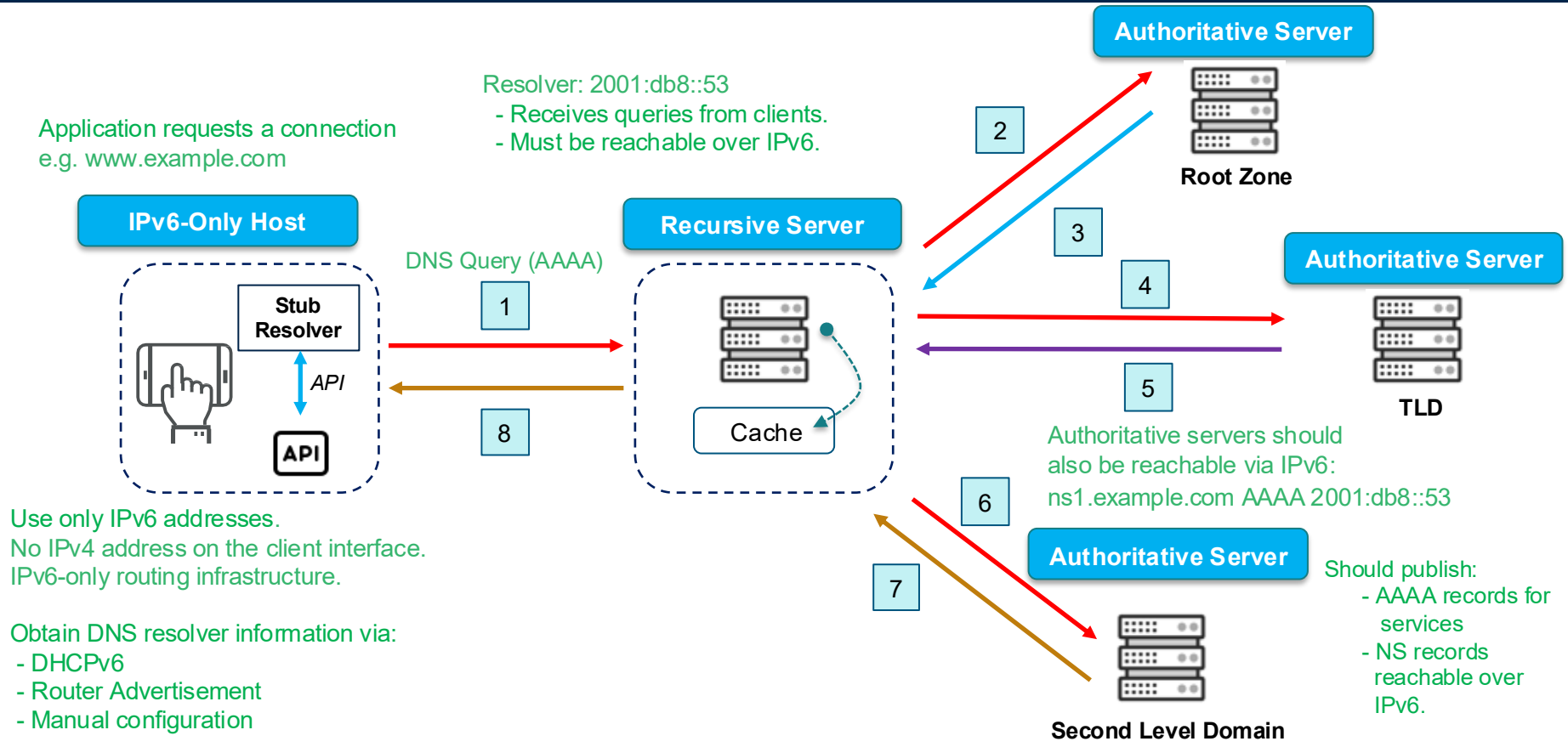
IPv6 Only

DNS Infrastructure in IPv6-Only Networks

- The DNS infrastructure itself must be reachable via IPv6
- The client is configured with an IPv6 DNS resolver
- Authoritative servers should also be reachable via IPv6

