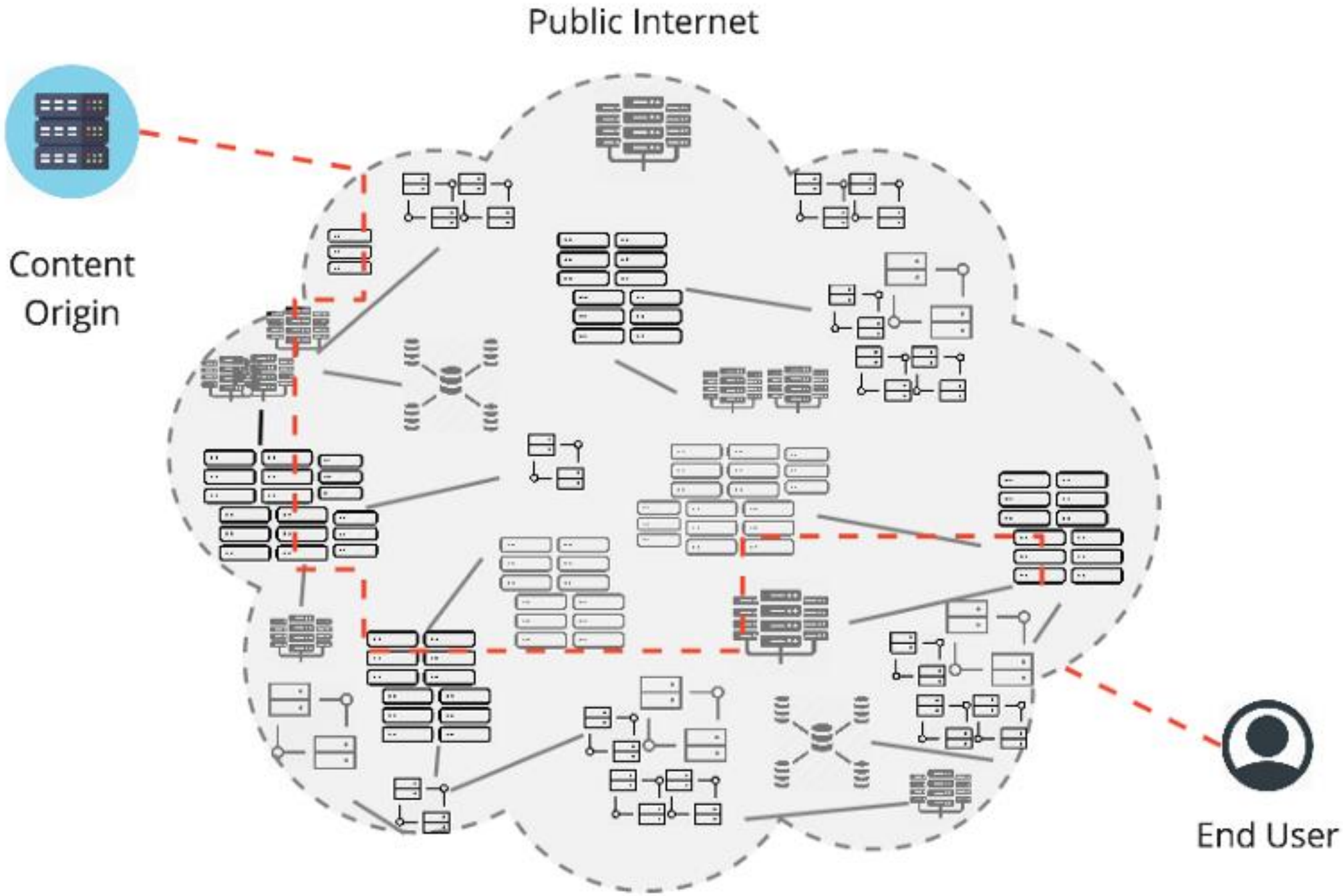
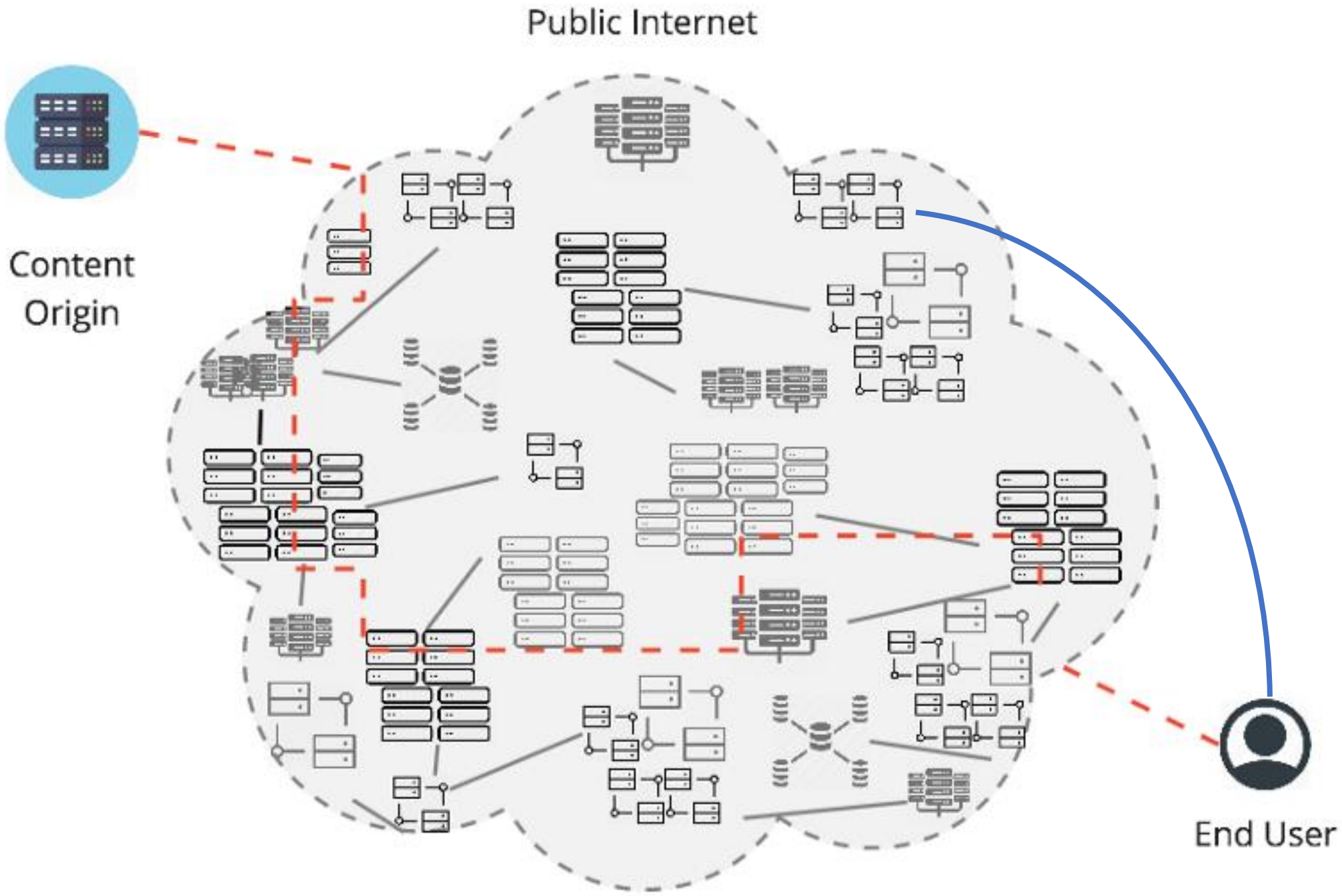
Alt-Svc and Friends