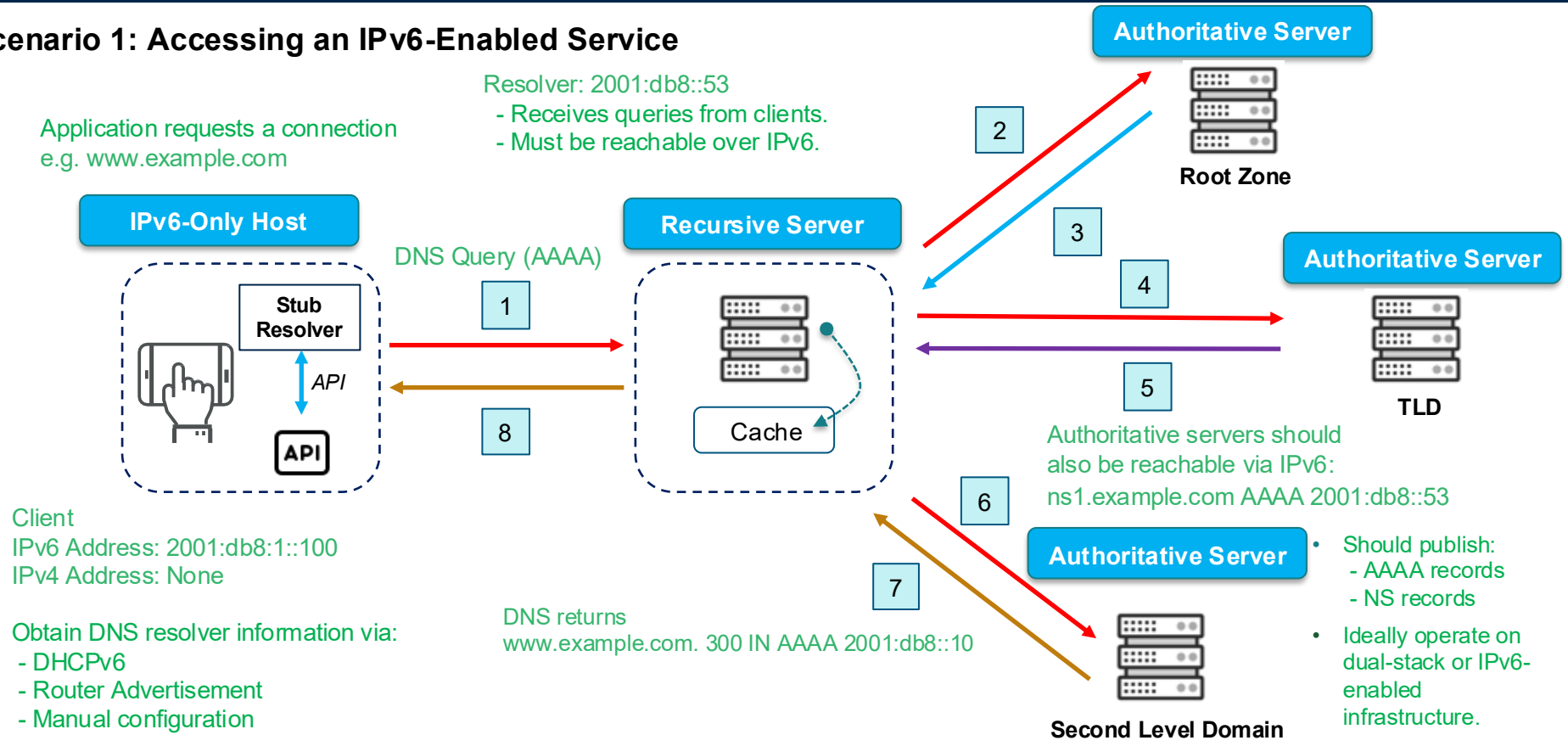
This allows the entire DNS resolution path to function over IPv6