What we have, where we’re going


Public Internet
Content Origin
End User


Public Internet
Content Origin
End User

Scenarios we care about

DNS mis-resolution	Anycast misrouting	Controlled endpoints	Protocol availability
• Resolver is far from client • Resolver doesn't forward Client Subnet to DNS authoritative	• Anycast reached a suboptimal endpoint	• Some server endpoints aren't public, but you're eligible for them (due to network, capabilities, etc.)	• Server supports more preferred protocol than client used, on this or a different endpoint

Ways to Redirect

Together?

Clients that implement support for both Alt-Svc and HTTPS records and are making a connection based on a cached Alt-Svc response SHOULD retrieve any HTTPS records for the Alt-Svc alt-authority, and ensure that their connection attempts are consistent with both the Alt-Svc parameters and any received HTTPS SvcParams. If present, the HTTPS record's TargetName and port are used for connection establishment (as in Section 3). For example, suppose that "https://example.com" sends an Alt-Svc field value of:

```
Alt-Svc: h2="alt.example:443", h2="alt2.example:443", h3=":8443"
```

The client would retrieve the following HTTPS records:

```
alt.example.                IN HTTPS 1 . alpn=h2,h3 ech=...
alt2.example.               IN HTTPS 1 alt2b.example. alpn=h3 ech=...
_8443._https.example.com.  IN HTTPS 1 alt3.example. (
    port=9443 alpn=h2,h3 ech=... )
```

Troubles with Alt-Svc

How to verify cached information remains valid?

- Supposed to clear on network change (with exceptions), but clients don’t always know when network changes
- Endpoint configuration or CDN load balancing may have changed since the cached record

What if they disagree?

- Headers received directly from origin are more trusted
- Information from DNS is fresher

Replacement? Delegate to SVCB/HTTPS

```
Alt-SvcB:  “oxford.svc2.example”
```

Semantics for Alt-SvcB

Now:

- Ignore any legacy Alt-Svc entries that may be present or cached
- Do an HTTPS lookup for the provided hostname
- Perform “SVCB-required” connection attempt as per SVCB/HTTPS spec
- Use that connection instead of this one for future requests, if successful

In Future:

- Remember the endpoint you wound up connecting to, if successful
- Prefer that endpoint if it appears in future HTTPS resolutions for this origin, regardless of prioritization between endpoints

Open Debate: Stickiness vs. Disclosure

- If client doesn’t remember the Alt-Svc or clears it too soon, it will get the same redirection from the origin and flip-flop between origin and alternative.
- If client remembers Alt-Svc too long, it will continue using an endpoint which might no longer be in service.
- Current design for stickiness relies on publishing all still-valid alternatives in the origin’s HTTPS record
  - Some providers might not want to publish all endpoints

Thoughts from HTTP Workshop

DNS is always current(-ish), so DNS should have exclusive say over:

- Which CDN is used, if any
- Properties of the endpoint being contacted (Protocol support, ECH keys, etc.)

Alt-Svc is most useful for endpoint redirection

- Primarily for the current session
- Stickiness might not be a priority