DNS Query Resolution – IPv6 Only



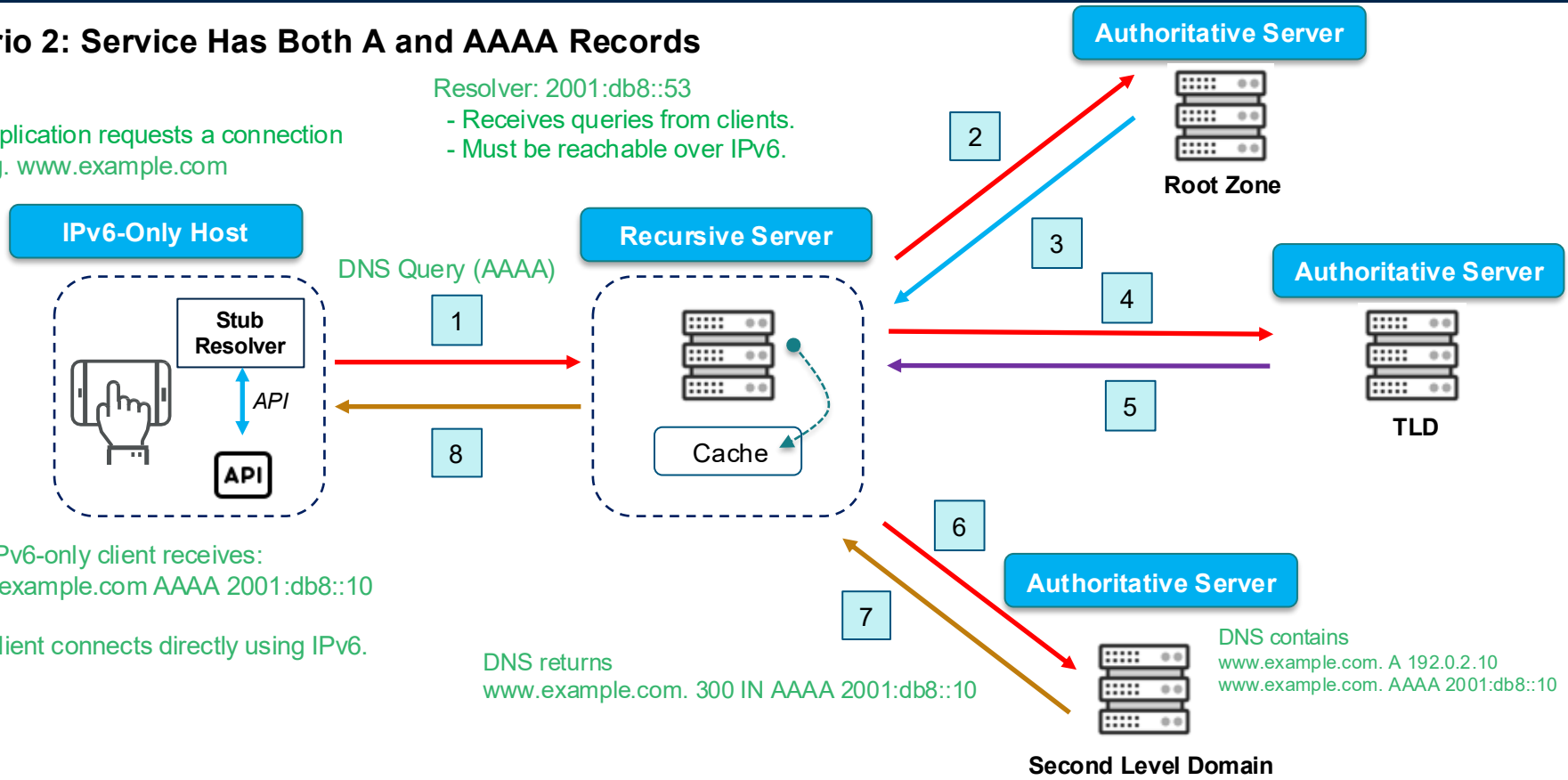
DNS Query Resolution – IPv6 Only

Scenario 1: Accessing an IPv6-Enabled Service



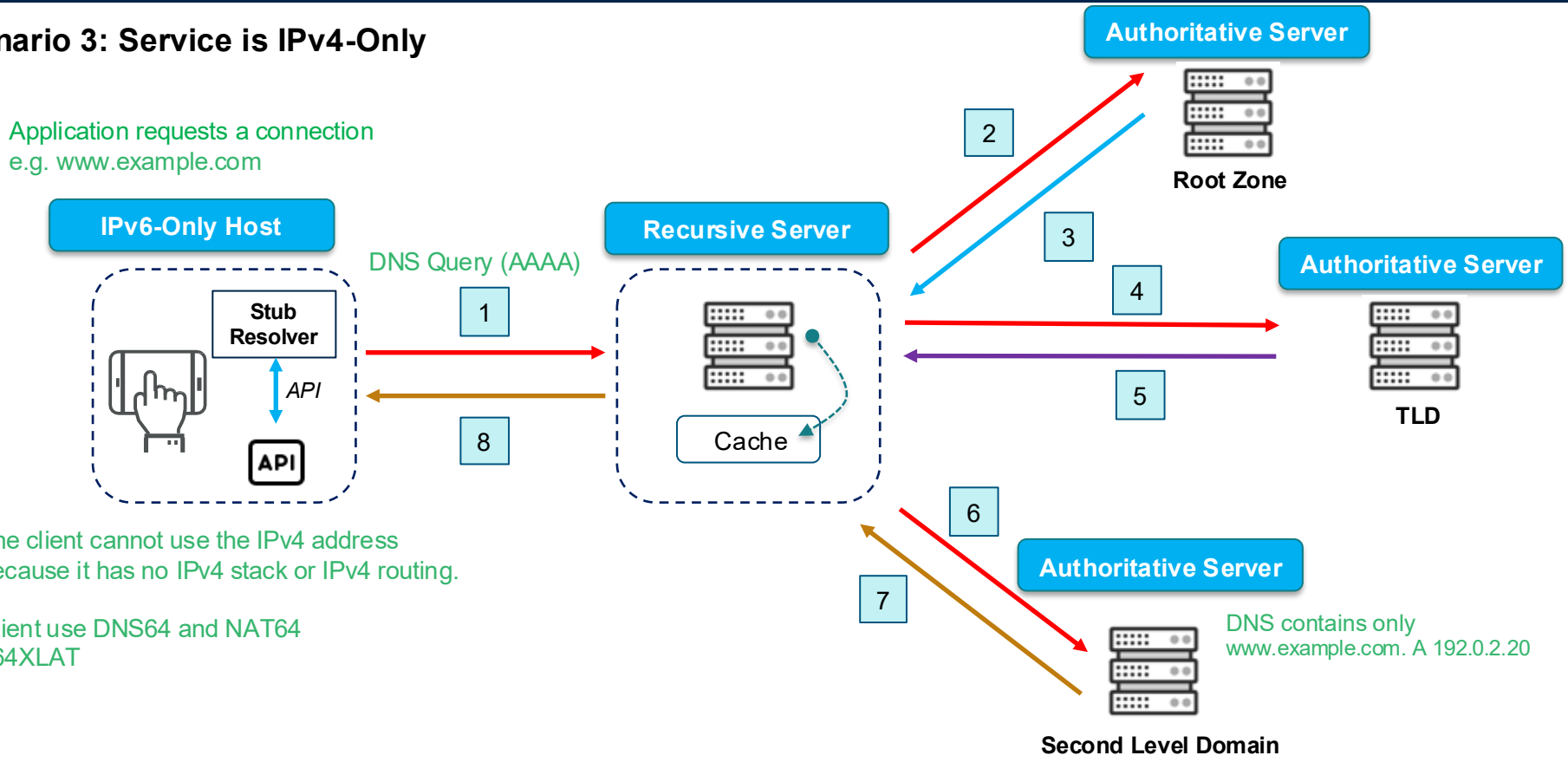
DNS Query Resolution – IPv6 Only

Scenario 2: Service Has Both A and AAAA Records



DNS Query Resolution – IPv6 Only

Scenario 3: Service is IPv4-Only



DNS Transport in IPv6 Networks

- DNS queries are transported over IPv6 using:
  - UDP/53
  - TCP/53
  - TLS/853 (DoT, DoQ)
  - HTTPS/443 (DoH)
- Client → Recursive Resolver (IPv6)
- Recursive Resolver → Authoritative Server (IPv6)

All DNS protocols work exactly as they do in IPv4 environments.

DNS Record Requirements

- AAAA Records
  - In IPv6-only environments, services should publish AAAA records:

    ```
    host.example.com.  IN AAAA 2001:db8::1
    ```

  - Clients primarily rely on AAAA records to reach services.
- PTR Records
  - Reverse DNS should come under:

    ```
    ip6.arpa
    ```

  - Example:

    ```
    1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. PTR host.example.com.
    ```

Accessing IPv4-only Services

- An IPv6-only client may receive:

```
www.example-legacy.com. IN A 192.0.2.20
```

- But the IPv6-only client cannot directly connect to that IPv4 address
- So, how to solve this issue?
  - DNS64 + NAT64
  - 464XLAT
  - Dual-Stack etc.

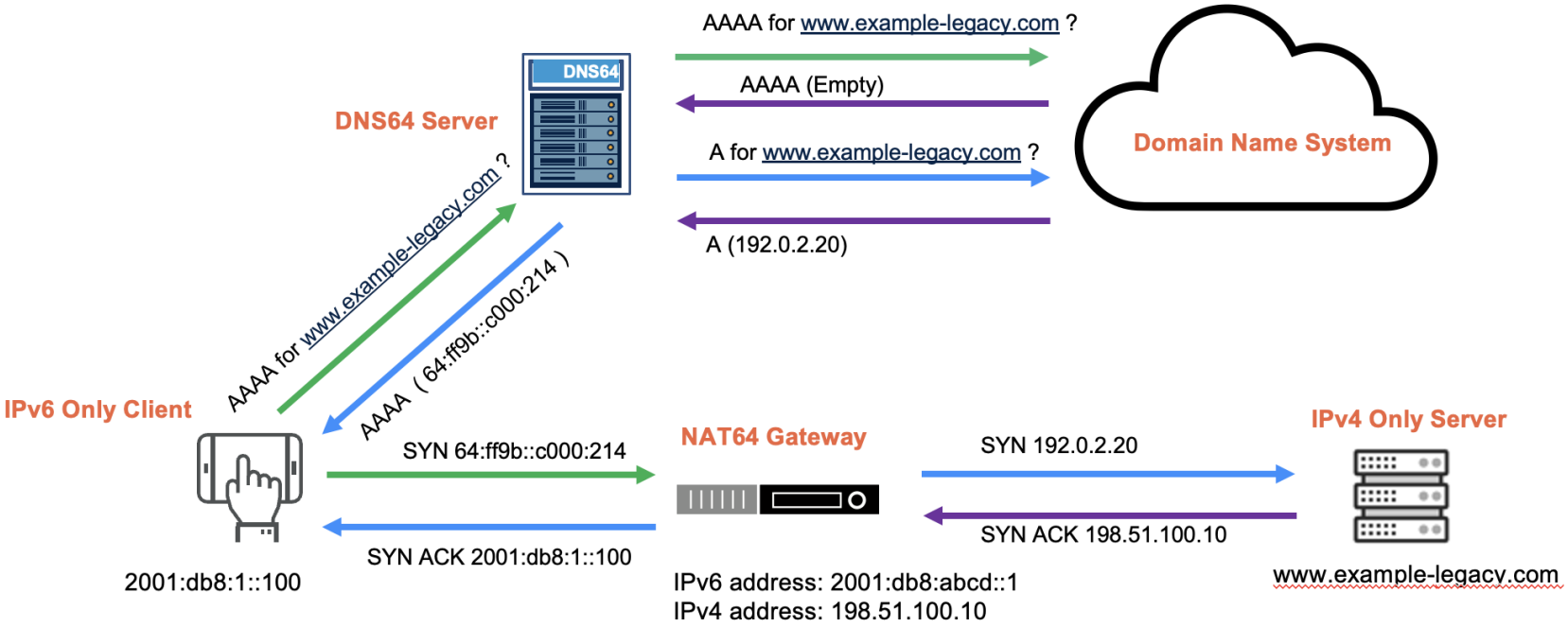
DNS64 + NAT64

- Widely deployed solution for IPv6-only networks.
  - No IPv4 required on clients.
  - Scalability
  - Allows IPv6-only hosts to continue reaching legacy IPv4 services while encouraging native IPv6 adoption

How DNS64 + NAT64 Works

1. An IPv6-only client requests the address of a website (AAAA).
2. DNS64 Checks Authoritative DNS.
   No AAAA record exists. Authoritative DNS returns A record.
3. The DNS64 server receives only an A record
4. DNS64 synthesizes an AAAA record using a special IPv6 prefix
5. Client receives synthesized AAAA.
6. The Client connects via IPv6
7. NAT64 translates the IPv6 address into IPv4 address.

How DNS64 + NAT64 Works



464XLAT

- An enhancement of NAT64.
- Some applications are hardcoded to use IPv4 literals and cannot use DNS64.
- 464XLAT allows such applications to continue working.
- Presents an IPv4 environment locally while transporting traffic over IPv6
- Components
  - CLAT (Customer-side translator)
  - PLAT (Provider-side translator/NAT64)

CLAT (Customer-side Translator)

- Functions
  - Provides a private IPv4 address to applications
  - Translates IPv4 packets into IPv6 packets
  - Uses stateless translation
- When the application wants to reach an IPv4 address CLAT converts that IPv4 destination into an IPv6 representation and sends it into the IPv6-only network

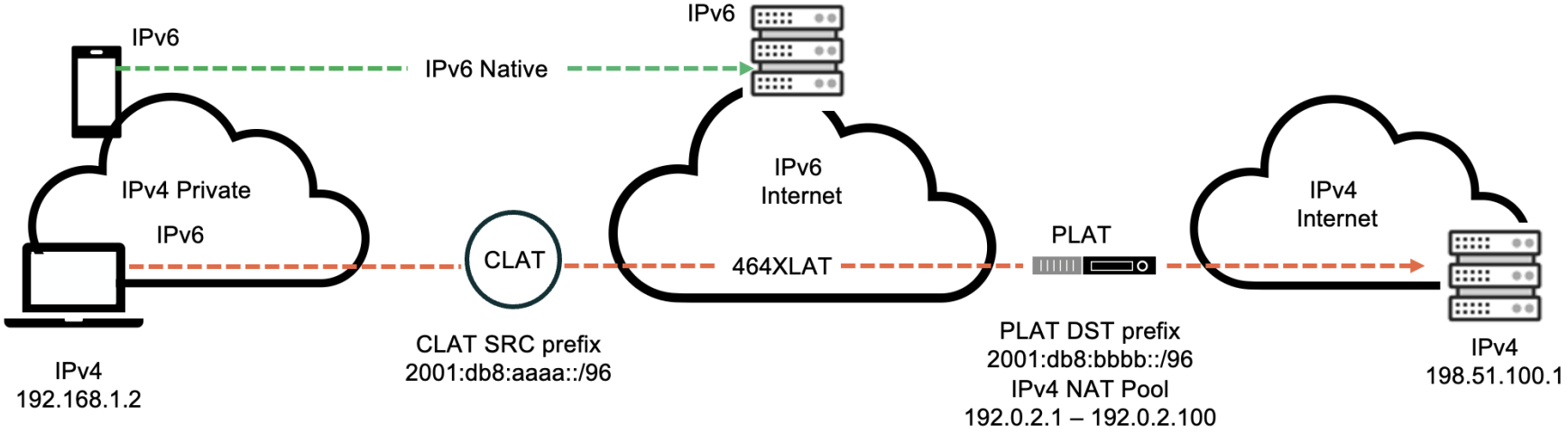
PLAT (Provider-side Translator)

- Located in the provider network
- Functions
  - Receives IPv6 packets from the CLAT
  - Performs stateful NAT64 translation
  - Communicates with the IPv4 Internet
- The PLAT is essentially a NAT64 gateway

How 464XLAT Works

1. Application generates IPv4 traffic and believes it is using IPv4
2. CLAT translates IPv4 → IPv6
3. The packet is now IPv6
4. IPv6-only network transports packet
5. PLAT performs NAT64
6. The packet is now IPv4 again
7. The client access the IPv4 service

How 464XLAT Works

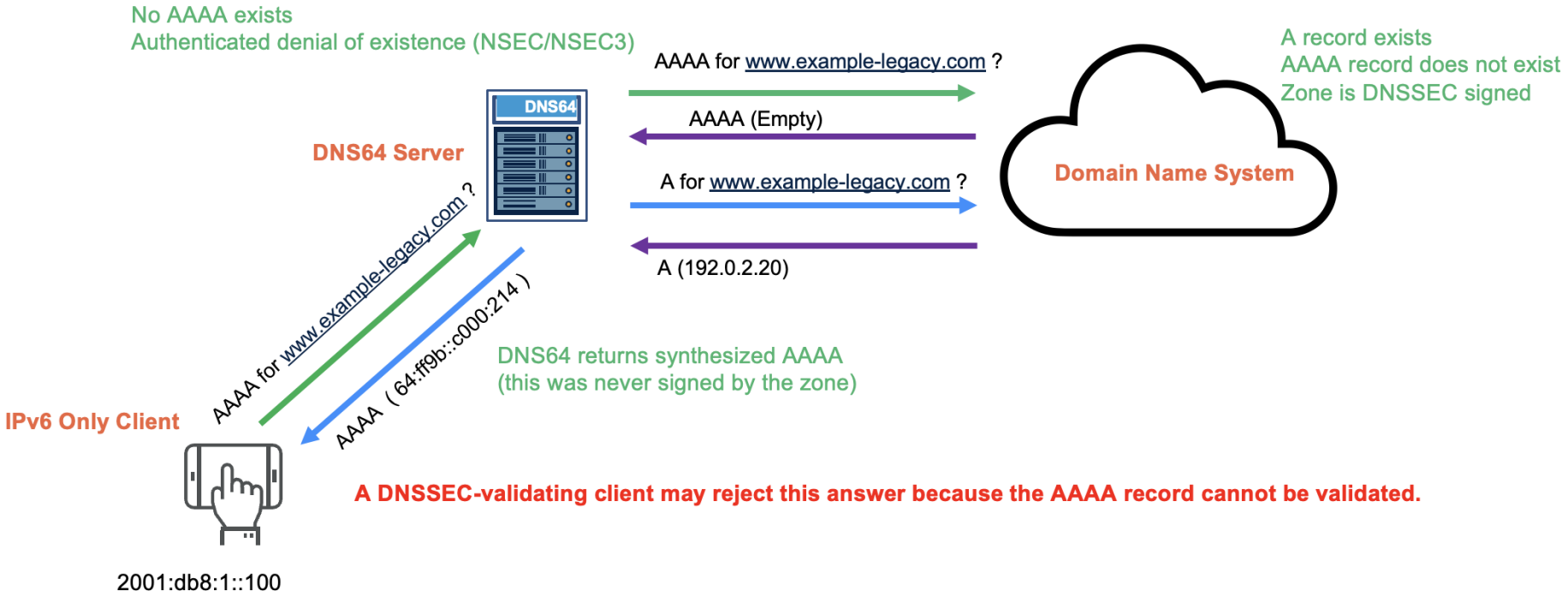


DNSSEC for IPv6 Only Networks

DNSSEC - Challenges with DNS64/NAT64?

- Synthesized AAAA record does **not exist in the authoritative zone**.
  - No AAAA record was signed.
  - No RRSIG exists for the synthesized AAAA.
  - DNS64 created data that DNSSEC cannot directly validate.
- This creates a conflict between:
  - DNS64's modification of DNS answers
  - DNSSEC's requirement that answers remain unchanged

DNSSEC - Challenges with DNS64/NAT64?



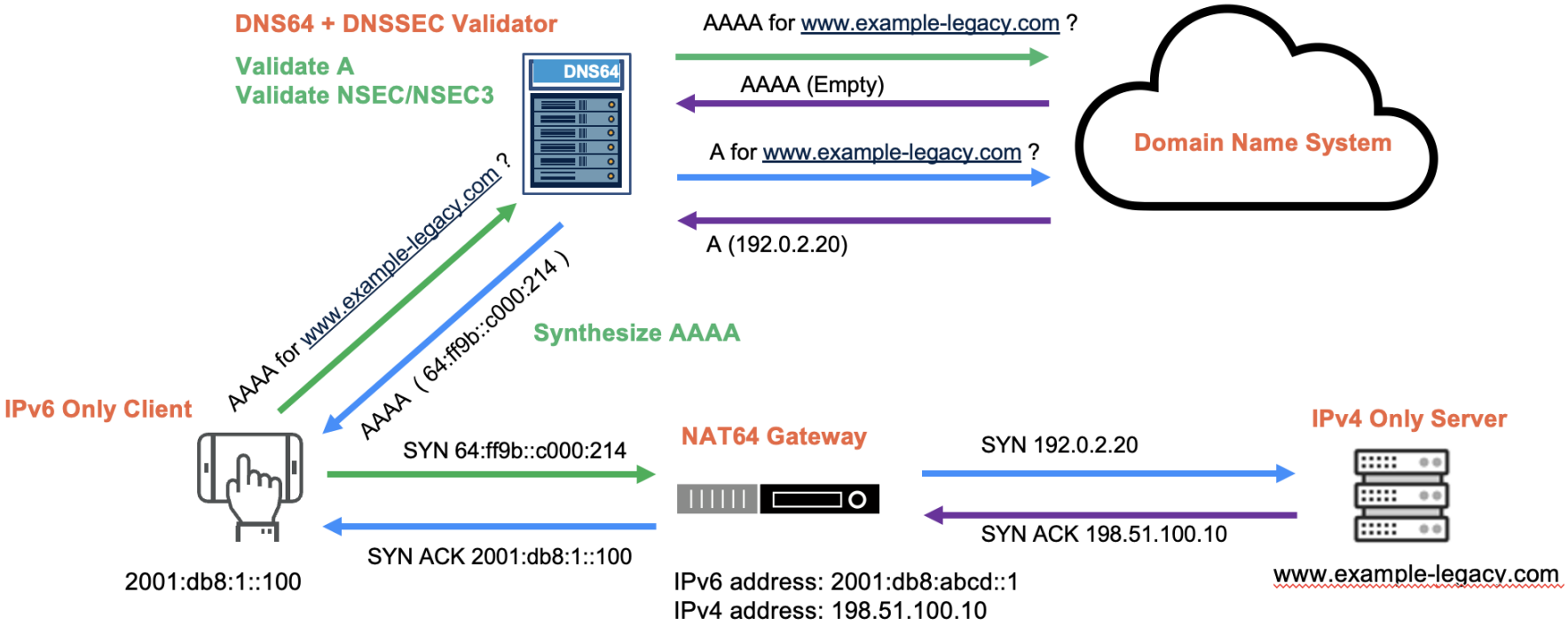
DNSSEC Validation Options

- Validation at DNS64 Resolver
  - Works correctly (Client trusts the recursive resolver's validation instead of validating the synthesized AAAA itself)
  - IPv6-only clients need no special handling
- Validation at End Client
  - Client receives synthesized AAAA records and these records were never signed.
  - DNSSEC validation fails

Solution – Enabling DNSSEC Validation on DNS64 Resolver

1. Client sends AAAA query
2. DNS64 resolver queries authoritative servers.
3. Resolver validates DNSSEC signatures
4. Resolver receives a valid A record and Authenticated proof that AAAA does not exist
5. Resolver synthesizes AAAA locally.
6. The DNS64 resolver knows that the A record is authentic, the AAAA truly does not exist and the synthesized AAAA was derived from validated information.
7. Resolver returns synthesized AAAA to the client

DNSSEC for DNS64/NAT64



Authenticated Denial of Existence

- DNS64 relies heavily on DNSSEC's authenticated denial mechanisms
  - NSEC
  - NSEC3
- Without this proof, a DNS64 resolver cannot safely determine whether synthesis is appropriate.

BCP for IPv6 Only Networks

- Enable DNSSEC validation on the recursive resolver
- Enable DNS64 synthesis on the same resolver
- Do not rely on DNSSEC validation at the client
- Use the resolver's AD bit as the trust indicator
- Ensure NSEC/NSEC3 responses are available and correctly validated

Summary – What we discussed

- IPv6 Deployment Stages
  - Dual-Stack
  - IPv6 Mostly scenarios
  - IPv6 Only scenarios
- DNS64
- NAT64
- 464XLAT
- DNS and DNSSEC for IPv6 Only Networks

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann